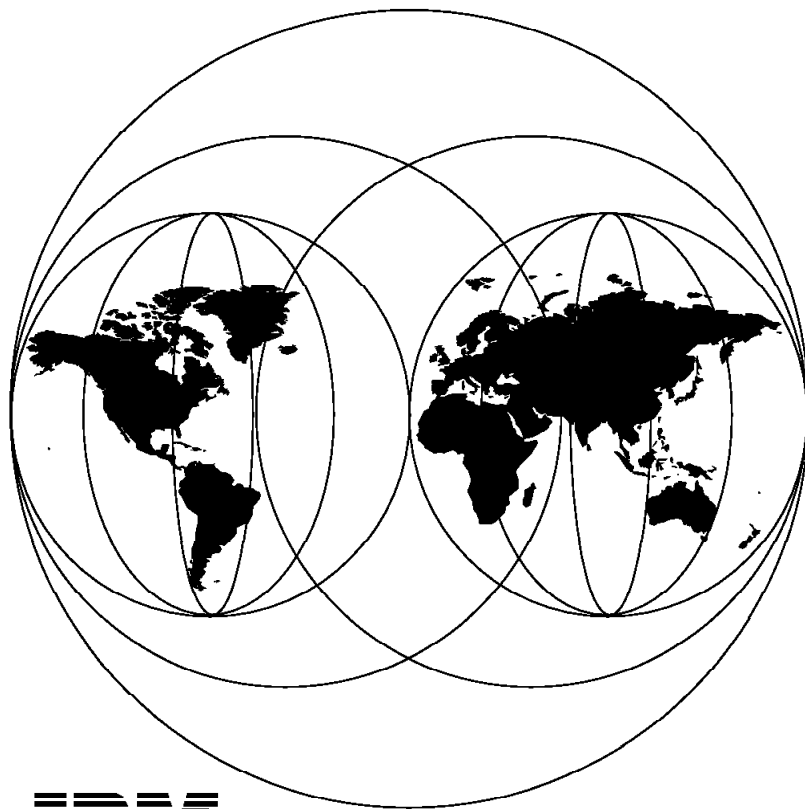


International Technical Support Organization

SG24-4579-00

**Enterprise-Wide Security Architecture and
Solutions Presentation Guide**

November 1995



**International Technical Support Organization
Poughkeepsie Center**



International Technical Support Organization

SG24-4579-00

**Enterprise-Wide Security Architecture and
Solutions Presentation Guide**

November 1995

Take Note!

Before using this information and the product it supports, be sure to read the general information under "Special Notices" on page xiii.

First Edition (November 1995)

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSO Technical Bulletin Evaluation Form for reader's feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 541 Mail Station P099
522 South Road
Poughkeepsie, New York 12601-5400

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1995. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Abstract

This presentation guide describes the IBM Security Architecture and its relationship to other IBM strategies, architectures, and ongoing international standards activities. Detailed security sections apply the security architecture concepts to specific system platforms, the client/server distributed computing environment, cryptographic facilities, network/Internet communications, application security support, anti-virus measures, and security management.

This document is intended for use as presentation material to IBM customers by IBM system engineers and other marketing personnel. Specific security products and solutions are included such as RACF, NetSP, ICRF, ICSF, Transaction Security System, the DSM Family, Distributed Key Management System, the Internet Connection Family and the IBM AntiVirus product.

(229 pages)

Contents

Abstract	iii
Special Notices	xiii
Preface	xv
How This Document is Organized	xv
How to Select which Foils to Use	xvii
Security Related Information on the World Wide Web (WWW)	xvii
Related Publications	xvii
International Technical Support Organization Publications	xviii
ITSO Redbooks on the World Wide Web (WWW)	xix
Acknowledgments	xix
Notices	xxi
Chapter 1. Enterprise-Wide Security Architecture and Solutions	1
1.1 Customer Testimonials	2
1.2 Current Environment	3
1.3 Security is a Serious Customer Problem	6
1.4 Threats in Today's Electronic World	8
1.5 Leading User Group Requirements	10
1.6 Strategic Security Drivers	12
1.7 Security Standards and Criteria	17
1.8 Responding to Customer Needs	19
1.9 Developing a Security Policy	22
1.10 The Security Process Cycle	23
Chapter 2. IBM Security Strategy and Architecture	25
2.1 IBM Security Strategy (Stage1)	26
2.2 IBM Security Strategy (Stage2)	29
2.3 IBM Security Architecture	30
2.3.1 System Integrity, Assurance and Trust	32
2.3.2 Security Services	35
2.3.3 Security Mechanisms	37
2.3.4 Security Objects	39
2.3.5 Identification and Authentication Service	41
2.3.6 Entity Authentication Mechanism	42
2.3.7 Access Control Service	45
2.3.8 Access Control Mechanisms	46
2.3.9 Confidentiality Service	50
2.3.10 Encipherment/Decipherment Mechanisms	52
2.3.11 Data Integrity Service	54
2.3.12 Data Integrity Mechanisms	55
2.3.13 Non-Repudiation Service	58
2.3.14 Digital Signature Mechanism	59
2.3.15 Security Management, Audit and Policy	61
2.4 IBM Security Architecture Summary	63
2.5 IBM's Ongoing Commitment	64
2.5.1 Standards, Interfaces and Architectures	67
2.5.2 Standards, Interfaces and Architectures (continued)	69
2.6 Related Strategies and Architectures	71
2.6.1 IBM's Open Blueprint	72

2.6.2 DCE Security Services	75
2.6.3 Object Oriented Security	77
2.6.4 System Management (SystemView)	81
2.6.5 Information Warehouse	83
2.6.6 IBM Common Cryptographic Strategy	86
2.6.7 Security Evaluation Strategy	88
Chapter 3. Platform Security	91
3.1 Platform Security Support Overview	92
3.2 MVS/ESA	93
3.2.1 MVS/ESA and RACF	93
3.2.2 MVS/ESA Open Edition	96
3.3 VM/ESA and RACF	98
3.4 System Authorization Facility (SAF)	100
3.5 OS/400	102
3.6 AIX/6000	104
3.7 OS/2	107
3.8 Process Resource/Systems Manager	109
Chapter 4. DCE Security	111
4.1 OSF DCE Structure	112
4.2 OSF DCE Security	114
4.3 DCE Security Services	116
4.4 Supported Platforms	119
4.5 MVS Specific	120
4.5.1 DCE - RACF Interoperation	120
4.5.2 DCE and OpenEdition MVS	122
Chapter 5. Application Security	123
5.1 CICS/ESA	124
5.2 IMS/ESA and DB2	127
5.3 Distributed Relational DB Architecture	131
5.4 DB2/x Data Security	134
5.5 Data Administration - DataHub	137
5.6 Structured Query Language (SQL)	139
5.7 MQSeries	141
5.8 ACF/VTAM	143
5.9 NetView Access Services (NV/AS)	145
5.10 NetSP Secured Logon Coordinator	146
Chapter 6. Cryptographic Security	149
6.1 Why Cryptography?	150
6.2 Cryptographic Algorithms	152
6.3 Keys Within Cryptography	155
6.4 Cryptographic Strategy	157
6.5 Common Cryptographic Architecture (CCA)	158
6.6 IBM CCA Offerings	161
6.6.1 Transaction Security System	163
6.6.2 Integrated Cryptographic Feature (ICRF)	168
6.6.3 Distributed Key Management System (DKMS)	170
Chapter 7. Internet Security	175
7.1 What is the Internet?	176
7.2 What is a Firewall?	178
7.2.1 Firewall Security Options	180

7.2.2 Internet Connection Secured Network Gateway	182
7.3 World Wide Web (WWW)	185
7.4 Internet Keyed Payment Protocol (iKP)	189
Chapter 8. AntiVirus Security	191
8.1 Computer Viruses	192
8.2 AntiVirus Security	194
8.3 IBM AntiVirus Product	196
Chapter 9. Security Management	199
9.1 Security Management - The Challenge	200
9.2 Security Management Strategy	202
9.3 System Management (SystemView)	203
9.4 Security Management Solutions	205
9.5 IBM DSM Family	207
9.5.1 IBM Distributed Security Manager/MVS Offering	209
9.5.2 IBM Distributed Security Manager/AIX & OS/2	211
Chapter 10. IBM Security Support and Services	213
10.1 I/T Security Consulting and Services - Issues and Answers	214
10.2 I/T Security Consulting and Services - I/T Executive Challenges	215
10.3 I/T Security Consulting and Services - Capabilities & Customized Proposals	217
10.4 IBM Security Support and Services - Summary	219
Chapter 11. Summary	223
List of Abbreviations	225
Index	227

Figures

1.	Enterprise-Wide Security Architecture and Solutions	1
2.	Customer Testimonials	2
3.	Current Environment	3
4.	Security is a Serious Customer Problem	6
5.	Threats in Today's Electronic World	8
6.	Leading User Group Requirements	10
7.	Strategic Security Drivers	12
8.	Security Standards and Criteria	17
9.	Responding to Customer Needs	19
10.	Developing a Security Policy	22
11.	The Security Process Cycle	23
12.	IBM Security Strategy and Architecture	25
13.	IBM Security Strategy (Stage1)	26
14.	IBM Security Strategy (Stage2)	29
15.	IBM Security Architecture	30
16.	System Integrity, Assurance and Trust	32
17.	Security Services	35
18.	Security Mechanisms	37
19.	Security Mechanisms	39
20.	Identification and Authentication Service	41
21.	Entity Authentication Mechanism	42
22.	Access Control Service	45
23.	Access Control Mechanisms	46
24.	Confidentiality Service	50
25.	Encipherment/Decipherment Mechanisms	52
26.	Data Integrity Service	54
27.	Data Integrity Mechanisms	55
28.	Non-Repudiation Service	58
29.	Digital Signature Mechanism	59
30.	Security Management, Audit and Policy	61
31.	IBM Security Architecture Summary	63
32.	IBM's Ongoing Commitment	64
33.	Standards, Interfaces and Architectures	67
34.	Standards, Interfaces and Architectures (continued)	69
35.	Related Strategies and Architectures	71
36.	IBM's Open Blueprint	72
37.	DCE Security Services	75
38.	Object Oriented Security	77
39.	System Management (SystemView)	81
40.	Information Warehouse	83
41.	IBM Common Cryptographic Strategy	86
42.	Security Evaluation Strategy	88
43.	Platform Security	91
44.	Platform Security Support Overview	92
45.	MVS/ESA and RACF	93
46.	MVS/ESA Open Edition	96
47.	VM/ESA and RACF	98
48.	System Authorization Facility (SAF)	100
49.	OS/400	102
50.	AIX/6000	104
51.	OS/2	107

52.	Process Resource/Systems Manager	109
53.	DCE Security	111
54.	OSF DCE Structure	112
55.	OSF DCE Security	114
56.	DCE Security Services	116
57.	Supported Platforms	119
58.	DCE - RACF Interoperation	120
59.	DCE and OpenEdition MVS	122
60.	Application Security	123
61.	CICS/ESA	124
62.	IMS/ESA and DB2	127
63.	Distributed Relational DB Architecture	131
64.	DB2/x Data Security	134
65.	Data Administration - DataHub	137
66.	Structured Query Language (SQL)	139
67.	MQSeries	141
68.	ACF/VTAM	143
69.	NetView Access Services (NV/AS)	145
70.	NetSP Secured Logon Coordinator	146
71.	Cryptographic Security	149
72.	Why Cryptography?	150
73.	Cryptographic Algorithms	152
74.	Keys Within Cryptography	155
75.	Cryptographic Strategy	157
76.	Common Cryptographic Architecture (CCA)	158
77.	IBM CCA Offerings	161
78.	Transaction Security System	163
79.	Integrated Cryptographic Feature (ICRF)	168
80.	Distributed Key Management System (DKMS) - Key Points	170
81.	Distributed Key Management System (DKMS) - Architectural Overview	172
82.	Internet Security	175
83.	What is the Internet?	176
84.	What is a Firewall?	178
85.	Firewall Security Options	180
86.	Internet Connection Secured Network Gateway	182
87.	World Wide Web (WWW)	185
88.	WWW Security	187
89.	Internet Keyed Payment Protocol (iKP)	189
90.	AntiVirus Security	191
91.	Computer Viruses	192
92.	AntiVirus Security	194
93.	IBM AntiVirus Product	196
94.	Security Management	199
95.	Security Management - The Challenge	200
96.	Security Management Strategy	202
97.	System Management (System View)	203
98.	Security Management Solutions	205
99.	IBM DSM Family	207
100.	IBM Distributed Security Manager/MVS Offering	209
101.	IBM Distributed Security Manager/AIX & OS/2	211
102.	IBM Security Support and Services	213
103.	I/T Security Consulting and Services - Issues and Answers	214
104.	IT Security Consulting and Services - I/T Executive Challenges	215
105.	I/T Security Consulting and Services - Capabilities & Customized Proposals	217

106. IBM Security Support and Services Summary 219
107. Summary 223

Special Notices

This publication is intended to help IBM marketing personnel communicate IBM's Security Architecture and solutions to IBM customers. The information in this publication is not intended to be the specification of any programming interfaces that are provided by any of the security products. Refer to the PUBLICATIONS section of the IBM Programming Announcement for specific security products such as RACF, ICRF, ICSF, DSM, DKMS, NetSP SLC, Internet Connection SNG, Transaction Security System and IBM AntiVirus for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

The following document contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples contain the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

You can reproduce a page in this document as a transparency, if that page has the copyright notice on it. The copyright notice must appear on each page being reproduced.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

IBM

The following terms are trademarks of other companies:

Windows is a trademark of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

C-bus is a trademark of Corollary, Inc.

Other trademarks are trademarks of their respective companies.

Preface

This document is a presentation guide for IBM customers, system engineers, and other marketing personnel. This presentation describes the IBM Security Architecture and its relationship to other strategies and international standards activities. Detailed security sections apply the security architecture concepts to specific system platforms, the client/server distributed computing environment, cryptographic facilities, network/internet communications, application security support, anti-virus measures and security management. Specific IBM security products and solutions are included such as:

- Resource Access Control Facility (RACF)
- Distributed Security Manager (DSM) Family
- Transaction Security System
- Integrated Cryptographic Feature (ICRF and ICSF)
- NetSP Secured Logon Coordinator (SLC)
- Internet Connection Secured Network Gateway (SNG)
- NetView Access Services (NVAS)
- Distributed Key Management System (DKMS)
- IBM AntiVirus Product

How This Document is Organized

This presentation guide contains half-size foils with text. The full-size foils and the Freelance source files are available on MKTTOOLS as SG244579 and available from an IBM representative. This document is organized into eleven chapters. An attempt has been made to make most of the chapters stand-alone presentations. This has caused some duplication of material but has greatly increased the usefulness of the document.

The document is organized as follows:

- Chapter 1, "Enterprise-Wide Security Architecture and Solutions"

The Introduction describes the current customer environments, top customer security concerns, security threats, customer user group security requirements, international standards activities, and the process for establishing a security policy.

- Chapter 2, "IBM Security Strategy and Architecture"

The IBM Security Architecture is based on the ISO Standards defining the basic security facilities of identification and authentication, access control, confidentiality, data integrity, non-repudiation, and security management. This chapter describes the IBM Security Architecture and its relationship to Open Blueprint, Distributed Computing Environment, SystemView, Object Oriented Security, Information Warehouse, and other international standards.

- Chapter 3, "Platform Security"

This chapter summarizes security for the MVS, VM, OS/400, AIX/6000, OS/2 and PR/SM platforms. On both MVS and VM, Resource Access Control

Facility (RACF) provides full security through the System Authorization Facility (SAF) programming interface.

- Chapter 4, “DCE Security”

This chapter describes the OSF Distributed Computing Environment structure, basic DCE security facilities such as Kerberos, and specific IBM platform and product support on MVS, AIX and OS/2.
- Chapter 5, “Application Security”

This chapter summarizes application security support in CICS, IMS, the DB2 family, DataHub, SQL, the Distributed Relational Data Architecture (DRDA), MQSeries, ACF/VTAM, NetView Access Services, and NetSP Secured Logon Coordinator.
- Chapter 6, “Cryptographic Security”

This chapter describes customer requirements for encryption, IBM’s Common Cryptographic Architecture (CCA), different cryptographic algorithms (including DES, CDMF and RSA Public Key) and IBM cryptographic products including the Integrated Cryptographic Feature (ICRF/ICSF), Transaction Security System, and Distributed Key Management System.
- Chapter 7, “Internet Security”

This chapter summarizes Internet security challenges, the World Wide Web (WWW), and solutions such as the Internet Connection Secured Network Gateway firewall, Secure Web Browsers, Secure Web Servers, and Internet Keyed Payment Protocol (iKP).
- Chapter 8, “AntiVirus Security”

This chapter defines viruses and other malicious code, anti-virus security policies, detection measures and IBM’s AntiVirus Product.
- Chapter 9, “Security Management”

This chapter summarizes the positioning of security management in the SystemView Strategy and IBM solutions such as the Distributed Security Manager (DSM) family, DataHub, SQL and the Distributed Relational Data Architecture.
- Chapter 10, “IBM Security Support and Services”

This chapter summarizes the different security publications, security education, Internet information, and security consulting services for analysis, implementation, migration, testing, emergency response team, and business recovery services.
- Chapter 11, “Summary”

The Summary shows how the set of IBM architectures, strategies, products, solutions, and consulting services addresses the key customer concerns in today’s complex multi-vendor, open, client/server, distributed computing environment.

How to Select which Foils to Use

This book contains many foils covering a multitude of security subjects, in order to cover many of the most common customer security concerns. Normally only a subset of the entire set of foils should be used for the typical marketing session.

The typical presentation should include:

- Most of the Introduction foils
- Most of the Security Architecture foils
- Most of the Related Strategy foils
- One of each of the Security Product foils depending on the customer: RACF, DSM, NetSP SLC, and Internet Connection SNG
- Some of the Encryption foils depending on the customer: Common Cryptographic Architecture, ICRF, ICSF, Transaction Security System, DKMS
- Some of the Internet foils depending on the customer: threats overview, internet overview, firewalls, and anti-virus support
- IBM Services Support and Summary foil

Depending on the specific customer environment and customer concerns, and the amount of presentation time scheduled, the marketing team can also select foils from the appropriate detailed security sections on Platform Security, DCE Security, Application Security, Cryptographic Security, Internet Security, AntiVirus Security, and Security Management.

Security Related Information on the World Wide Web (WWW)

IBM has an I/T Security Home Page, located at

<http://www.ibm.com/Security>.

The home page provides a range of valuable information services on I/T security, including offerings on protecting the enterprise, news on security issues, information on computer viruses, and more. There are also additional home pages sponsored by individual IBM product divisions regarding specific security products.

Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this document.

- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC28-8135
- *Security in the Open Blueprint*, from the IBM Open Blueprint Reference Library (SBOF-8702)
- *MVS/ESA Planning: B1 Security*, GC28-1440
- *MVS Planning: Security*, GC28-1439
- *RACF General Information*, GC23-3723
- *RACF Planning: Installation and Migration*, GC23-3736

- *RACF System Programmer's Guide*, SC23-3725
- *RACF Security Administrator's Guide*, SC23-3726
- *System Programming Library RACF*, SC28-1343
- *CICS/ESA CICS-RACF Security Guide Version 4 Release 1*, SC33-1185
- *AS/400 Security - Basic*, SC41-3301
- *AS/400 Security - Reference*, SC41-3302
- *Guide to Enabling C2 Security*, SC41-0103
- *Distributed Security Manager for AIX, General Information*, GH12-6216
- *Distributed Security Manager for MVS, General Information*, GC28-1511
- *Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference*, SC40-1675
- *Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference - Public Key Algorithm*, SC40-1676
- *Network Security Program Product Guide*, SC31-6500
- *Internet Connection Secured Network Gateway for AIX: Installation, Configuration, and Administration Guide*, SC31-8113
- *IBM TCP/IP V2 R2.1 for MVS: Planning and Customization* SC31-6085
- *Distributed Relational Database Architecture Reference*, SC26-4651
- *DataHub General Information*, GC26-4874
- *DataHub User's Guide*, SC26-3045
- *DataHub Installation and Administration Guide*, SC26-3043
- *IBM SQL Reference*, SC26-3255

International Technical Support Organization Publications

- *ITSC The Library for Systems Solutions: Security Reference*, GG24-4106
- *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200
- *IBM Distributed Key Management System, Installation and Implementation Guide*, GG24-4406
- *IBM Transaction Security System Concepts and Guidelines - Workstation*, GG24-3590
- *IBM Transaction Security System 4753/MVS Installation and Session Level Encryption Guidelines*, GG24-3591

A complete list of International Technical Support Organization publications, known as redbooks, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, SG24-3070.

To get a catalog of ITSO redbooks, VNET users may type:

```
TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
```

A listing of all redbooks, sorted by category, may also be found on MKTTOOLS as ITSOCAT TXT. This package is updated monthly.

How to Order ITSO Redbooks

IBM employees in the USA may order ITSO books and CD-ROMs using PUBORDER. Customers in the USA may order by calling 1-800-879-2755 or by faxing 1-800-284-4721. Visa and Master Cards are accepted. Outside the USA, customers should contact their local IBM office. Guidance may be obtained by sending a PROFS note to BOOKSHOP at DKIBMVM1 or E-mail to bookshop@dk.ibm.com.

Customers may order hardcopy ITSO books individually or in customized sets, called BOFs, which relate to specific functions of interest. IBM employees and customers may also order ITSO books in online format on CD-ROM collections, which contain redbooks on a variety of products.

ITSO Redbooks on the World Wide Web (WWW)

Internet users may find information about redbooks on the ITSO World Wide Web home page. To access the ITSO Web pages, point your Web browser (such as WebExplorer from the OS/2 3.0 Warp BonusPak) to the following:

<http://www.redbooks.ibm.com/redbooks>

IBM employees may access LIST3820s of redbooks as well. Point your web browser to the IBM Redbooks home page:

<http://w3.itsc.pok.ibm.com/redbooks/redbooks.html>

Acknowledgments

This publication is the result of a residency conducted at the International Technical Support Organization, Poughkeepsie Center.

This project was designed and managed by:

Cees Kingma
International Technical Support Organization, Poughkeepsie, N.Y.

Anne Lescher
S/390 Division, Poughkeepsie, N.Y.

Curt Symes
S/390 Division, Poughkeepsie, N.Y.

The authors of this document are:

Ian Allison
IBM Australia

Bernhard Buehler
IBM Germany

Riccardo Carletti
IBM Italy

Christof Lauck
IBM Germany

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Peter Callaway
IBM Security Architecture, Standards, and Strategy

Sandy Coats Campbell
IBM NetSP

Alan Fedeli
IBM AntiVirus

Art Gilbert
IBM Consulting Group

Rich Guski
IBM RACF Design

Dave Hemsath
IBM MVS DCE Development

Chris Holloway
IBM UK

Armin Hummel
IBM DSM AIX Support

Don Johnson
IBM Cryptographic Competency Center

Stuart Jones
IBM UK MQSeries

Lori Kikuchi
IBM SMPO RACF Conversion

Salvatore la Pietra
IBM AIX EMEA Security Center of Competence

Jeri Lesser
IBM Cryptographic Solutions

Susan Meyer
IBM Security and Smart Card

Terry Schwartz
IBM DSM Design

Peter Thull
IBM SMPO Security

Kathy Troidle
IBM RACF Marketing

Nev Zunic
IBM Cryptographic Solutions

Notices

The following statements are provided by the Open Software Foundation.

The information contained within this document is subject to change without notice.

OSF MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

OSF shall not be liable for errors contained herein, or for any direct or indirect, incidental, special or consequential damages in connection with the furnishing, performance, or use of this material.

Copyright © 1993 Open Software Foundation, Inc.

This documentation and the software to which it relates are derived in part from materials supplied by the following:

- © Copyright 1990, 1991 Digital Equipment Corporation
- © Copyright 1990, 1991 Hewlett-Packard Company
- © Copyright 1989, 1990, 1991 Transarc Corporation
- © Copyright 1990, 1991 Siemens Nixdorf Informationssysteme AG
- © Copyright 1990, 1991 International Business Machines Corporation
- © Copyright 1988, 1989 Massachusetts Institute of Technology
- © Copyright 1988, 1989 The Regents of the University of California

All Rights Reserved Printed in the U.S.A.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED HEREIN ARE FURNISHED UNDER A LICENSE, AND MAY BE USED AND COPIED ONLY IN ACCORDANCE WITH THE TERMS OF SUCH LICENSE AND WITH THE INCLUSION OF THE ABOVE COPYRIGHT NOTICE. TITLE TO AND OWNERSHIP OF THE DOCUMENT AND SOFTWARE REMAIN WITH OSF OR ITS LICENSORS.

FOR U.S. GOVERNMENT CUSTOMERS REGARDING THIS DOCUMENTATION AND THE ASSOCIATED SOFTWARE

These notices shall be marked on any reproduction of this data, in whole or in part.

NOTICE: Notwithstanding any other lease or license that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Section 52.227-19 of the FARS Computer Software-Restricted Rights clause.

RESTRICTED RIGHTS NOTICE: Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013.

RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the Government is subject to restrictions as set forth in paragraph (b)(3)(B) of the rights in Technical Data and Computer Software clause in DAR 7-104.9(a). This computer software is submitted with "restricted rights." Use, duplication or disclosure is subject to the restrictions as set forth in NASA FAR SUP

18-52.227-79 (April 1985) "Commercial Computer Software-Restricted Rights (April 1985)." If the contract contains the Clause at 18-52.227-74 "Rights in Data General" then the "Alternate III" clause applies.

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract.

Unpublished - All rights reserved under the Copyright Laws of the United States.

This notice shall be marked on any reproduction of this data, in whole or in part.

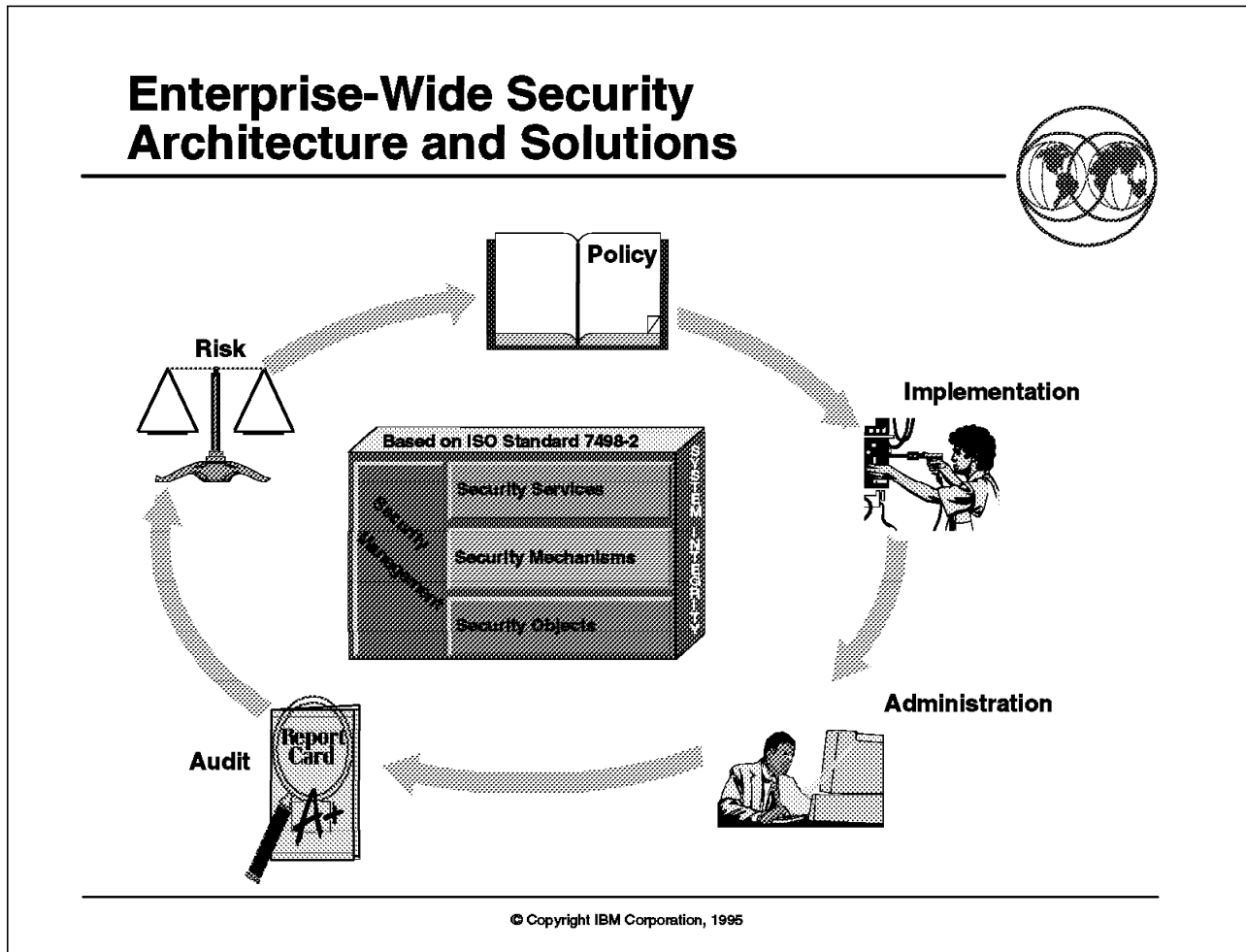
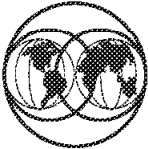


Figure 1. Enterprise-Wide Security Architecture and Solutions

1.1 Customer Testimonials

Customer Testimonials



- "By building on the ISO 7498-2 Security Standard, the IBM Security Architecture and Products should be open, enabling interoperability across heterogeneous environments."
 - ▶ William Malik, Research Director from the Gartner Group
- "The Guide Security Architecture project uses the IBM Security Architecture as the basis for its planning for effective enterprise-wide security across diverse hardware software platforms."
 - ▶ Louis Ferretti, Guide User Group Security Advocate
- Duke Power Co. in Charlotte, N.C., uses IBM's AntiVirus product on 8,000 PCs and will soon buy licenses for all 14,000 of the company's machines ... "The Internet is not a safe playground."
 - ▶ Jim Appleyard, SHARE Security Chairperson

© Copyright IBM Corporation, 1995

Figure 2. Customer Testimonials

Key Points

Consultants, user groups and customers use IBM's Security Architecture as the basis for their security policy, planning and implementation.

Presentation Script

Customer testimonials as well as customer feedback to IBM is key, as this positions IBM to focus on the real customer security issues/challenges of the ever evolving computing environment.

Open standards and criteria are becoming more important to our customers who are participating in the information highway and in the multi-vendor, open, client/server, distributed computing environment.

1.2 Current Environment

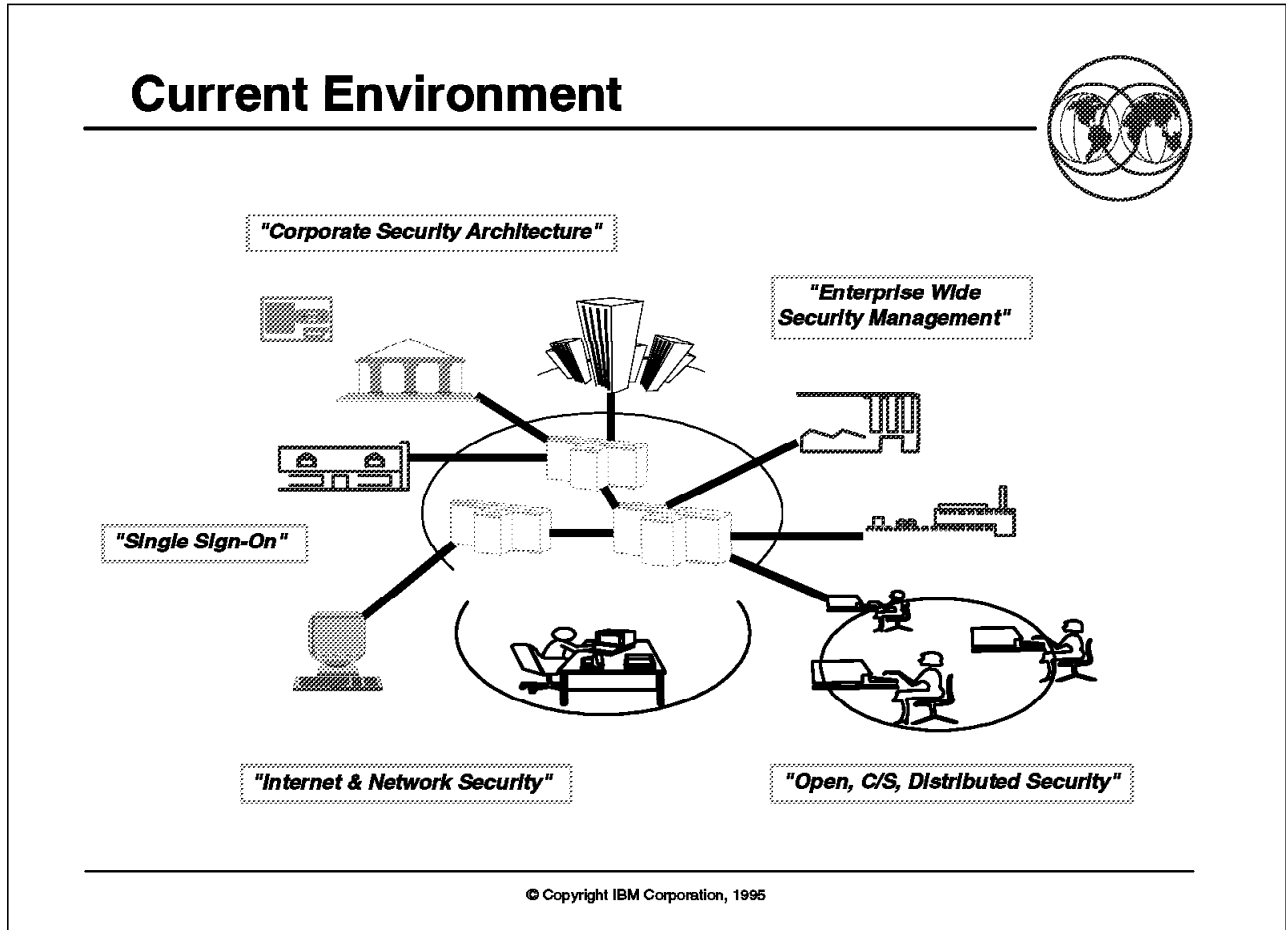


Figure 3. Current Environment

Key Points

Current customer environments require consistent security solutions for their multi-vendor, open, client/server distributed computing environment, and Internet/network communications.

Presentation Script

Information processing has undergone rapid and significant change in the last several years. This change has caused a corresponding increase in concern for the security of information assets. In the past, most businesses and other organizations have found that the security functions delivered in IBM products, working in conjunction with their policies, procedures, and administrative processes, have been adequate for the centralized configurations for which they were designed. However, these configurations have changed significantly as I/S organizations have moved toward networking, open, client/server, distributed computing structures. As a result, the security products and tools have to make similar changes to provide sufficient security in the new enterprise structures.

In particular, several environmental and technological changes have impacted management's ability to continue to exercise control over the totality of information resources. These changes include:

- The exploitation of programmable and portable workstations
- The installation of local area networks and departmental systems
- The increased use of public and private networks for interconnection of systems and organizations
- The increased use of new communication technology, such as satellite and mobile/wireless communication
- The increased connection to public networks, such as the Internet and the future Information Highway
- The interconnection of heterogeneous vendor equipment in new enterprise configurations
- The distribution of processing to uncontrolled and autonomous environments
- The general increase in the number of systems in an organization
- The growth of new application technologies, such as object oriented, multimedia, and image processing

Some of these changes have been addressed successfully by utilizing new or enhanced security functions as they have become available. In other cases, security has not kept up due to the lack of attention given to updating processes and procedures, including the definition of new policies as needed. The introduction of industry standards, the move toward heterogeneous environments, and the corresponding necessity for a consistent level of function, have created the need for a common approach to security facilities across all systems.

Increased use of local area networks (LANs) and public or private wide-area networks (WANs) for interconnecting programmable workstations, non-programmable terminals, and hosts in various enterprise configurations has presented a significant security challenge for both system designers and systems administrators. Potentially complete user control over programmable workstations and network traffic and autonomous use of various distributed-system components both intensified existent security threats and introduced new ones.

The spread of malicious software and code (viruses, worms, and Trojan horses) into workstation, network, and host processing environments has had a tremendous impact on executives' focus on the protection of information resources. The solution to these problems involves both management and technical solutions. This architecture helps to provide a framework for developing the technical solutions. IBM will continue to provide guidance for management solutions through education offerings, seminars, publications, and other consulting offerings.

The security challenge posed by distributed systems is amplified by requirements of:

- Scalability of systems
- Interoperability of IBM and non-IBM systems
- Use of both trusted and untrusted system components (for example, network components, workstations, and terminals)
- Support of multiple security-hardware technologies (for example, smart cards, cryptographic devices, and so forth)

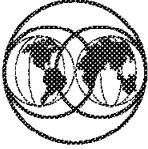
These requirements imply that large numbers of component systems may be interconnected, even though they each may support potentially divergent system security policies. These component systems typically are administered independently from one another. This makes it difficult to determine what global system security policies can, or cannot, be supported. In trying to alleviate the complexity of determining what global system security policies can be supported, additional challenges of integrating new security functions and mechanisms into existent systems and products have been created.

To address the security challenges in a systematic way, we need to define precisely (1) requirements that delimit the types of security designs that systems need to support, and (2) a basic structure that allows us to determine whether the security requirements are satisfied.

The IBM Security Architecture attempts to address these challenges.

1.3 Security is a Serious Customer Problem

Security is a Serious Customer Problem



Wall Street Journal (6/7/93):

- \$864M loss due to credit card fraud last year

Computer Emergency Response Team:

- 5-7 incidents/day involving 5-6 users
- One incident involved about 62,000 users (Internet)

Every night \$30 Trillion transferred between banks & Institutions

Computerworld
August 11, 1993
Communications Fraud Control Association:
Last year loss due to unauthorized access to computer & telephones estimated to exceed \$500M in U.S.; \$2B Worldwide

58% customer want cross-platform security products

43% customers want Single Sign On Network Access Devices

Survey Finds Losses Linked to lax Computer Security

*More than half of the companies in a new US survey say they have had financial losses due to lax computer security.

The new study, based on interviews Street & Young conducted with 1,237 companies of various sizes, found that more than half admitted to having sustained losses, amounting of more than 7 million dollars, due to security problems.

WSJ 22.11.94 p.4

We are at risk... To date we have been remarkably lucky...

From "Computers At Risk" by Dr. David Clark.

© Copyright IBM Corporation, 1995

Figure 4. Security is a Serious Customer Problem

Key Points

Increases in security incidents, make security a key customer concern.

Presentation Script

Organizations today cannot afford the loss of, or damage to, their information resources. Many organizations today exist in an environment of multiple systems with remote users and inter-organizational computing. The exploitation of satellite and mobile/wireless communication technology are adding new complexities to security solutions. Portable laptop systems are becoming more common and encourage mobile end user exploitation. Information resources are increasingly being made more available. Application technology is evolving in new directions with image processing, multimedia capabilities, and object oriented solutions.

Examples of these technology directions are evident in all industries; for example:

- Companies market products on the Internet.
- Banks share automated teller machine networks.

- Corporate executives travel with laptop PCs and log on from hotel rooms.
- Manufacturing firms have electronic data interchange arrangements with suppliers and customers.
- Doctors and health services agencies have electronic connections to laboratories and diagnostic specialists.

Establishing effective security policy and measures in this new environment becomes an exceedingly complex customer challenge. As technologies continue to evolve, the security requirements are essentially the same, but the security risks increase significantly.

1.4 Threats in Today's Electronic World

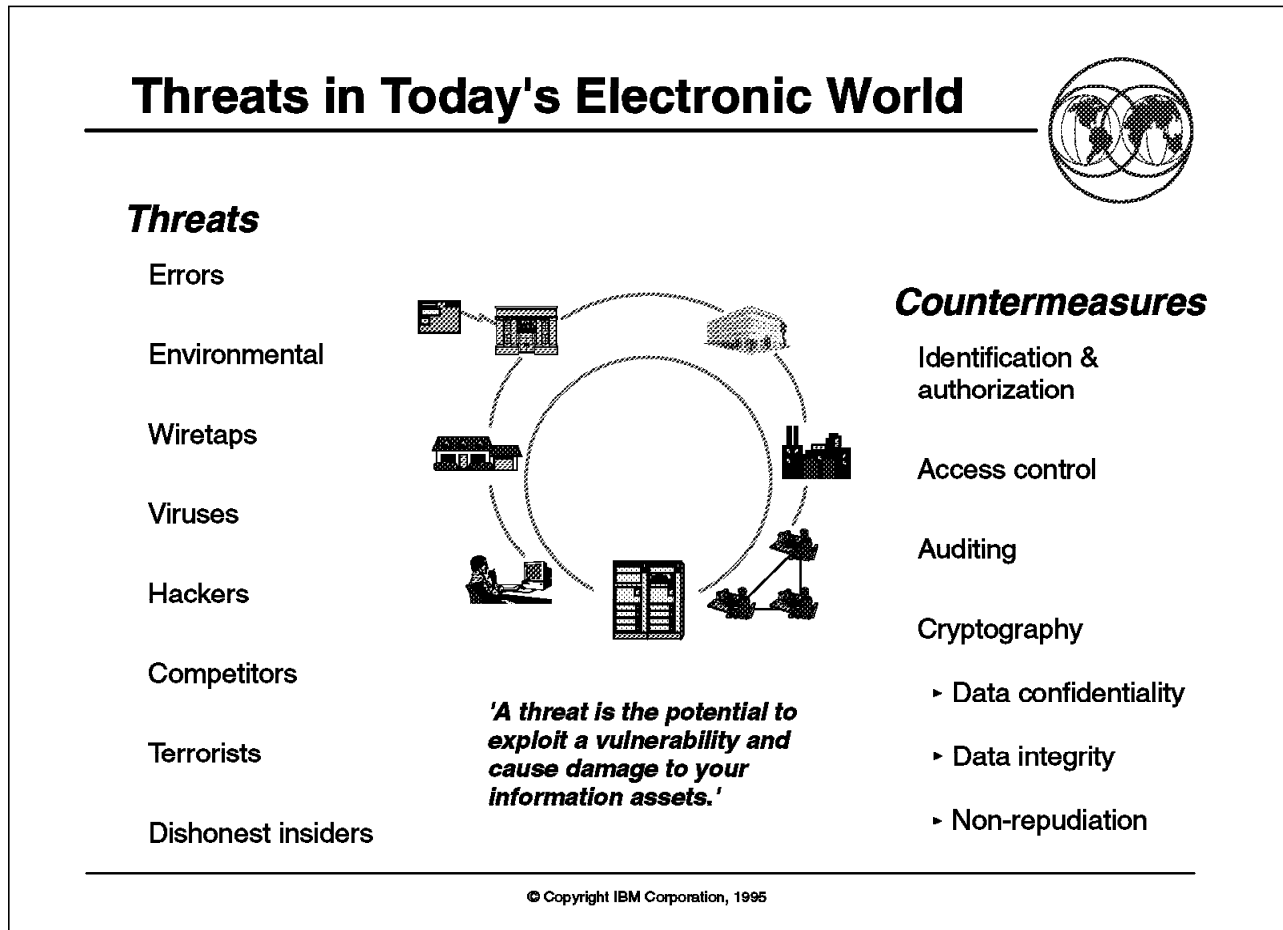


Figure 5. Threats in Today's Electronic World

Key Points

Secure countermeasures can decrease the likelihood of threats in today's electronic world.

Presentation Script

The threats that exist in a centralized environment are well recognized. For the purposes of this discussion, a threat is defined as the potential for exploitation of an exposure resulting in the unauthorized disclosure, modification, or destruction of information contained within a computer system.

As the environments for information systems change, going from the strictly centralized to the fully distributed, the nature of the threats that must be guarded against also change. The security threats of distributed systems can be thought of as (1) threats that exist in centralized systems but are amplified by distributed systems, and (2) threats that are specific to distributed systems and do not appear in centralized systems. The distinction between these two classes of threats is valuable for two reasons. First, it helps demonstrate that only a subset of the security policies and services used in centralized systems to counter existing threats apply to distributed systems for countering the same class of threats. Thus, some existent security policies and services need to be redefined

for use in distributed systems. Second, it helps focus on the definition of new policies and services meant to counter new threats not addressed by centralized systems that appear in distributed systems.

1.5 Leading User Group Requirements

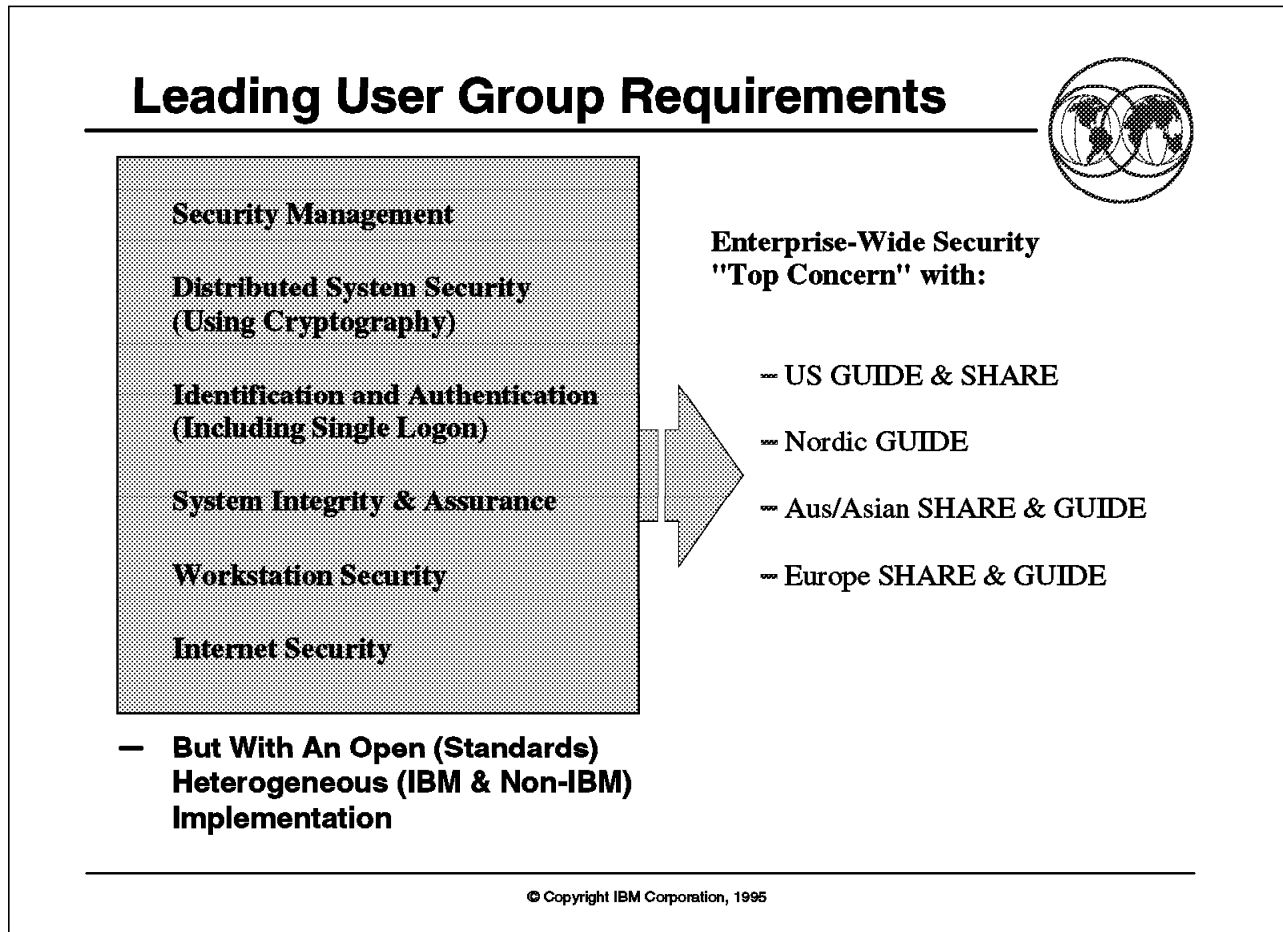


Figure 6. Leading User Group Requirements

Key Points

Customer user groups such as SHARE and GUIDE have ranked security high in their top concerns.

Presentation Script

In the last several years, both GUIDE and SHARE have been very active in the presentation of position papers outlining their security needs. Originally in November 1984, SHARE issued the Security Requirements for IBM Developed Program Products white paper, which was responded to by IBM in March 1986. Then in 1989, GUIDE issued the Information Security Architecture paper, which IBM responded to in the spring of 1990.

These papers focus on the need for a security architecture to provide coordinated and compatible security functions across product lines. The papers note that the architecture should be applicable for single system image systems, distributed systems, and peer connected systems. The architecture adopted by IBM, and described in this document, addresses the major points presented in these original white papers.

In both cases, IBM urged customers to develop additional detailed papers on specific security subjects of concern and/or product level requirements based on the architecture. As a result:

- SHARE issued the Information Architecture Relational Data Base Security White Paper in 1993.
- GUIDE issued the Architectural Requirements for an Automated Administration Tool in 1994.
- SHARE is currently drafting a Security Audit White Paper to address centralized audit requirements in a distributed environment.

The need for an open security architecture was also echoed by a set of international customers who participated in the IBM Security Customer Advisory Council from 1989 through 1991. As part of the response from the initial meeting, they voiced a need to be compliant with existing and emerging standards. The IBM Security Architecture addresses this need.

1.6 Strategic Security Drivers

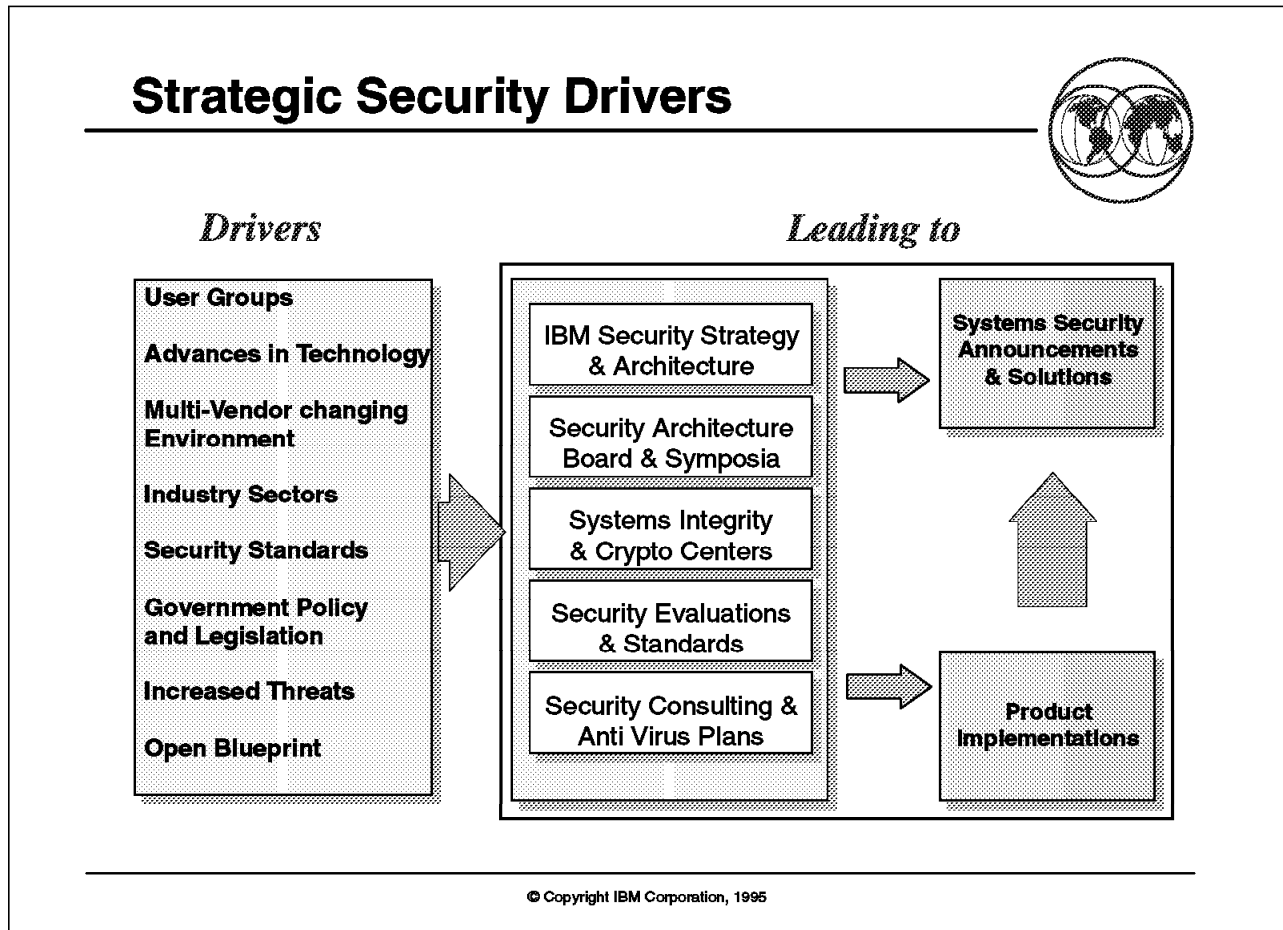


Figure 7. Strategic Security Drivers

Key Points

Security requirements “drive” the IBM security strategy, architecture, standards activities and competency centers to deliver security products and solutions.

Presentation Script

The requirements that drive the security strategy and architecture have come from a number of different customer group, vendor consortia, and international standards sources. This section presents a view of the requirements from the major sources. Detailed product requirements that helped shape the strategy may be found in the appropriate product literature, and are not presented here. This section is intended to provide a brief survey of the direct and indirect drivers that justify the security structure.

Increased Threats: The threats that exist in a centralized environment are well recognized. For the purposes of this discussion, a threat is defined as the potential for exploitation of an exposure resulting in the unauthorized disclosure, modification, or destruction of information contained within a computer system.

As the environments for information systems change, going from the strictly centralized to the fully distributed, the nature of the threats that must be guarded

against also change. The security threats of distributed systems can be thought of as (1) threats that exist in centralized systems but are amplified by distributed systems, and (2) threats that are specific to distributed systems and do not appear in centralized systems. The distinction between these two classes of threats is valuable for two reasons. First, it helps demonstrate that only a subset of the security policies and services used in centralized systems to counter existing threats apply to distributed systems for countering the same class of threats. Thus, some existent security policies and services need to be redefined for use in distributed systems. Second, it helps focus on the definition of new policies and services meant to counter new threats not addressed by centralized systems which appear in distributed systems.

Multi-Vendor Changing Environment: The majority of organizations today have multi-vendor computing environments. In the past, they may have operated them as autonomous domains with little interoperability. Recent networking solutions have provided the base for communications interoperability, and common applications have allowed for increased processing interoperability. Users have come to expect a high level of security in their systems, and these same users now require security for interconnected systems.

Interoperability with other vendors' security services is addressed by the services presented in this architecture. Product implementations in today's environment do not provide for total interoperability for the following reasons:

1. The lack of a single standard for security that all vendors could agree with and conform to
2. The prohibitive cost that would be incurred by any single vendor trying to support every operating system solution

IBM's strategy is to participate in the standards process to help drive to an open systems standard that all vendors could use, and to evolve the strategic security mechanisms to ensure conformance to that standard.

The security services discussed here do provide a high level of interoperability. First, there are industry standards that are endorsed by this strategy, such as ISO 7498-2 Security Architecture and the ANSI/ISO cryptographic standards. Second, there are existing IBM security standards that are endorsed by this strategy (LU6.2 security) and implemented by a number of other vendors. The strategy for security management also supports the ability to manage multi-vendor systems.

Advances In Technology: Evolution of the computing environment, from centralized operations centers to the emerging world of fully distributed capabilities, has changed the requirements significantly for how security is to be provided and delivered. Increasing the complexity from single systems to LAN/WAN configurations; using concentrators, routers, and various client/server scenarios; and the increasing power and capability of the workstation have all increased the need for an overall security structure that can span the technological advances taking place.

Security Standards: An attempt has been made to incorporate the various security standards efforts into the strategy. However, most of the standards work has yet to mature. Given customer concern with providing security in mixed (multi-vendor) environments, it is important that products conform to open systems standards for security functions. Because there are multiple standards bodies at work defining different facets of security, IBM will encourage, through

active participation, convergence to a single set of coherent standards. IBM has a continuing involvement with ISO, Open Systems Foundation (OSF) and X/Open.

ISO is guiding many efforts to define the protocols that support the security architecture. A set of standards is being developed in various ISO work groups that address upper and lower layer models, OSI security management framework, security services framework, and OSI security services definition and protocol specification.

In addition to the ISO standards efforts, there are a number of other groups preparing security standards. Among these are:

- American National Standards Institute (ANSI)
- European Computer Manufacturers Association (ECMA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Telegraph and Telephone Consultative Committee (CCITT)
- National Institute of Standards and Technology (NIST)
- Internet Engineering Task Force (IETF)
- Open Software Foundation (OSF)
- X/Open

Government Policy and Legislation: The increasing focus of many governments, especially in Europe, on the implications of computer technology to privacy issues demands increased security to comply with various legislative actions. This demand becomes even more critical as multi-national companies implement world-wide networking of systems.

In addition to privacy issues, we have seen a much greater focus on security issues in general.

The National Security Agency (NSA) supports an organization devoted to encouraging the development of trusted computing systems by defining a hierarchical arrangement of security functionality and architectural, documentation and testing requirements. This set of requirements is known as the Trusted Computer System Evaluation Criteria (TCSEC) or Orange Book. The NSA has a large organization supporting a process called the Trusted Product Evaluation Process (TPEP), to perform evaluations of systems, subsystems and products against these criteria. The products successfully evaluated against these criteria are added to the Evaluated Products List (EPL), which is used as a reference list for the Department of Defense (DoD) and its contractors.

Additionally, there are criteria documents that have been or are currently being developed by individual country government organizations. Since the NSA will only perform evaluations in the U.S., the European Community has sponsored the development of their own evaluation criteria known as the Information Technology Security Evaluation Criteria (ITSEC). In the U.S., a combined effort between the NSA and NIST is attempting to expand the scope of the Orange Book to address the needs of the commercial and civil arena. This effort is known as the Federal Criteria. The initial focus of this effort is to identify a minimum set of security functions required for civil/commercial systems. This set is known as the Minimum Security Functionality Requirements (MSFR). The MSFR is expected to form the new base for the future criteria scheme for evaluating all secure systems.

Industry Sectors: Historically, several industry sectors have displayed a greater level of concern for security than most others. These sectors include the U.S. Department of Defense (DoD), the aerospace industry, and the financial services industry, including banking, insurance, and securities.

These sectors have influenced the work of many standards bodies, and continue to be heavily involved in the definition of requirements, the development of standards, and the application of standards to their own environments. Ongoing communications with these groups has helped IBM develop a comprehensive understanding of their requirements, as well as those of industry in general.

Industry concerns over the lack of harmony among various national evaluation criteria and their emphasis on the security needs of the military/intelligence communities have led to the development of sets of security requirements by commercial organizations.

In 1990 a document called the Commercial International Security Requirements (CISR) was published by Ken Cutler of The American Express Travel Related Services and Fred Jones of the Electronic Data Systems Corporation. The CISR was adopted by the International Information Integrity Institute (I-4). Somewhat in parallel, Bellcore was developing its Standard Operating Environment Security Requirements so that all system procurements could specify a consistent level of security. These two documents were used by the National Institute of Standards and Technology (NIST), along with the Orange Book functionality criteria, to produce the Minimum Security Functionality Requirements (MSFR) for commercial systems. The MSFR was to be published as a FIPS but instead became absorbed into the functionality requirements part of the Federal Criteria and subsequently the Common Criteria.

Following the publication of the MSFR, the European Computer Manufacturers Association (ECMA), derived the Commercially Oriented Functionality Class (COFC) as an ECMA Standard to be used as a sample Functionality Class for evaluations under the ITSEC.

Recently the X/Open Security Working Group has been working on the concept of extending its software branding process to perform security branding. Security branding would initially be limited to XPG3 or XPG4 compliant systems and would be based on the X/Open Baseline Security Services (XBSS) X/Open Baseline Security Services (XBSS), which is defined in the form of the functionality part of a protection profile and built from the security functionality components defined in the Federal criteria. XBSS is defined as the minimum security services needed by interconnected commercial systems. These services allow installations to run secure systems by default and implement reasonable security policies to protect their assets against minimal risks at reasonable cost. The assurance gained from an X/Open Security Branded system would be based on supplier testing and declaration of compliance with XBSS requirements, backed up by the warranty contained in the Trade Mark Licensing Agreement (TMLA) entered into with X/Open.

The X/Open Security Branding process has the potential of being much shorter and cheaper than a government-sponsored formal evaluation, yet should meet the security needs of the majority of commercial users. The European Security Forum and the I-4 are strongly supportive of the X/Open initiative and are working closely with X/Open to ensure that the effort is successful. The Preliminary Specification for XBSS underwent X/Open Company Review in April and May of 1995, and, should the X/Open business considerations be satisfied

and the Security Branding process be successfully created, trial Security Branding may begin in 1996.

IBM has played an active role in critiquing the MSFR and working with ECMA and X/Open in the creation of the COFC and the XBSS. IBM is thus well positioned to address the security needs of commercial systems through these standards, should our users express sufficient interest.

ISO 9000 Quality: The IBM Corporation recognizes the growing acceptance of ISO 9000 as a quality system standard in many countries. We believe the IBM quality system goes well beyond the ISO 9000 requirements and that the products and services with the IBM logo consistently exceed the quality levels that the ISO 9000 program will achieve. However, to satisfy the requirements of our customers, we are taking measures to formally demonstrate conformance to the ISO 9000 requirements. The ISO 9000 activities are being integrated within the framework of our Market-Driven Quality (MDQ) strategy, which represents a customer-oriented approach to total quality system management.

IBM's worldwide plants and laboratories have achieved or are undergoing assessment and registration with the objective of conforming to ISO 9000 standards.

Harmful Code/Viruses: Computer viruses have received much attention in recent years. In addition, other types of malicious software have been reported, including Trojan horses, logic bombs, and worms. These problems have affected personal computers, minicomputers, mainframes, and networks. Because they are destructive, or potentially destructive, they have served as a reminder that protection against these types of attacks is required. Traditional computer security measures are helpful, but new measures are needed to deal with the problems effectively. The computer security management of an organization plays a key role in reducing the risk, but education and ongoing participation of the users are also vital.

User Groups: Customer user groups such as SHARE and GUIDE have ranked security high in their top concerns. For further information see section 1.5, "Leading User Group Requirements" on page 10.

Open Blueprint: The Open Blueprint is a standards-based architecture that defines the services required by applications in a distributed multivendor environment. The Security Service is a key component of the Distribution Services which is based on the DCE security Standards. For further information see section 2.6.1, "IBM's Open Blueprint" on page 72.

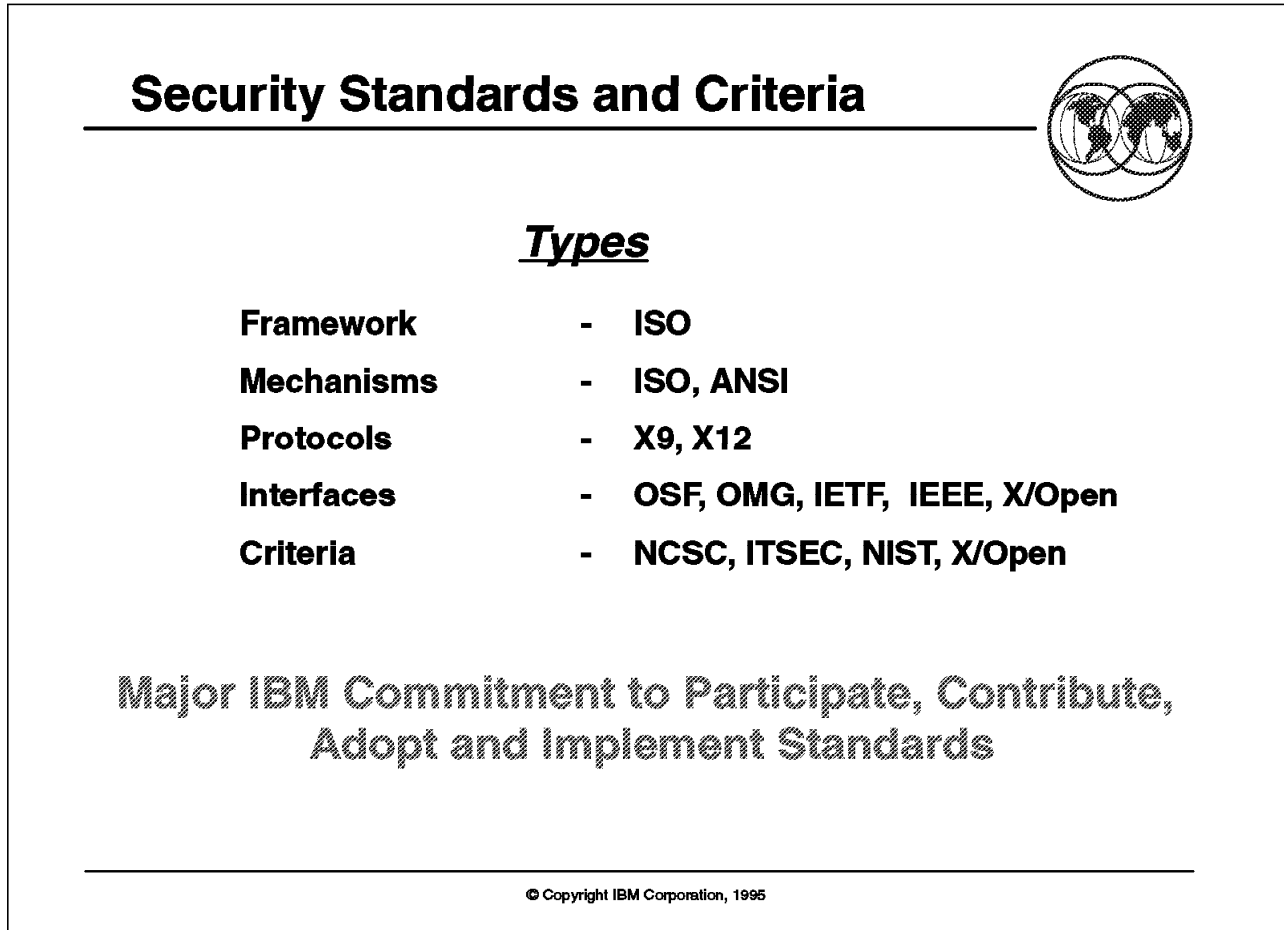


Figure 8. Security Standards and Criteria

Key Points

IBM’s participation in international consortia/groups provides the basis for the security strategy and architecture.

Presentation Script

An attempt has been made to incorporate the various security standards efforts into the strategy. However, most of the standards work has yet to mature. Given customer concern with providing security in mixed (multi-vendor) environments, it is important that products conform to open systems standards for security functions. Because there are multiple standards bodies at work defining different facets of security, IBM will encourage, through active participation, convergence to a single set of coherent standards. IBM has a continuing involvement with ISO, Open Systems Foundation (OSF) and X/Open.

ISO is guiding many efforts to define the protocols that support the security architecture. A set of standards is being developed in various ISO work groups that address upper and lower layer models, OSI security management framework, security services framework, and OSI security services definition and protocol specification.

In addition to the ISO standards efforts, there are a number of other groups preparing security standards. Among these are:

- American National Standards Institute (ANSI)
- European Computer Manufacturers Association (ECMA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Telegraph and Telephone Consultative Committee (CCITT)
- National Institute of Standards and Technology (NIST)
- Internet Engineering Task Force (IETF)
- Open Software Foundation (OSF)
- X/Open

For more information on the evaluation criteria (NCSC TCSEC and ITSEC), see section 2.6.7, “Security Evaluation Strategy” on page 88.

For more information on Standards Activities, see section 2.5, “IBM’s Ongoing Commitment” on page 64.

1.8 Responding to Customer Needs

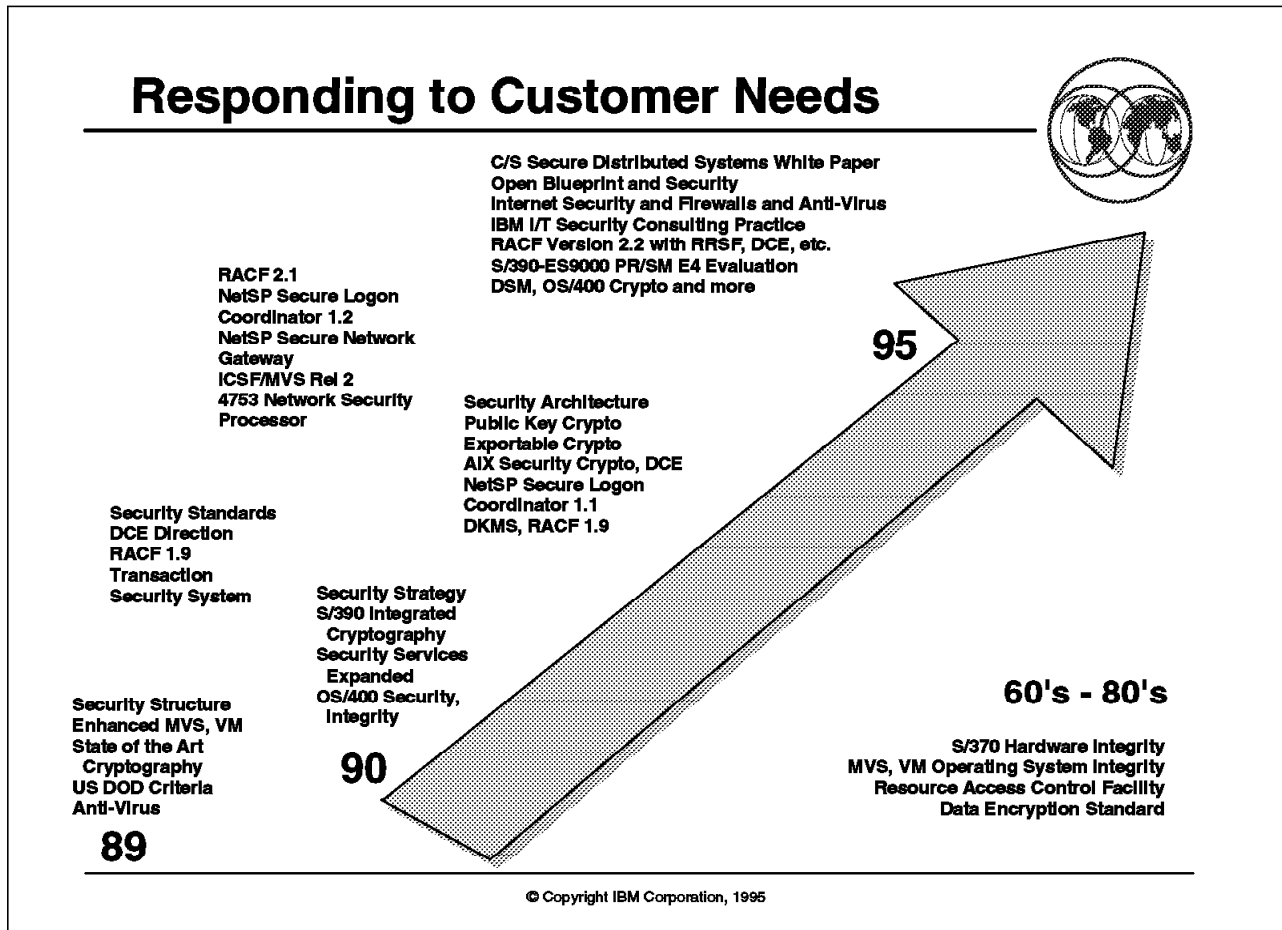


Figure 9. Responding to Customer Needs

Key Points

IBM has been and continues to be a world leader in providing security products, solutions and services.

Presentation Script

Security features have been present in IBM hardware and software products for more than two decades. During that time, there have been many firsts, including hardware integrity, the data encryption algorithm, and operating system integrity. With the announcements over the last several years, IBM has continued to re-enforce and strengthen its commitment to security and responding to customer needs.

The following list shows some of the more significant security announcements made in 1989, 1990, 1991, 1992, 1993, 1994, and early 1995:

1989

- IBM Security Structure
- Transaction Security System
- Anti-virus Measures and Tools
- Security Consulting Services

- Multi-Level Security for IBM MVS/ESA
- RACF 1.9

1990

- IBM Systems Security
- Security and SAA
- IBM Networking Overview
- NetView Access Services
- IBM Common Cryptographic Architecture
- Integrated Cryptographic Feature and Service Facility
- Secure Workstation Solutions
- Transaction Security System for OS/2
- Distributed Database Security
- Additional Anti-Virus Measures and Tools
- IBM MVS/ESA JES2 and JES3 Security System Packages
- OS/400 1.3 with System Integrity
- VM/ESA System Integrity
- IBM ES/9000 Processors

1991

- IBM Systems Security Enhancements
- Commitment to the Open Enterprise
- Secure Distributed Computing Statements of Direction
- Security Management with SystemView
- AIX/6000 3.1.5
- OS/400 2.1
- New IBM ES/9000 ICRF and PR/SM enhancements
- VM/ESA enhancements
- VTAM 3.4 for MVS Enhancements
- NetWare Network Computing Products

1992

- 8250 Multi-Protocol Intelligent Hub
- DFDSM Distributed Storage Manager for MVS and VM
- AIX/6000 DCE Security Server
- ALERT from Legent for VSE Security
- PS/2 models 56, 57, UltiMedia M57, and UltiMedia DV-M57 announce Hardware Integrity features
- New security features for Transaction Security System (TSS) including Public Key cryptographic support
- TCP/IP Version 2 Release 2 for MVS
- AIX Version 3.2.2 for RISC System/6000
- RACF Version 1.9.2 enhanced security features
- VM/ESA planned support for DoD C2 and B1
- DataHub family of products for SystemView Information Warehouse
- IBM AntiVirus for DOS, Windows and OS/2 Version 1.0 announced

1993

- IBM Network Security Program V1R1 Secured Logon Coordinator
- VM/ESA DCE Statement of Direction
- AS/400 V2 R3 Security Support “Designed to Meet”C2 with enhanced auditing, resource security and System Integrity
- IBM Network Security Processor MVS Support Program Release 2.2

- Commercial Data Masking Facility Algorithm for 4753/4755
- Distributed Key Management System
- IBM Network Signon Coordinator/2 Version 1.1
- IBM AIX Distributed Computing Environment Product Family Version 1.2
- IBM Distributed Computing Environment for OS/2 and Windows V1.0 Toolkit including security
- IBM AntiVirus for DOS, Windows and OS/2 Version 1.1, 1.2, 1.3, 1.4
- IBM AntiVirus for Netware announced

1994

- RACF Version 2 Release 1
- IBM Distributed Security Manager for MVS
- IBM MVS/ESA SP 5.1 and Open Edition Enhancements with security client support
- IBM Distributed Computing Environment Base Services/400 Version 3 security client function
- IBM OpenEdition Distributed Computing Environment for MVS/ESA application security support for CICS and IMS
- IBM OpenEdition Distributed Computing Environment for VM/ESA
- IBM Distributed Computing Environment Client for Windows Version 1.0
- IBM DCE 1.3 for AIX 3.2.5 with exportable data masking
- IBM Distributed Computing Environment Base Services/400 Version 3 with security client function
- IBM OS/2 LAN Server Version 4.0
- IBM NetSP Secured Network Gateway for Internet Firewall Security
- IBM Network Security Program V1R2 Secured Logon Coordinator
- IBM 4753 Network Security Processor Model 014
- IBM AntiVirus for DOS, Windows and OS/2 Version 1.5, 1.6, 1.7, 2.0
- IBM AntiVirus for Netware Version 1.6, 1.7, 2.0
- Integrated Cryptographic Service Facility/MVS Release 2
- DFSMS 1.2 NFS Server R3 security enhancements

1995

- RACF DCE Security Support Statement of Direction
- RACF 2.2 and the Remote Sharing Facility
- OS/400 C2 Evaluation
- PR/SM ITSEC E4 Certification
- I/T Internet Security Announcement
- Internet Connection Secured Network Gateway V2R1 announcement
- MVS/ESA 5.2.2 DCE Security Server Statement of Direction including:
 - Upgrade to OSF DCE Version 1.1 functionality
 - DCE Security Server for MVS
 - Interoperability between RACF and DCE security

For further information concerning these announcements and products, please contact your IBM marketing representative.

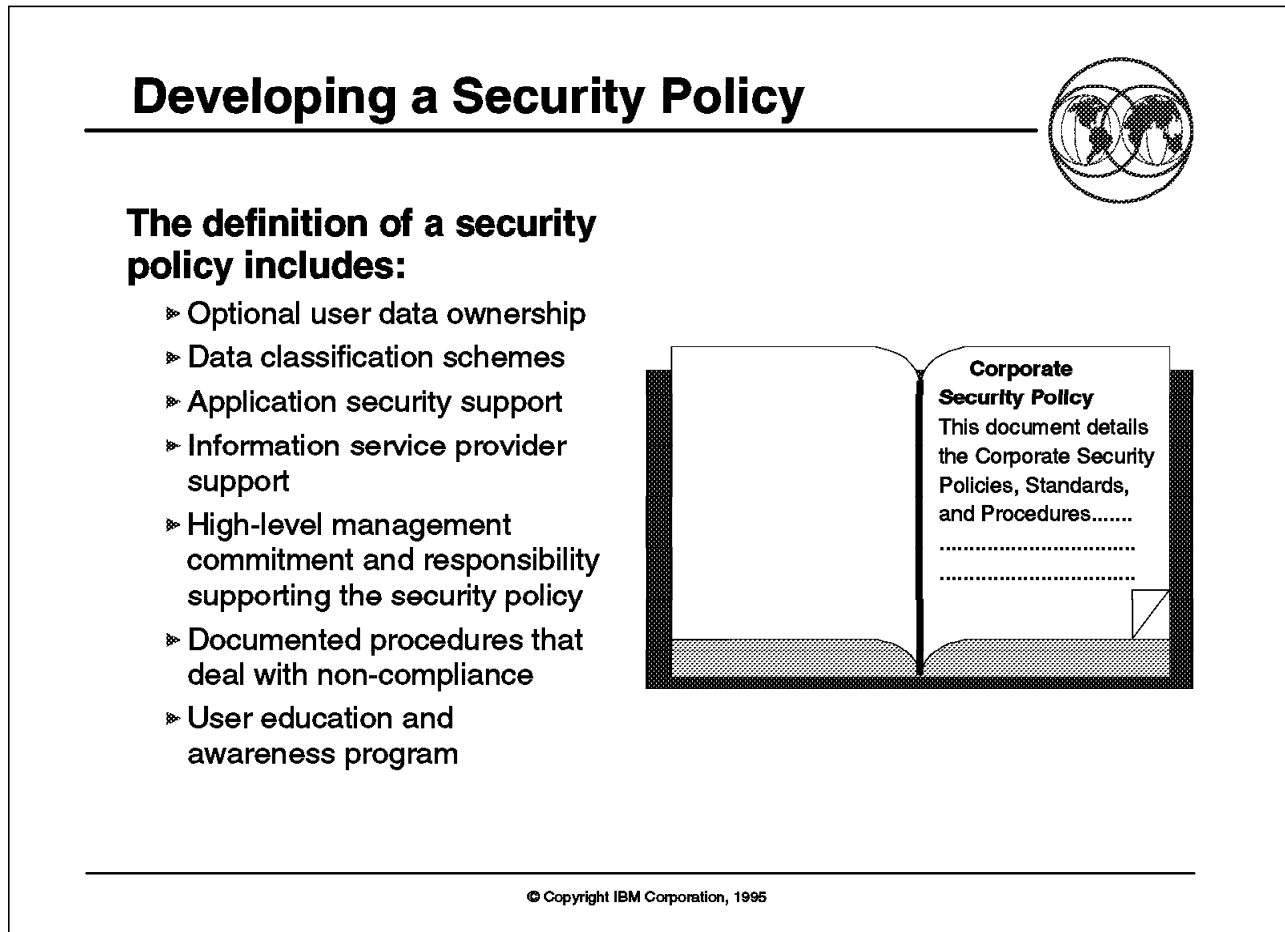


Figure 10. Developing a Security Policy

Key Points

A security policy is essential for an enterprise's implementation of effective security controls.

Presentation Script

A business must define its security needs in order to establish a management security policy and practice guidelines. The definition of a security policy includes:

- Optional user data ownership, data classification schemes, application security support, and information service provider security support, which must ultimately define the specific responsibilities for protecting the business assets
- High level management commitment and responsibility supporting the security policy
- Documented procedures that deal with non-compliance
- User education and security awareness program

1.10 The Security Process Cycle

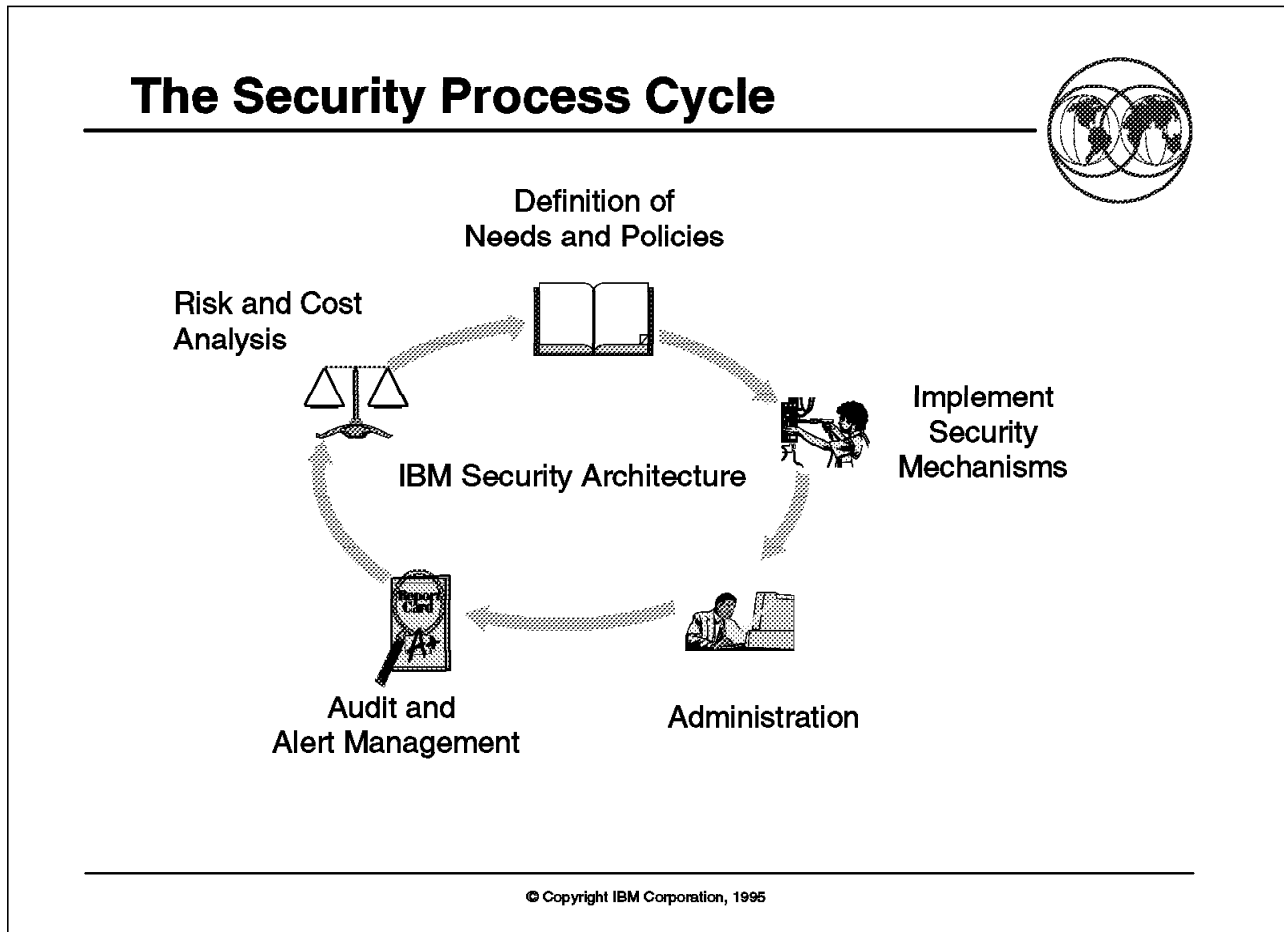


Figure 11. The Security Process Cycle

Key Points

In order to implement an effective security policy, an enterprise must establish an ongoing security process cycle of risk analysis, policy definition, implementation, administration and audit.

Presentation Script

The process of securing an information system is a cyclical, on-going effort with involvement from all levels of the corporation, from the highest level of management down to the end users and programmers. There are five primary stages in the security process cycle, as depicted in Figure 11.

- Risk Management:

Risk management is the process that studies the potential security exposures and determines an acceptable level of security controls, implementation costs, and risk acceptance for those exposures that are not fully covered. The process is much like that of insurance appraisals and insurance policies. The risk management activities include:

- Identifying security exposures such as natural disasters, external hackers, employee errors, and disgruntled employees along with the probability of occurrence

- Identifying valuable business data assets such as customer databases, research information, new product plans, and accounting data
- Quantifying the value of potential loss for each exposure and valuable business asset
- Determining the costs of implementing appropriate security controls
- Weighing the cost of controls against the potential value of a loss
- Recommending changes in the security policy and implementation
- Documenting acceptance of all risk exposures not covered by plans
- Defining Security Policy:

Discussed in section 1.9, “Developing a Security Policy” on page 22.
- Security Implementation:

Security implementation is the process of procuring, installing, and initializing the appropriate security products and system controls. The process of security implementation includes:

 - Selecting security mechanisms appropriate for the security policies
 - Installing security hardware and software products
 - Defining system security controls and options
 - Grouping users and resources for effective administration
 - Classifying data and resources
- Security Administration:

Administration is the process of applying the security policies and practices for an organization, which is largely the administration of security objects such as:

 - User IDs and passwords
 - Special system and user privileges such as administrator, auditor or operator
 - Resources such as datasets, application access, transactions, and devices
 - Encryption objects such as keys
 - Security logs
- Security Audit:

Audit is the continuous review of security controls and security events. Audit results are periodically reported to management and used as input for subsequent security process cycle efforts to update the security policy and implement new controls. Security audit can include:

 - Self testing or independent testing
 - Penetration testing
 - Internal compliance
 - External certification

Chapter 2. IBM Security Strategy and Architecture

IBM Security Strategy and Architecture

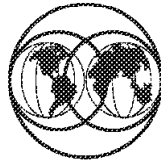


Figure 12. IBM Security Strategy and Architecture

2.1 IBM Security Strategy (Stage1)

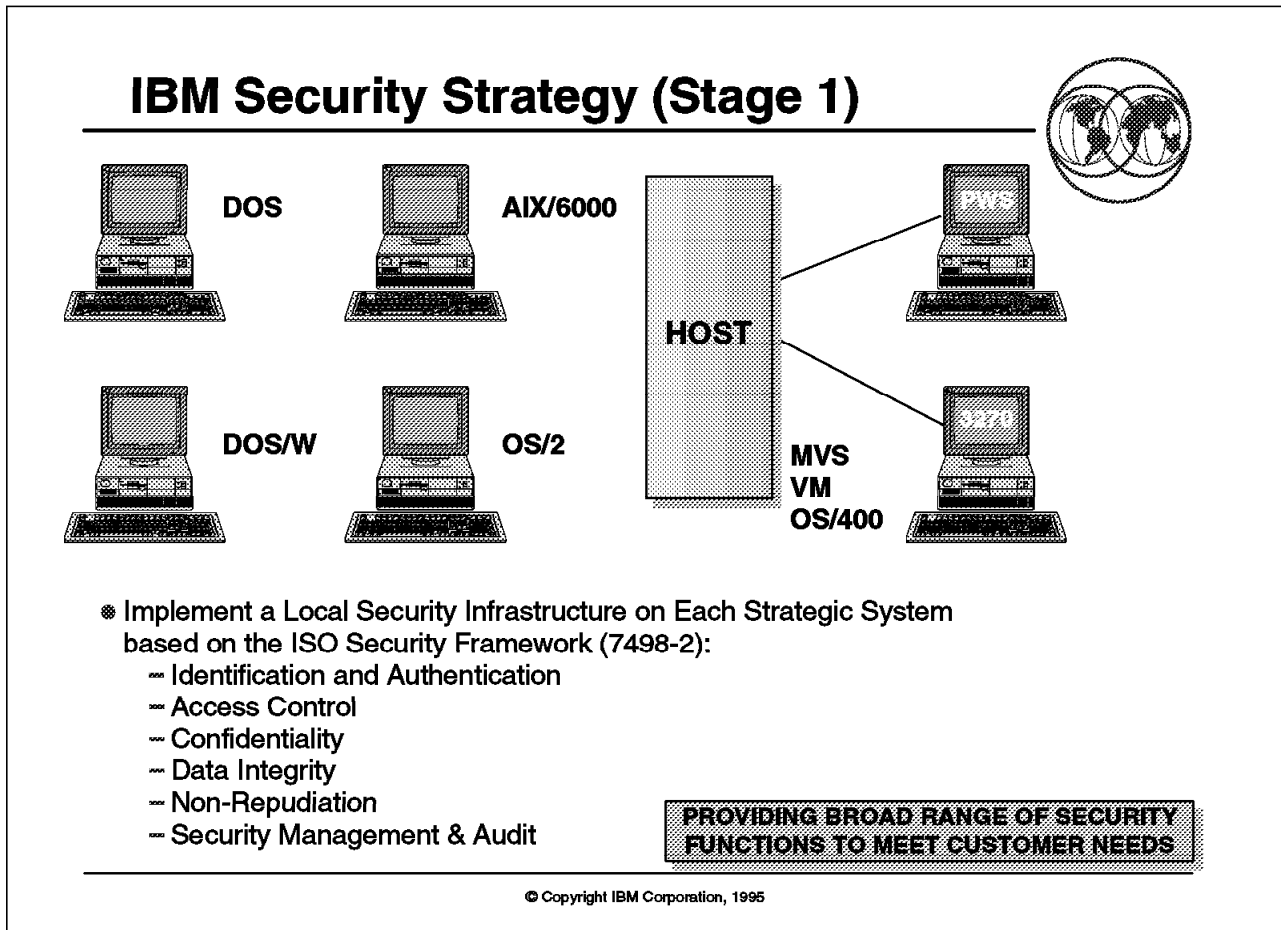


Figure 13. IBM Security Strategy (Stage1)

Key Points

Stage 1 of the IBM security strategy is to implement an infrastructure on each strategic IBM platform.

Presentation Script

The Need for a Strategy: Many factors have led to today's emerging environment of interconnected systems and distributed processing. However, in many cases, the security solutions have not kept pace with the inter-connectivity of systems. This is not simply a "product" problem. In addition to the products being used for security, organizations must develop and maintain policies, practices, and procedures for providing a secure systems environment. In the absence of these, most users have had to deal with these problems in manual ways (multiple logons, multiple copies of data, overlapping administrative tasks, and so forth). In addition, most organizations have not been able to predict how their systems would be interconnected, or what the effects of doing so would be. The security solutions that must be provided in the future need to allow for connectivity of systems in any way and still provide security without loss of administrative control or unnecessary complexity.

The security services provided by each operating system must address the requirements of those operating environments where that system might be used. In the simplest case, this will be a stand-alone environment. MVS, VM, OS/400 and AIX currently provide security solutions for the stand-alone environment.

The IBM system security structure allows for the attachment of workstations, via LAN and WAN connections, and still provides the required security services end-to-end.

The structure defined in support of this strategy provides for flexibility of use. The user and resource naming structure of the directory allows the establishment of unique names.¹ In addition, it provides the basis for allowing user authentication to be performed once for a user session and allows users to access applications in any system for which they are authorized. Data integrity and confidentiality services are enabled for use between any two points. Security management and administration are expanded to allow control and reporting across multiple systems, thus providing a single system image.

Most organizations today have systems composed of equipment from multiple vendors. The structure presented here defines those security services that are required in each system so that they are interoperable. The need for a common security structure is driven by the requirement for distributed processing across the strategic environments. Initially, the requirement was driven by an environment of interconnected MVS and VM systems, and was addressed by the introduction of RACF on VM and shared RACF databases.

As the use of personal computers became more than stand-alone personal computing, there arose the need for solutions to the security problems of cooperative processing. These problems were partially addressed by SNA security architecture extensions. SAA introduced the notions of common application programming interfaces, common user access, and common applications across MVS, VM, OS/400, OS/2, and AIX. The evolution from SAA to open distributed systems with requirements for interoperability has resulted in the need for a system structure to support distributed processing across the strategic platforms.

Organizational requirements force the need for consistency of security services across the strategic systems. In general, consistency of security means that resources are provided the same level of protection regardless of where they reside or how they are moved from system to system. For example, if a user is not allowed access to a given resource on MVS, moving that resource to OS/2 should not allow the user to access the resource in that environment. Application and resource portability requires consistency of security services. Open distributed processing likewise necessitates a level of consistency for security. This level of consistency requires that security protocols and functionality, administration, and structural elements be identical in the platforms.

¹ There are two instances of names in the open distributed system environment. The first is the externally visible (seen by humans) name. This is referred to as the user name or resource name. This name may be of variable length, thereby making it unwieldy for use internally by the security facilities. This gives rise to the second instance of a user or resource name. This internal name is referred to as the globally unique ID (GUID), which is a fixed length value. While the names are unique to ensure no security problems result from duplication, the GUID is unique in both "time and space" ensuring that no two individuals will ever be assigned the same value.

The security services include the functions described in the ISO 7498-2 guideline and are intended to conform with the emerging open systems security standards. Accordingly, the IBM strategy is to implement the ISO security protocols as they are adopted. It may also be necessary for some systems to support additional security standards, in particular, UNIX standards.

In addition to the basic services, the structure must also provide a level of assurance that the services will function as expected when invoked. There are two measurements of assurance that are addressed by the strategy. The first is the IBM definition of assurance, which is defined uniquely for each operating system and is termed system integrity. The other measurement is defined by the level of trust, which is a hierarchy of requirements designed to measure the trustworthiness of the security controls.

Distributed operation among the IBM platforms is not the only set of operating systems that must be supported. In addition, systems must be able to interoperate with non-IBM open platforms, UNIX systems, and other vendor proprietary operating systems and networks. In order to provide continued security for the strategic operating systems in these environments, there must be some way to interact with the security services in those systems. Application Programming Interfaces (APIs) will enable this to happen.

The IBM Security Strategy essentially may be divided into two different stages, Stage 1 and Stage 2.

Stage1: Implement a local security infrastructure on each strategic system based on the ISO Security Framework (7498-2):

- Identification and Authentication
- Access Control
- Confidentiality
- Data Integrity
- Non-Repudiation
- Security Management & Audit

2.2 IBM Security Strategy (Stage2)

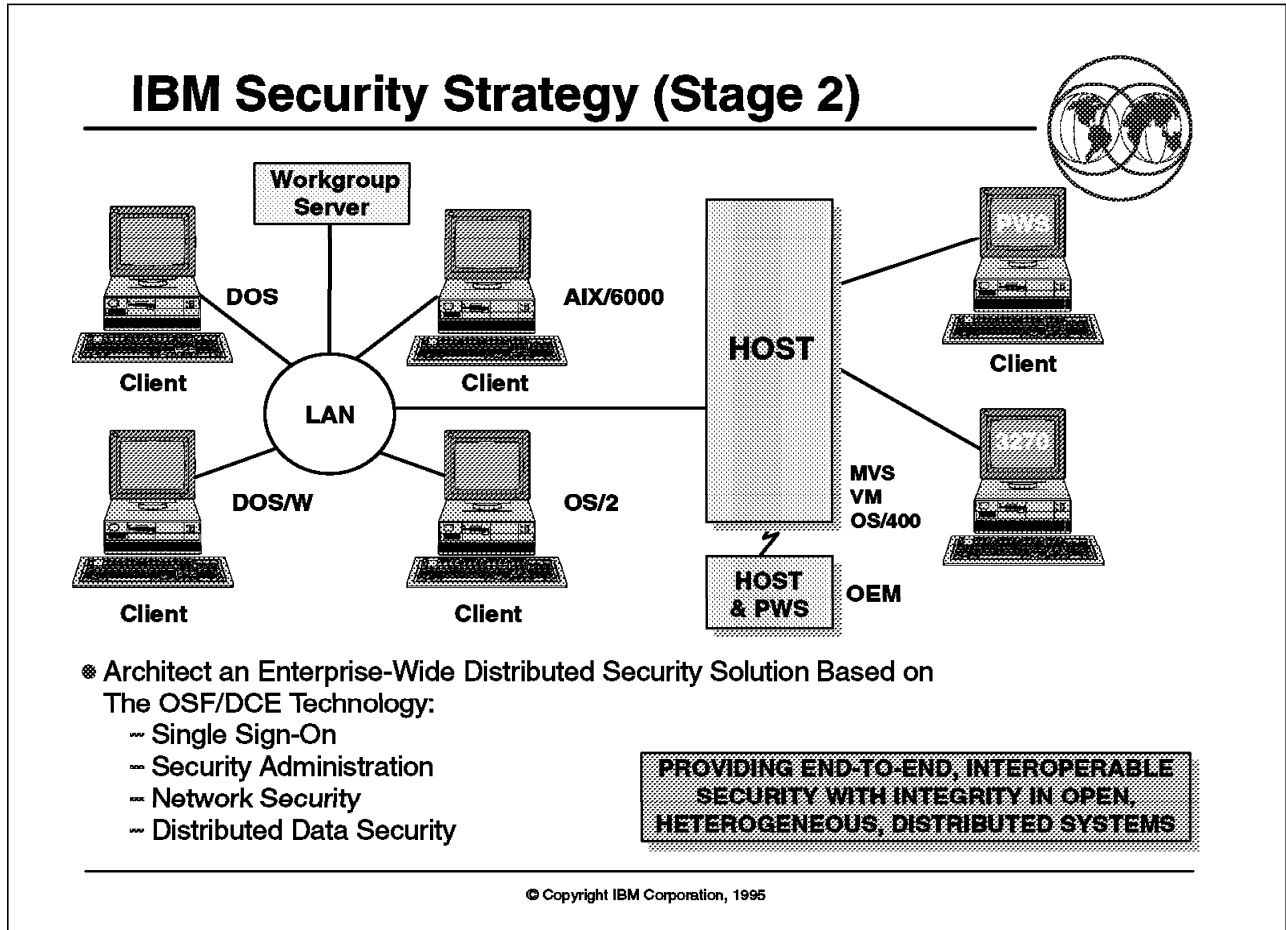


Figure 14. IBM Security Strategy (Stage2)

Key Points

Stage 2 of the IBM security strategy is to provide a broad range of security functions to meet the top customer concerns across platforms in a distributed enterprise.

Presentation Script

Stage 2: Architect an enterprise-wide distributed security solution based on the OSF/ DCE technology that addresses security support across secure system platforms to provide:

- Single sign-on within an enterprise
- Security administration across enterprise platforms
- Network security for communications
- Distributed data security

2.3 IBM Security Architecture

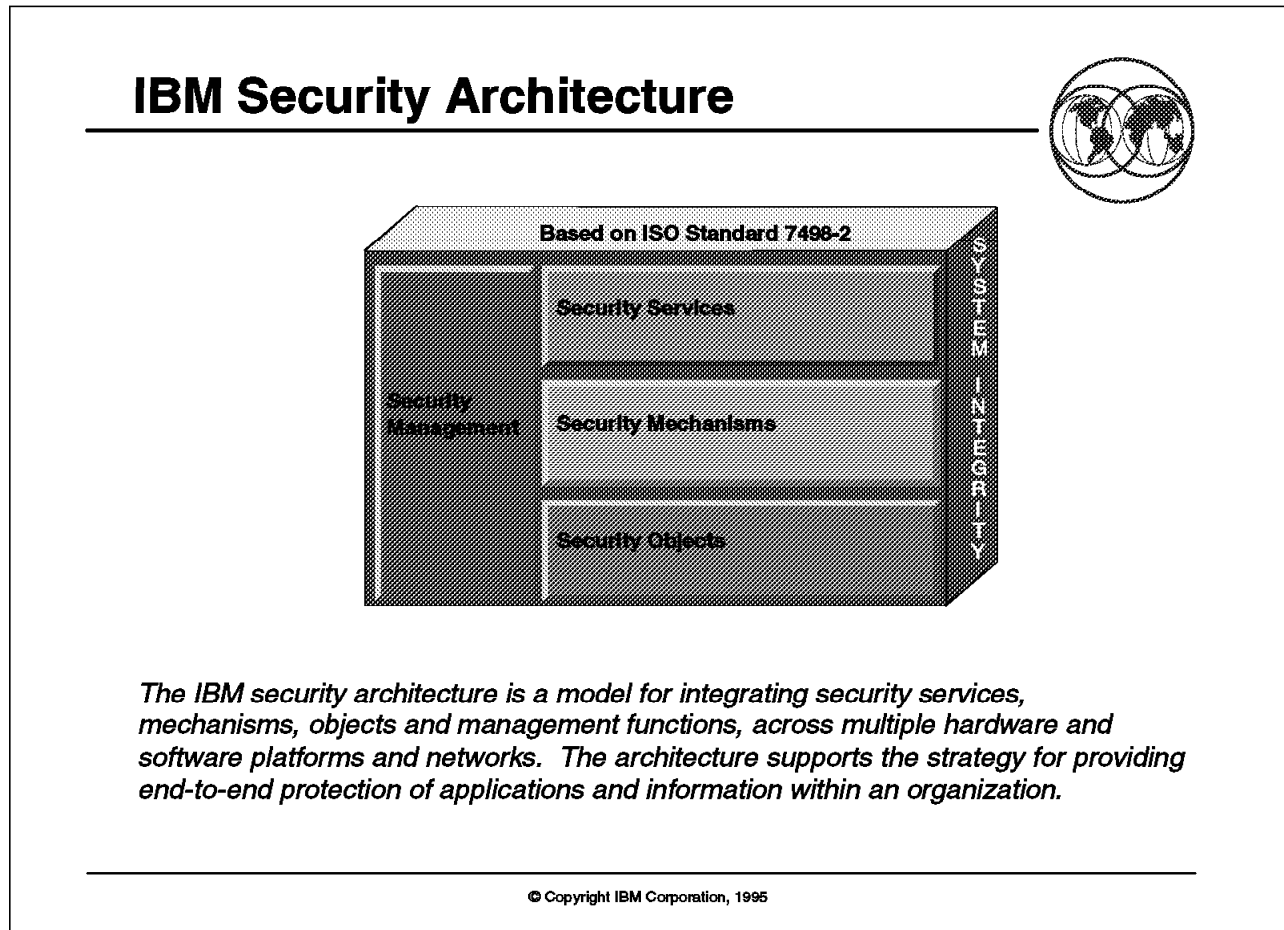


Figure 15. IBM Security Architecture

Key Points

IBM's security architecture is based on ISO Standard 7498-2 to provide consistent security services, mechanisms, objects, and security management.

Presentation Script

The IBM security architecture is a model for integrating security services, mechanisms, objects, and management functions, across multiple hardware and software platforms and networks. The architecture supports the strategy for providing end-to-end protection of applications and information within an organization.

IBM's current information security solutions are designed to protect valuable information in all of IBM's products, from workstations to mainframes. IBM maintains its leadership in security, including cryptography, anti-virus measures and the introduction of new technologies, by providing offerings that enable an organization to fully utilize its information and processing resources in a secure fashion. IBM recognizes the need for an overall security framework to support open systems standards that address the needs of a multi-vendor environment. Standards are viewed as critical to achieving openness, and thereby allowing participation in a multi-vendor environment. IBM will continue to evaluate and

possibly select recognized international standards in order to help support an open heterogeneous environment that has consistent security services available.

As stated, the objective of this architecture is to graphically describe the framework and boundaries that define the IBM total solution for system security. It is a framework for implementing available security services, as well as for planning for changes expected in the future. By using this framework to reduce complexity of security implementations and provide consistency across system platforms, an organization will be able to maintain security as the environment continues to evolve.

2.3.1 System Integrity, Assurance and Trust

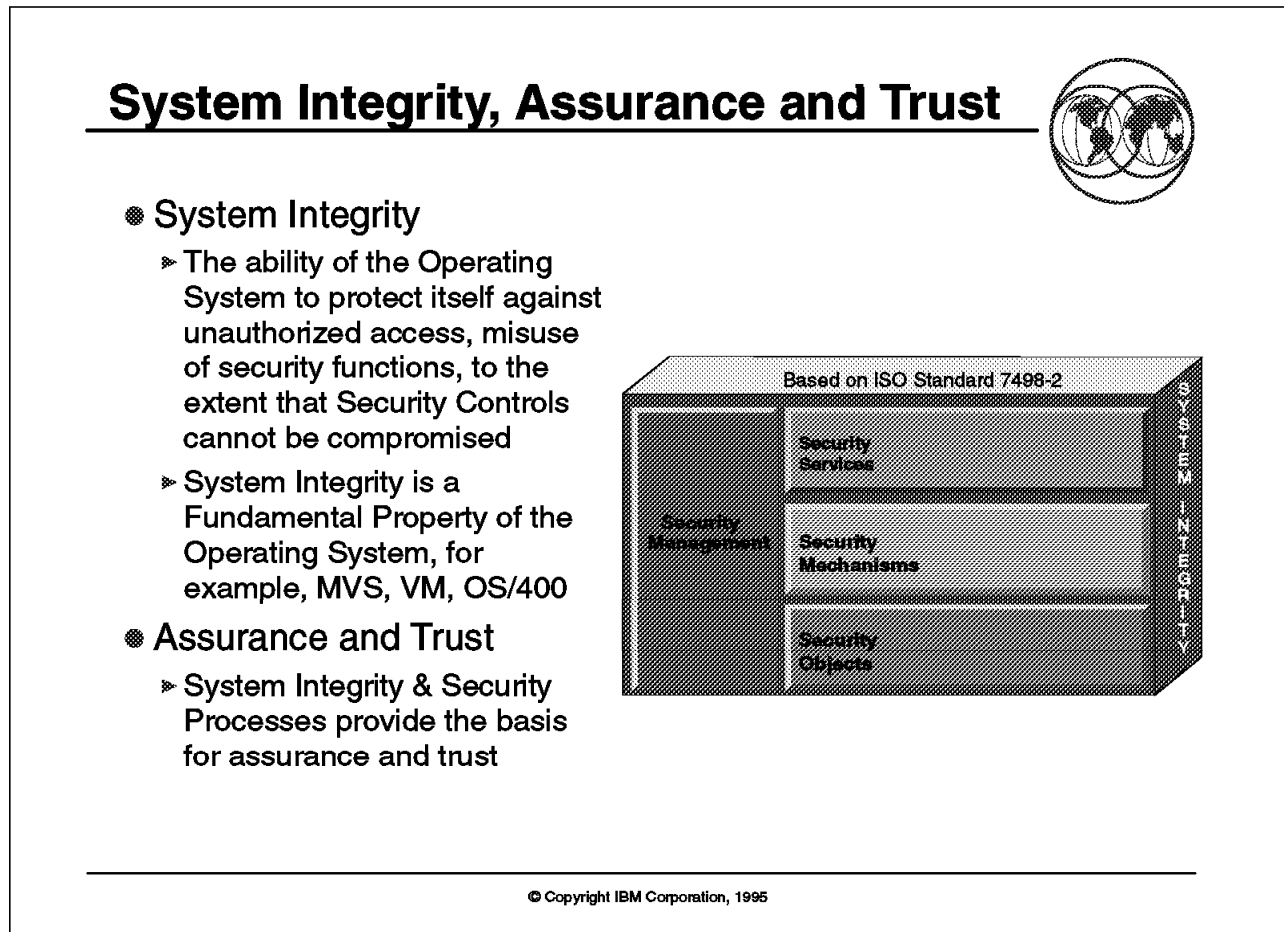


Figure 16. System Integrity, Assurance and Trust

Key Points

System integrity and assurance are the “cornerstone” for security in an operating system.

Presentation Script

System Integrity: While there are specific IBM definitions of system integrity that differ for each system, in general terms, system integrity is the ability of an operating system to prevent the circumvention or bypassing of its security mechanisms. System integrity has been an important characteristic of IBM’s MVS operating system since 1973 and of IBM’s VM operating system since 1983. In 1990, IBM announced support for system integrity in OS/400.

System integrity adds strength to the base systems on which security facilities are built. This strength can then be maintained by ensuring that installation-added extensions (such as exits or other authorized programs) support system integrity by implementing security controls (such as protection of system libraries) that support integrity. In a system with system integrity, application programs that run unauthorized should not be able to breach system integrity.

System integrity is a basic component of the IBM Security Architecture. It is IBM's intent, as part of this strategy and architecture, to ensure that its products provide a level of system integrity that supports the effectiveness of the other architectural components.

Assurance: Assurance in the context of formal government agency evaluation of trusted systems, refers to specific criteria for assessing the effectiveness and correctness of the vendor defined security functions.

In the context of this architecture document, security assurance for information systems, encompasses a variety of areas, including physical security, administrative security, system and application software security, and personnel security. In principle, security assurance must be obtained in all of these areas. However, from the point of view of this architecture, only administrative and system/application software security measures that require system support will be addressed.

Assurance is concerned with proving the ability of a (distributed) system to provide for the following:

1. Establishing the identity of a distributed system component (such as workstation, host, and so forth) that acts on behalf of users, clients, and servers
2. Controlling the origin, type, integrity, and placement of system and application software; not just that of hardware components
3. Identifying system services that are meant to support security policies, and:
 - Determining whether the specified security properties of these services are indeed implemented and are effective
 - Protecting these services from unauthorized circumvention and tampering by other non-security related services and applications

Properties of Trust: The following statements define those conditions that must exist for the term "trusted" to be of value when used in describing a system or its attributes.

- Trusted systems

A system is said to be trusted if assurance evidence exists which shows that:

- The security services and mechanisms are isolated from, and are uncircumventable by, ordinary users and application programs.
- The security services effectively support the security policies and counter the security threats or risks they are designed to address.
- The system is identified, content-controlled, and physically secure.
- The administrative personnel running the system have the required skills to run the system in a secure manner, and have placed the interests of the organization above their own.

- Trusted functions, programs, processes or services

A function, program, process, or service is said to be trusted if assurance evidence exists which shows that it effectively behaves in accordance with its specifications. This may include evidence which shows that (1) the security policy is sound; for example, the policy model is internally consistent; and (2) the security function, program, process or service has

been specified, designed, implemented, verified, tested, and documented in a cohesive and consistent manner.

- Trusted privileged role

An authority is said to be trusted if all users allowed to run in that privileged role have the skills and interests specified for that role and run only trusted functions, programs, processes or services.

The relationship between trust and assurance implies that trust dependencies exist among system components. These dependencies need to be identified in providing a total solution, and indicate the need for trust analysis.

2.3.2 Security Services

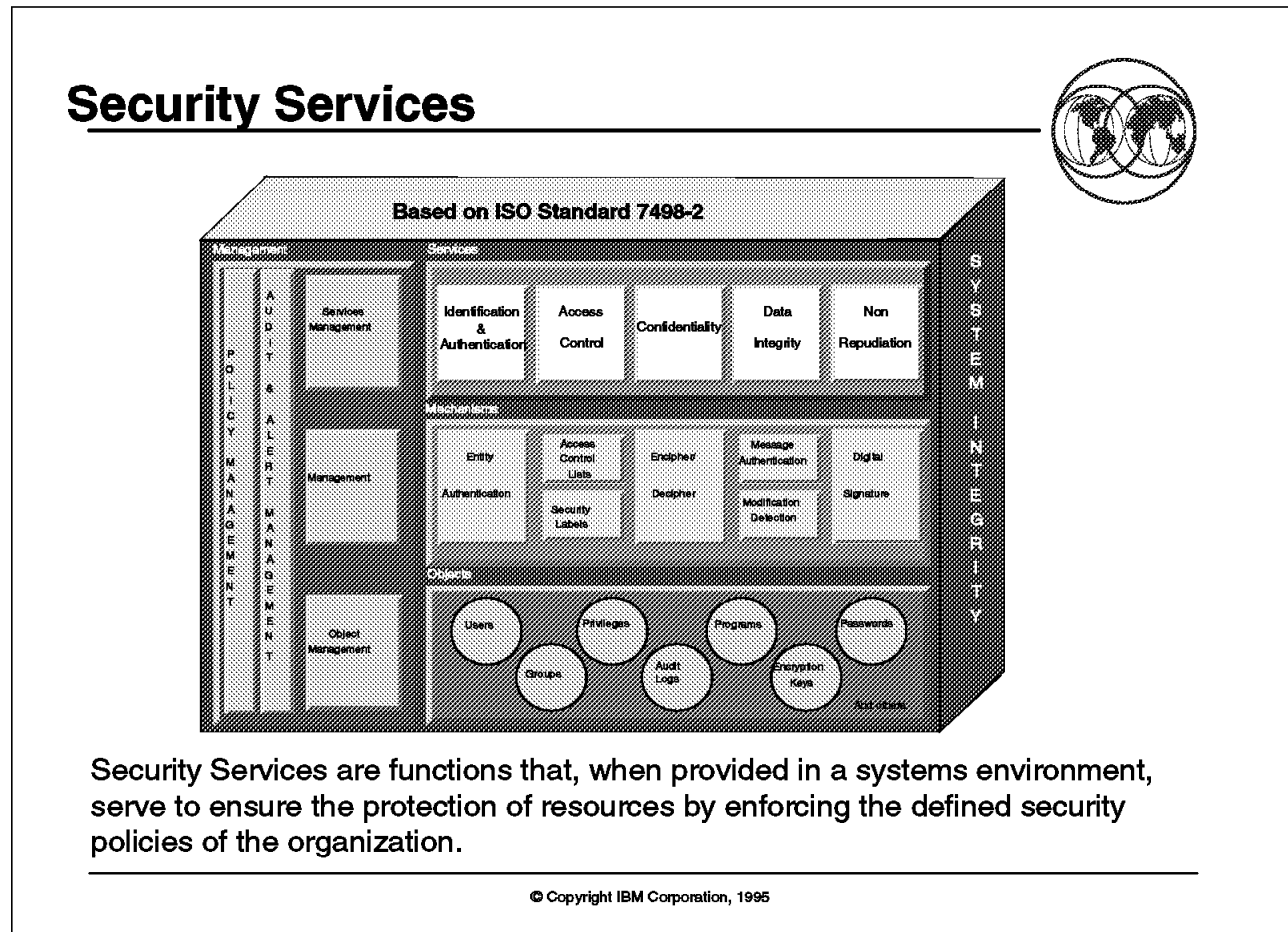


Figure 17. Security Services

Key Points

Security services are the key facilities necessary for an enterprise to implement security controls.

Presentation Script

Security services are those functions that, when provided in a systems environment, serve to ensure the protection of resources by enforcing the defined security policies of the organization.

Identification and Authentication: Identification and Authentication (I&A) facilities verify the identity of individuals. The basic function uniquely identifies users and programs, verifies these identities, and assures individual accountability. Authentication may be single authentication, for an individual user to the system, mutual authentication of peers, such as two party authentication for distributed applications, or three party authentication when dealing with local authentication servers in a distributed environment.

Authenticated user identification provides the basis for additional security functions, such as access control and auditing. Authentication technology may take the form of passwords, smart tokens, smart cards, and biometric measuring devices.

Access Control: Access control allows the installation to protect critical resources by limiting access to only authorized and authenticated users. Depending on the environment, access may be controlled by the resource owner, or, it may be done automatically by the system through security labels. The resource owner can specify who can access the information, how it can be accessed, when it can be accessed, and under what conditions it can be accessed (for example, when executing specific applications, programs, or transactions). The functional goal is to assure that security is maintained for resources, whether they are in a central system, distributed, or mobile (as in the case with files and programs).

Confidentiality: Confidentiality protects sensitive information from disclosure. When it is stored locally, sensitive data can be protected by access controls or encryption mechanisms. For network communication security, sensitive data should be encrypted as it is transmitted from system to system. The IBM architecture for confidentiality is the IBM Common Cryptographic Architecture. There are specific ISO standards (8730, 8731, and 9564) relating to use of cryptography for confidentiality and data integrity, which are supported by IBM's Common Cryptographic Architecture products: the Transaction Security System, the Integrated Cryptographic System Facilities/MVS, and the ES/9000 Integrated Cryptographic Feature.

Data Integrity: Data integrity provides detection of the unauthorized modification of data. Organizations must allow for the use of data by authorized users and applications, as well as the transmission of data for remote processing. Data integrity facilities can indicate whether information has been altered. Data may be altered in two ways: because of hardware or transmission errors or because of an attack. For years, many IBM products have used a checksum mechanism in disk and tape storage systems and in network protocols to protect against transmission and hardware errors. Active attacks on data integrity require a different mechanism, which uses cryptography and allows for the verification of data integrity.

To address active attacks on data integrity, IBM supports message authentication based on cryptographic functions that adhere to international standards. The IBM Common Cryptographic Architecture is the IBM architecture for data integrity, and it defines functions for both message authentication codes (MAC) and modification detection codes (MDC).

Non-Repudiation: Non-repudiation may be viewed as an extension to the identification and authentication services. The non-repudiation service can protect a recipient against the false denial by an originator that the data has been sent, and it can protect an originator against the false denial of a recipient that the data has been received. In general, non-repudiation applies to the transmission of electronic data, such as an order to a stock broker to buy/sell stock; a doctor's order for medication to a specific patient; or approval to pay an invoice by a company to its bank. The overall goal is to be able to verify, with virtually 100% certainty, that a particular message can be associated with a particular individual, just as a handwritten signature on a bank check is tied back to the account owner.

2.3.3 Security Mechanisms

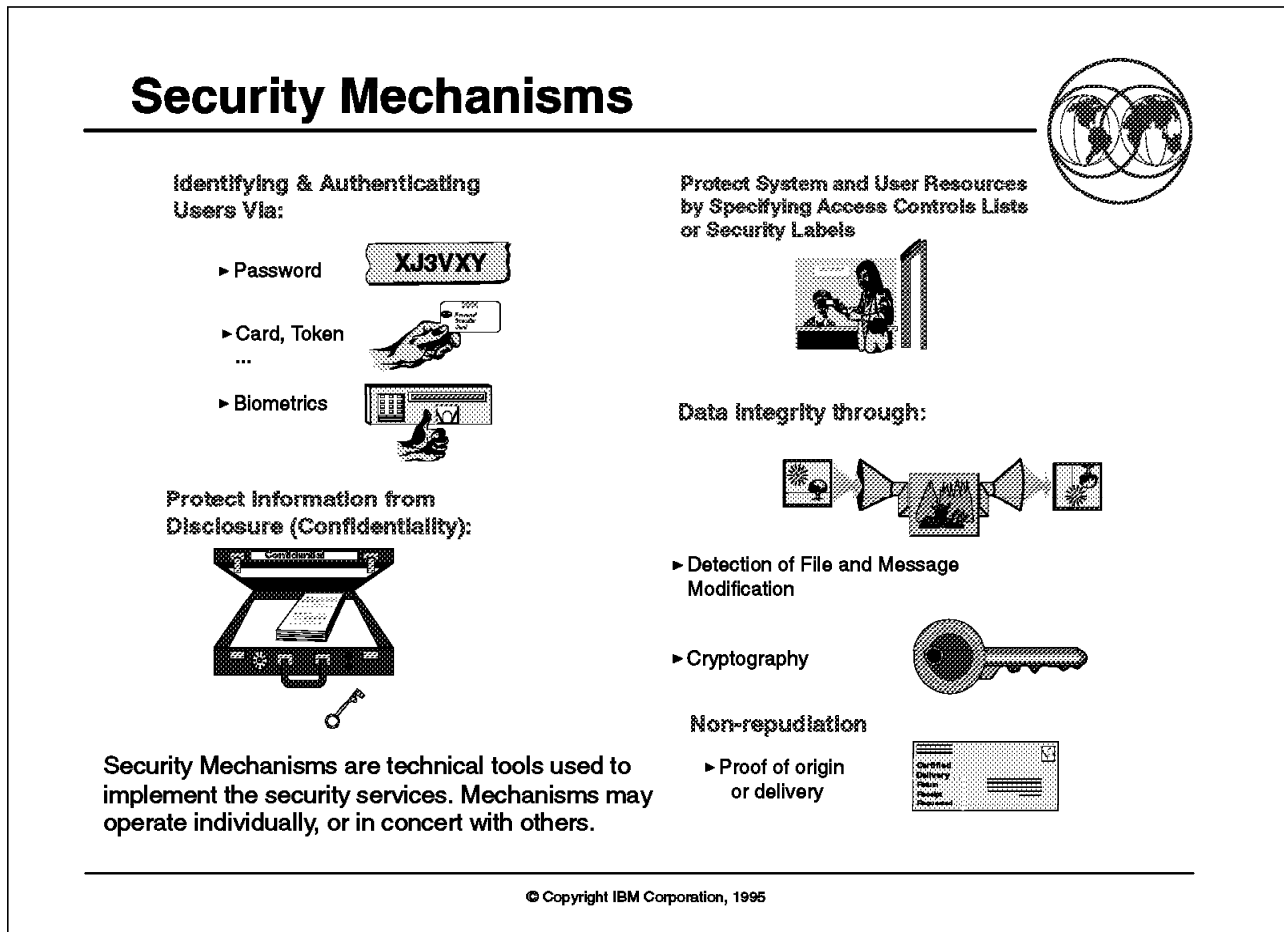


Figure 18. Security Mechanisms

Key Points

Security services are implemented via a selection of available security mechanisms.

Presentation Script

Security mechanisms are technical tools and techniques used to implement the security services. Mechanisms may operate individually, or in concert with others, to provide a particular service.

Entity Authentication: Entity authentication verifies the identity of the entity by comparing identification information provided by the entity to the content of a known and trusted information repository. This information may take the form of something the user knows, something the user has, or something the user is. Stronger verification might require more than one of these characteristics.

Access Control Lists and Security Labels: Access control lists are a form of information repository that contain data relative to the rights and permissions of access granted to each authenticated identity known to the system. Security labeling provides a mechanism to enhance or refine the levels of control imposed on a resource or entity, by defining specific controls on the label tag itself.

Encipherment/Decipherment: Cryptography is the mechanism used to provide the confidentiality service. It is also used quite frequently to complement some other mechanisms to provide total security solutions. Encipherment and decipherment essentially deal with the transformation of data and/or information from an intelligible format, to an unintelligible format, and back to an intelligible format. This is basically a mathematical process employing the use of keys (conversion factors) and algorithms that apply the key values against the data in a predetermined fashion.

MDC and MAC: Data integrity is supported by the use of some sort of checking code. Three methods of calculating the checking code are in common use: cyclic redundancy check (CRC), modification detection codes (MDC), and message authentication codes (MAC). A CRC is relatively easy to compute, and has typically been used to recognize hardware failures. It is a weak check for detecting attacks. The MDC is computed using cryptography, but no secret key is used. As a result, MDC is a much stronger check than CRC, since it is very difficult to find a second message with the same MDC as the legitimate one. However, an MDC has the same delivery requirements as a CRC, in that a CRC or an MDC may be delivered with data by encrypting it using a secret key shared by the sender and the recipient. The MAC is cryptographically derived using a secret key shared by the sender and recipient, so it may be delivered with the data being protected without further trouble.

Digital Signature: In addition to data integrity, non-repudiation services such as digital signature are becoming more important to many customers. Digital signatures provide proof of data origin and/or proof of delivery. The first provides the recipient with proof of who the data sender was. The second provides the sender with a “receipt” for the delivery of data to the intended party. Cryptographic methods are employed in using this technique, and support is provided by the IBM Common Cryptographic Architecture.

2.3.4 Security Objects

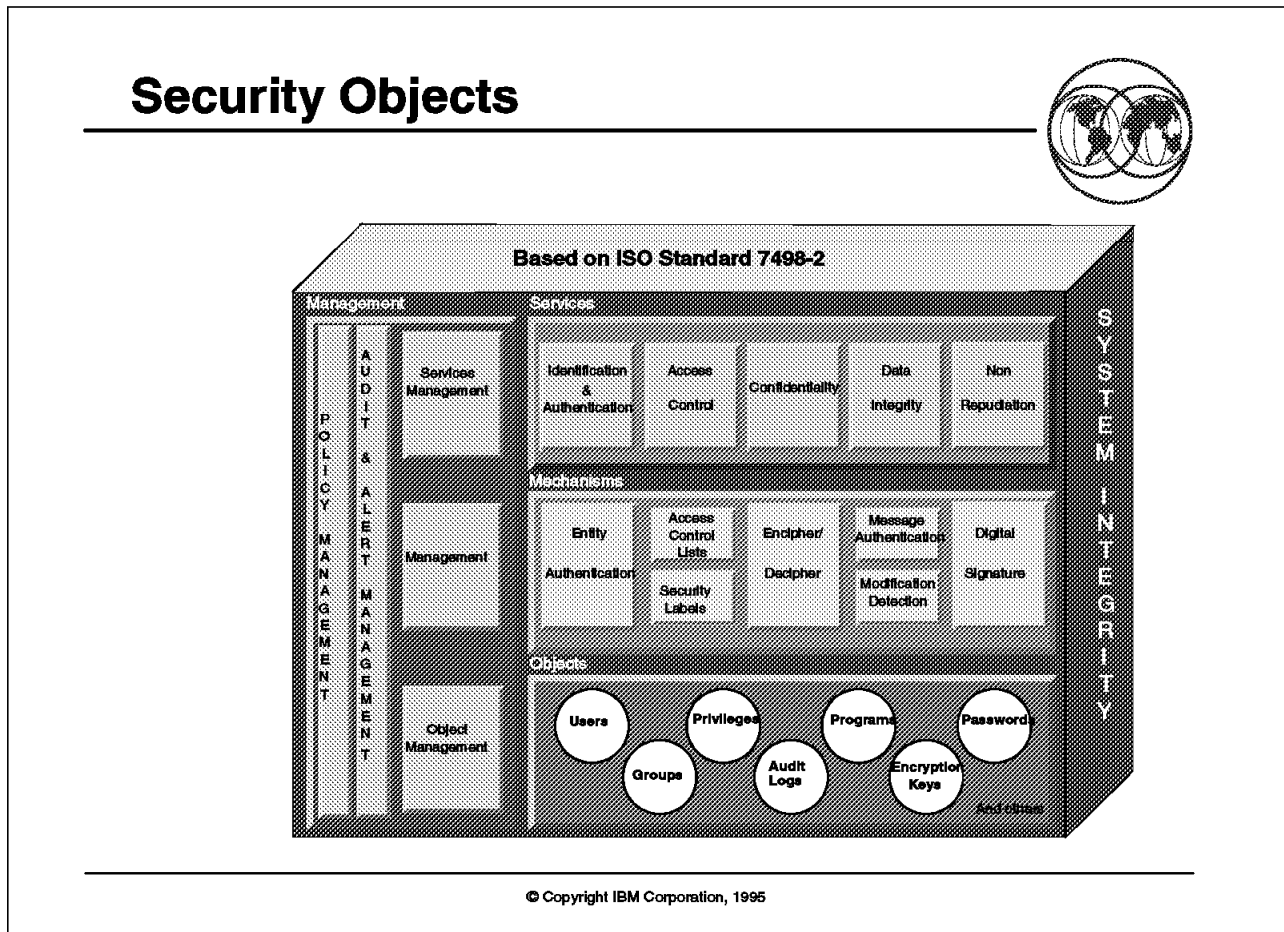


Figure 19. Security Mechanisms

Key Points

Security objects contain the security relevant information about users, groups, privileges, policies, programs, passwords, encryption keys, audit logs, and others.

Presentation Script

Security Objects: The OSI Management Model is based on the definition of the system as a set of “objects.” The structure consists of three components: managed objects, managing objects, and the framework. Managed objects describe what is managed and how it behaves. The definition of managed objects includes specification of their attributes and their behavior, which provides a concrete description of what is manageable. The “how” of management is defined by managing objects consisting of applications and data, which support the management and use of the rest of the system.

In OSI terminology, the security management data is called the Security Management Information Base (SMIB); this is the conceptual repository of all security relevant information needed by open systems. The SMIB is distributed to the extent necessary to enforce a consistent security policy across a (logical or physical) grouping of end systems. This grouping, or security domain, refers

to the set of entities (security objects) that are under the scope of a single organization's set of security policies.

Some examples of security objects might include:

- User profiles (user IDs, group definitions)
- User authorization (to resources)
- Cryptographic keys
- Security labels

The architecture provides for the identification and use of security objects to help meet the requirements for policy enforcement.

2.3.5 Identification and Authentication Service

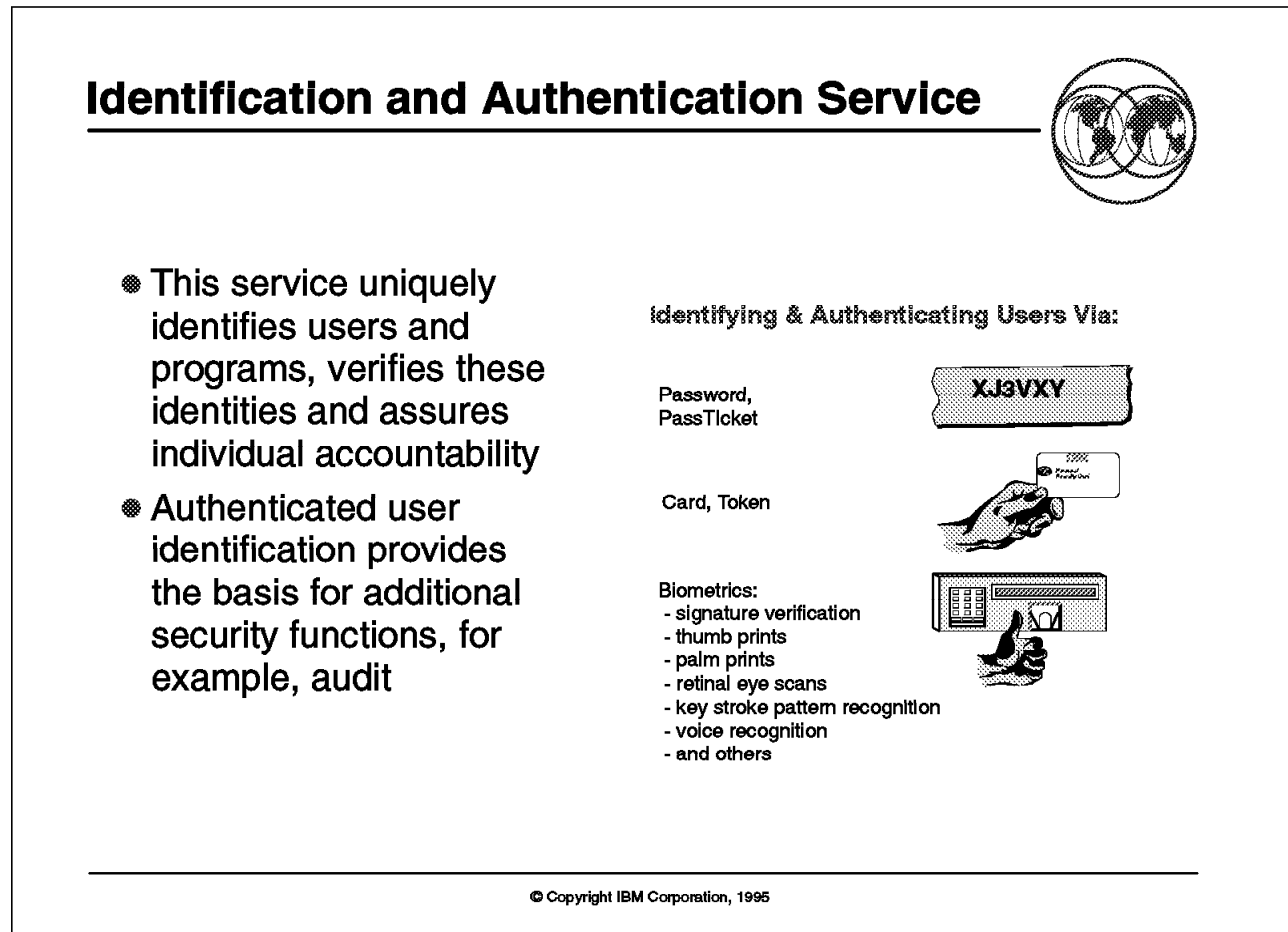


Figure 20. Identification and Authentication Service

Key Points

Identification and authentication provides the basis for all additional security services.

Presentation Script

Identification and Authentication (I&A) facilities verify the identity of entities. The basic function uniquely identifies users and programs, verifies these identities, and assures individual accountability. Authentication may be single authentication, for an individual user to the system, mutual authentication of peers, such as two party authentication for distributed applications, or three party authentication when dealing with local authentication servers in a distributed environment.

Authenticated user identification provides the basis for additional security functions, such as access control and auditing. Authentication technology may take the form of passwords, PassTickets smart tokens, smart cards, and biometric measuring devices.

2.3.6 Entity Authentication Mechanism

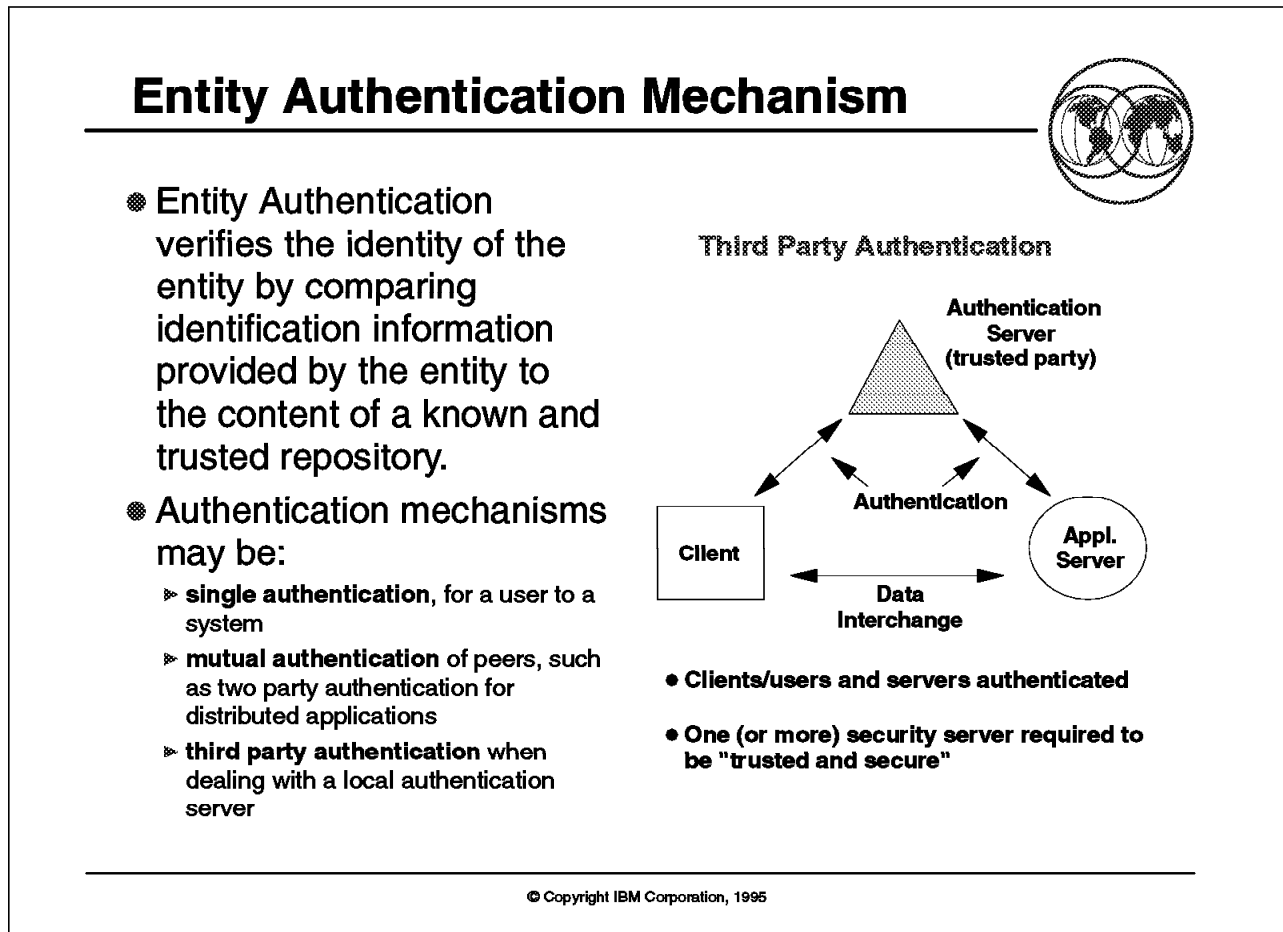


Figure 21. Entity Authentication Mechanism

Key Points

The authentication mechanism level which is selected depends on how an enterprise decentralizes their local trusted security servers and the user security registry administration.

Most local area networks rely on third party authentication mechanisms to provide single sign-on in distributed computing environments.

Presentation Script

Authentication is currently performed at each system that the user accesses. The use of an authentication server in a distributed system will provide the capability to support single sign-on (authentication). Ideally, single sign-on entails one user ID per user regardless of the size or complexity of the network and number of systems where that user has accounts or obtains service. This is essential to support the notion of a single system image.

The authentication mechanism consists of two cooperating processes. The client part accepts an authentication request from a logon program (currently a part of each subsystem or operating system). The client then locates the server process, which may be either local or remote. The server process must be located in a system that can provide confidentiality and integrity of the stored

authentication data. The client passes the user ID and (optionally) the authentication data (such as a password) to the server.

Protection of the user password from interception has become a major concern, especially in unprotected network environments. User authentication must provide a scheme whereby the password is not usable if intercepted, and this scheme must be based on cryptography for the level of confidence required. There are currently two proposed means (referred to as two-party and three-party authentication) to provide user authentication without exposing the password in a network.

Two Party Authentication: Conventional or symmetric cryptography (such as the Data Encryption Standard) involves the use of keys whose value must be kept secret. Client workstations that have protected storage capability can store and protect a secret key. This key can be used to encrypt the password, and the password can be sent to the authentication server along with the user ID. The server can then verify that the password is correct for the user ID supplied. Notification of the success or failure of user authentication is returned to the client workstation. However, some workstations have no capability to protect the secret key from applications on the workstation or from the workstation users. For these workstations, there are several alternatives.

One alternative is to treat them like non-programmable terminals and send the password to the authentication server unprotected. An improvement over this scheme is a "smart token" which yields a one-time password.² Another is to use a trusted third-party authentication scheme.³

Three-Party Authentication: The trusted third-party approach is to have the client workstation send only the user ID to the authentication server. The authentication server then prepares a "ticket," which is an encrypted package containing, among other things, the user ID. The ticket is encrypted with a derivative of the user's password and is usable by the client workstation only when decrypted by applying the user's password as the key. If the user supplies the correct password, the ticket can be decrypted and the user ID can be compared for equality. A successful match of the user ID completes the authentication cycle. The client can then proceed to make requests of system services.

The use of an authentication server simplifies the administration of user passwords; they can be stored in one database and updates need not be replicated to all systems. This centralization can be done for an entire organization, or there can be multiple authentication servers in an organization. The client process must be implemented and available on all systems. An MVS system might be a client in a domain and provide client support for attached non-programmable workstations as well as programmable workstations. Each strategic system must provide the authentication server function.

The user identification and authentication service must also provide for re-authentication of users via application invocation. In addition, the

² Note that smart token support is presently available through the use of appropriate RACF exits.

³ An example of a trusted third-party scheme is documented in *Kerberos Authentication and Authorization System* by S. P. Miller, B. C. Newman, J. I. Schiller, and J. H. Saltzer, Project A Technical Plan, Section E.2.1, Massachusetts Institute of Technology, 1987, and *Kerberos: An Authentication Service for Open Network Systems* by C. Neuman, J. I. Schiller, and J. G. Steiner, Proceedings USENIX Winter Conference, Dallas, Texas, Feb. 1988.

authentication service must support tailorable settings of timeouts, protection against repeated logon attempts, time of last access notification, password expiration notification, and time of day/day of week logon restrictions.

At this point, passwords remain the dominant and most popular type of authentication approach. However, this is changing as the technology for authentication evolves. The server must be able to accept other forms of authentication data with a mixture of technology being presented by a given user population. The use of additional methods of user authentication are anticipated, and the architecture allows for a general interface for authentication data input.

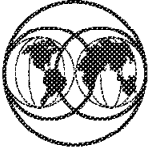
Certification: Certification is the means by which an authenticated user identification is passed between systems. There are two approaches that can currently be used to provide this service. The first is based on mutual trust between systems. The second is based on the use of a trusted third party. The architecture provides for supporting both types of mechanisms.

The LU6.2 conversation security approach does not support the protection of passwords in a PWS without protected storage, as described in the previous section. Certification is provided via one of two methods. After a successful authentication, the workstation is required to send the user ID to each system accessed. If the system trusts the workstation, an "already verified" indicator is sent along with the user ID. If the system does not trust the workstation, the workstation must send the user ID and the password (encrypted or unencrypted). This certification can be cascaded to other systems as required. Note that with this approach the password has to be stored, and a capability to update the password has to be provided, in each system, or the password must be repeatedly sent to the authentication server for (re-)verification.


The trusted third party approach relies on a server trusted by all other systems to provide verification that a GUID is valid. Since there is no implied trust between any of the other systems, the information must be protected from modification by any systems through which it is transmitted. After successful authentication, the certification server (the trusted third party) provides tokens (similar to tickets described earlier for user authentication) to the client system. These tokens are encrypted with a key that is shared only by the certification server and the target system, thus protecting them from modification and disclosure. The tokens contain the GUID and other information related to the user or user session. Each time a different system is accessed, a new token is generated for that system. This approach eliminates the need to store a user password anywhere but at the authentication server at the expense of additional message traffic between the client and certification server, and presumes the presence of a cryptographic key distribution and management system supported by the certification server and the target system.

2.3.7 Access Control Service

Access Control Service



- This service allows an Installation to protect resources by limiting access to only authorized and authenticated users
- The resource owner specifies:
 - ▶ Who can access the information
 - ▶ How it may be accessed
 - ▶ When it may be accessed
- The goal of this service is to ensure that the security is maintained for the resources, whether in a centralized or distributed environment



Access control:-
"who may go through"

© Copyright IBM Corporation, 1995

Figure 22. Access Control Service

Key Points

Access control allows authorized usage of protected resources.

Presentation Script

Access control allows the installation to protect critical resources by limiting access to only authorized and authenticated users. Depending on the environment, access may be controlled by the resource owner using access lists, or, it may be done automatically by the system through security labels.

The resource owner can specify who can access the information based on either user identification or group identification; how it can be accessed such as read, write, or execute; when it can be accessed such as day or week or time of day; and under what conditions it can be accessed (for example, when executing specific applications, programs, or transactions). The functional goal is to assure that security is maintained for resources, whether they are in a centralized system, distributed, or mobile (as in the case with files and programs).

2.3.8 Access Control Mechanisms

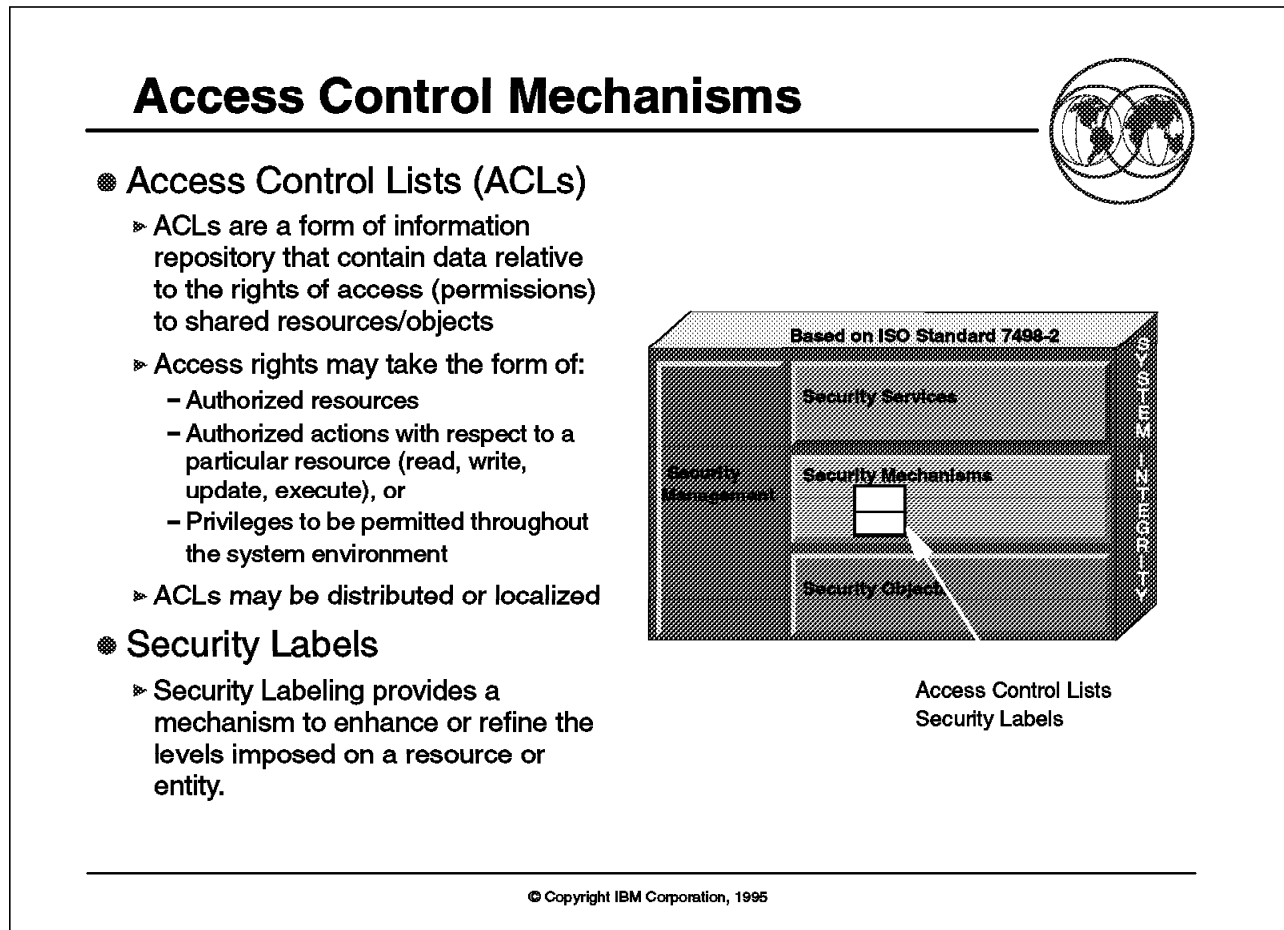


Figure 23. Access Control Mechanisms

Key Points

Access control services are implemented by access control lists and/or security labels.

Presentation Script

Access Control Lists: Access control lists (ACLs) are a form of information repository that contain data relative to the rights of access (permissions) to shared resources/objects granted to authenticated users of the system. The access rights might take the form of authorized resources, authorized actions with respect to a particular resource (read, write, update, execute), or privileges to be permitted throughout the system environment. Access control lists are categorized as discretionary access control (DAC) mechanisms.

Access control lists may be distributed, as in the case of a global directory of network resources, or they may be localized, as in the case of controlling access to resources owned by a particular resource manager. Management of the ACLs may be done by a single centralized authority using remote management interfaces, or it may be done locally by an individual resource manager using internal management interfaces.

Security Labels: Security labeling provides a mechanism to enhance or refine the levels of control imposed on a resource or entity. For example, the label could specify sensitivity information (classification), or could provide additional constraints on resource access based on the role of the user, the function being performed, department, or categories in a manner similar to group controls. Security labels are also called mandatory access control (MAC) mechanisms.

DCE's Model for An Access Control Resource Manager (ACRM): The DCE model for an ACRM is considerably different from the model which has generally, but not always, been implemented on IBM's strategic platforms. In DCE, each application server that manages resources is responsible for its own implementation of an ACRM. This is in contrast, for example, with MVS where RACF or other vendor products have provided the equivalent of ACL management and access control checking functions in a single product that can be used by many different application servers. Products such as RACF also supply an implementation of an auditing mechanism integrated with the access control checking facilities.

The DCE code provided by OSF contains a "reference implementation" for an ACRM that server writers can use as a model to implement their own ACRMs. The model addresses the management of ACL objects both locally and remotely and specifies the algorithms for checking access control. The four basic parts of the reference implementation are described below.

1. *sec_acl APIs*

The set of callable APIs prefixed with *sec_acl* are intended for use by clients. These interfaces are used by the OSF-supplied ACL editor to implement its command-line and interactive user interface modes for editing ACLs. All of the DCE components that have implemented their own ACL manager "export" a connection to this interface, and the *sec_acl* API calls are the interfaces used to invoke the server's ACL manager. The *sec_acl* calls invoke the security client *rdac* stub code (described below) shipped by OSF in a library called *libdce*. The *sec_acl* calls are used for:

- Binding (getting addressability) to an object's ACL
- Listing the access permissions which a caller has for an object
- Testing an object's ACL for permissions matching those of the caller
- Obtaining returned error information
- Listing the manager types for the ACLs protecting an object
- Returning ACL information in printable form
- Returning an object's ACL

In a typical scenario, the *acl_edit* application will use the above routines to get a handle and the management type of an ACL, then load the ACL into temporary storage. It would then manipulate entries and fields within entries or sometimes rebuild the whole ACL using *acl_edit* subcommands. The application will then replace the revised ACL and release the temporary storage.

2. *acl_edit*

The ACL editor supports a command line mode and an interactive mode of operation which prompts the user for input parameters. The ACL editor works at three levels: the entire ACL, individual ACL entries, or permission bits within an entry. When dealing with the entire ACL, it can list its contents, list the available permission tokens, remove or replace all entries, and assign the modified ACL to its object. At the ACL entry level, it can add or

delete a single entry. At the entry field level, it can display permissions, test for permissions, and change permissions.

Note that there is significantly more function defined in POSIX 1103.6 for the manipulation of ACL entries and entry fields using a callable programming interface. The POSIX command line utilities, *getacl* and *setacl*, provide equivalent function to the DCE *acl_edit* application.

3. *rdacl*

The set of interfaces prefixed with *rdacl* are specified in the DCE documentation so that ACRM writers will know what they must implement to interface with the client-side calls to the ACRM. OSF does not supply a library of routines that implement these interfaces but does supply the Interface Definition Language (IDL) files that, when linked with the client or server, provide the necessary stub code for marshalling and demarshalling parameters for the calls. Each ACRM must implement the code behind the *rdacl* interfaces for:

- Reading a privilege attribute certificate
- Listing the types of ACLs protecting an object
- Returning printable ACL strings
- Getting a referral to an ACL update site
- Returning the ACL for an object
- Replacing an ACL
- Testing access to an object
- Testing access to an object on behalf of another process

4. *sec_acl_mgr*

The set of interfaces, prefixed with *sec_acl_mgr*, are specified in OSF's DCE documentation. Sample source code for implementing the interface is supplied as part of the Registry Resource Manager. The DCE approach is for each server writer to develop the code (using the sample as a guide) that implements the functions specified in the interface, as well as provide a separate file or database, as necessary, in which to store the ACLs.

The set of API calls that an ACRM is required to implement are intended for the local use of the server and provide for:

- Configuring an ACL manager
- Reading a privilege attribute certificate
- Returning the types of ACLs that are protecting an object
- Returning printable ACL strings
- Comparing a privilege attribute certificate with an ACL
- Finding an ACL using its key
- Replacing an ACL

POSIX Access Control Lists: In November 1990, IBM adopted POSIX access control lists as extended for the distributed environment by OSF's DCE, with possible IBM extensions, as the basis for the implementation of common cross-platform access control mechanisms.

Draft 12 of the IEEE POSIX 1003.6 Security Interface standard contained a definition for an access control list mechanism. The draft defined several aspects of the mechanism but did not dictate the actual implementation, such as specific internal representation or ordering of entries within an ACL. The draft defined:

- The relationship between this ACL mechanism and the ACL permission bits defined in IEEE POSIX 1003.1-1990
- The composition of an entry within an ACL
- Default ACLs and the association of an ACL with an object at object creation time
- The ACL access check algorithm
- Functions for managing the ACL working storage area
- Functions for manipulating ACL entries
- Functions for reading and writing an ACL
- Functions for translating an ACL between internal and external representations
- User-level utilities for displaying and changing the contents of an ACL

An implementation of an access control list mechanism based on OSF's DCE model would not include several of the elements defined in Draft 12. Only the first four of the above listed elements could be considered to be covered in the DCE model, because no interfaces are provided in DCE for the POSIX ACL and ACL entry manipulation functions. To claim compliance with the eventual POSIX standard, it will be necessary to implement all of the defined APIs.

DCE Extensions to POSIX ACLs: DCE ACLs (called DACLs) contain extensions to the mechanism defined in POSIX 1003.6. DACL extensions provide the following:

- Owner/administrator privileges can be extended to multiple users.
- Users and groups from foreign cells can appear on DACL entries.
- Extensibility mechanisms are provided that allow clients with an older version number to manipulate DACLS on newer generation servers.
- An ability for principals in the owner class to set the permissions associated with the owner, group, and other masks.
- An "unauthenticated" entry to control access to objects of unauthenticated users.

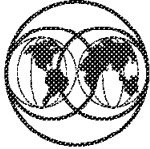
ACL Manipulation Interface Levels: There is a distinct difference between the intended levels of the POSIX and DCE ACL APIs. The POSIX manipulation functions are defined so that the caller is isolated from the internal representation of ACLs and the representation and ordering of entries within them. On the other hand, the DCE interfaces are intended to provide the caller with access to the actual internal representations of ACLs and ACL entries.

Application servers that must remain independent of the way ACLs are represented on a particular platform should use the POSIX APIs.

Application servers that must be portable to any DCE platform, IBM or non-IBM, that can only rely on the DCE ACL APIs being supported, might have to deal with the internal representations of the ACLs.

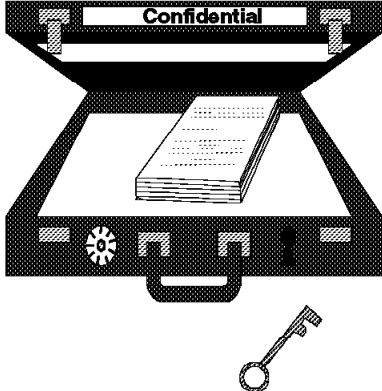
2.3.9 Confidentiality Service

Confidentiality Service



- Confidentiality protects sensitive information from disclosure
- When information is stored locally, it may be protected by access control mechanisms or more stringently via encryption mechanisms
- For network communication security, sensitive data should be encrypted, as it is transmitted from system to system
- There are ISO standards (8730, 8731 and 9564) relating to use of cryptography for confidentiality and data integrity

Protect Information from Disclosure



© Copyright IBM Corporation, 1995

Figure 24. Confidentiality Service

Key Points

Confidentiality is the key security service for ensuring non-disclosure of sensitive information travelling on untrusted communication networks.

Presentation Script

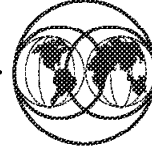
Confidentiality services protect information from unauthorized disclosure. The mechanism used is cryptography. This service provides protection of information in both storage and transmission. Requirements for confidentiality services, which exist at every level in the processing structure, depend on the granularity of protection necessary. The security architecture provides a common mechanism in each strategic operating system, allowing resource managers, applications, and the operating system itself to benefit from this cryptographic service, as appropriate. At a minimum, each strategic system supports the Common Cryptographic Architecture Application Programming Interface, which defines the calls for the confidentiality service. The architecture for this common mechanism is defined in the IBM Common Cryptographic Architecture (CCA).

Requirements also exist for transparent encryption/decryption of data in database, file, office, and communications applications. In this case, transparent means transparent to the calling program. For instance, files could be encrypted

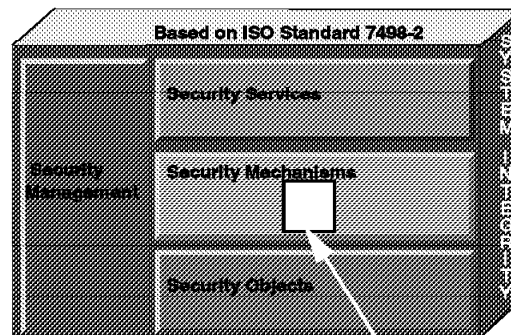
automatically when saved and decrypted automatically when retrieved. Also requirements exist for controlling the encryption/decryption process in database, office, and communications applications which may not be transparent. This necessitates the use of additional encryption parameters on called services. For example, a program requesting use of a file could specify decryption on file open and encryption on file close.

2.3.10 Encipherment/Decipherment Mechanisms

Encipherment/Decipherment Mechanisms



- Encipherment is the process used to transform data from an intelligible format to an unintelligible format
- Decipherment is the reverse process
- Encipherment/Decipherment algorithms:
 - Data Encryption Algorithm (DES)
 - Commercial Data Masking Facility (CDMF)



Encipher/Decipher

© Copyright IBM Corporation, 1995

Figure 25. Encipherment/Decipherment Mechanisms

Key Points

The confidentiality services are dependent on mechanisms that encrypt and decrypt data based on standard algorithms such as the Data Encryption Algorithm and Commercial Data Masking Facility.

Presentation Script

While cryptography is the mechanism used to provide the confidentiality service, it is also often used to complement other mechanisms in providing total security solutions. Encipherment is a process that transforms data from an intelligible format to an unintelligible format. Decipherment is the reverse process.

Data Encryption Standard (DES): The Data Encryption Standard (DES), also known as the Data Encryption Algorithm (DEA), is a symmetric key algorithm with an input and output blocksize of 64 bits and a key of 64 bits. The key contains 56 independent bits that determine the specific cryptographic transformation and 8 bits that may be used for parity checking. The DES is defined in USA Federal Information Processing Standard (FIPS) 46-1; the DEA is defined in ANSI standard X3.92. The DES was designed by cryptographers at IBM with assistance from NSA. The DES is the best known and most used

commercial cryptographic algorithm. It is used to protect stored files, messages, personal information numbers (PINs), electronic funds transfer (EFT) transactions, and cryptographic keys.

The DES was recertified in 1992 by the U.S. National Institute of Standards and Technology (NIST).

Commercial Data Masking Facility (CDMF): Since implementations of DES--when used for data confidentiality--are not generally exportable, IBM cryptographers designed the Commercial Data Masking Facility (CDMF) algorithm. The CDMF has the external attributes of DES. It makes use of a DES-based kernel and a key that is shortened to an effective key length of 40 DES key-bits. Although the effective key length is shorter, the CDMF meets the needs of customers who do not desire to send clear data.

Implementations of CDMF--when used for data confidentiality--are generally exportable from the USA. The CDMF is registered in the ISO registry of cryptographic algorithms, according to ISO/IEC standard 9979.

Because the CDMF is not as strong as DES, the CDMF is called a "masking" algorithm rather than an "encryption" algorithm. The CDMF has advantages over other exportable data confidentiality algorithms. For instance, by using a simple key transformation, a system that implements only CDMF for data confidentiality can interoperate with a system implementing only DES for data confidentiality.

More information about CDMF can be found in the March 1994 issue of the IBM Journal of Research and Development (Volume 38, Number 2, Reprint G322-0191-00).

2.3.11 Data Integrity Service

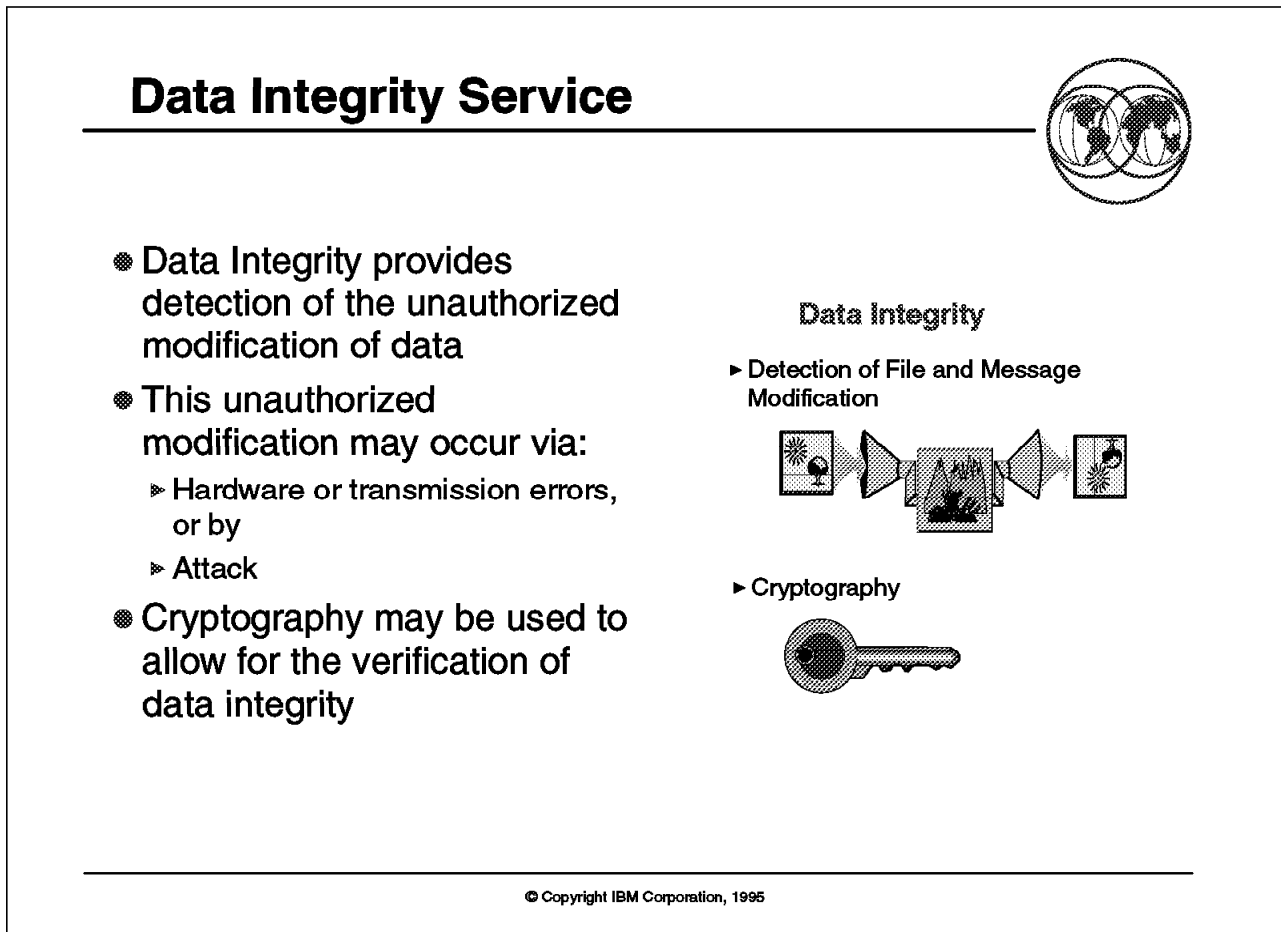


Figure 26. Data Integrity Service

Key Points

Data Integrity is the key security service for detecting unauthorized modification of data due to errors or malicious attack.

Presentation Script

Data integrity provides detection of the unauthorized modification of data. Organizations must allow for the use of data by authorized users and applications, as well as the transmission of data for remote processing. Data integrity facilities can indicate whether information has been altered. Data may be altered in two ways: because of hardware or transmission errors or because of an attack. For years, many IBM products have used a checksum mechanism in disk and tape storage systems and in network protocols to protect against transmission and hardware errors. Active attacks on data integrity require a different mechanism, which uses cryptography and allows for the verification of data integrity.

To address active attacks on data integrity, IBM supports message authentication based on cryptographic functions that adhere to international standards. The IBM Common Cryptographic Architecture is the IBM architecture for data integrity, and it defines functions for both message authentication codes (MAC) and modification detection codes (MDC).

2.3.12 Data Integrity Mechanisms

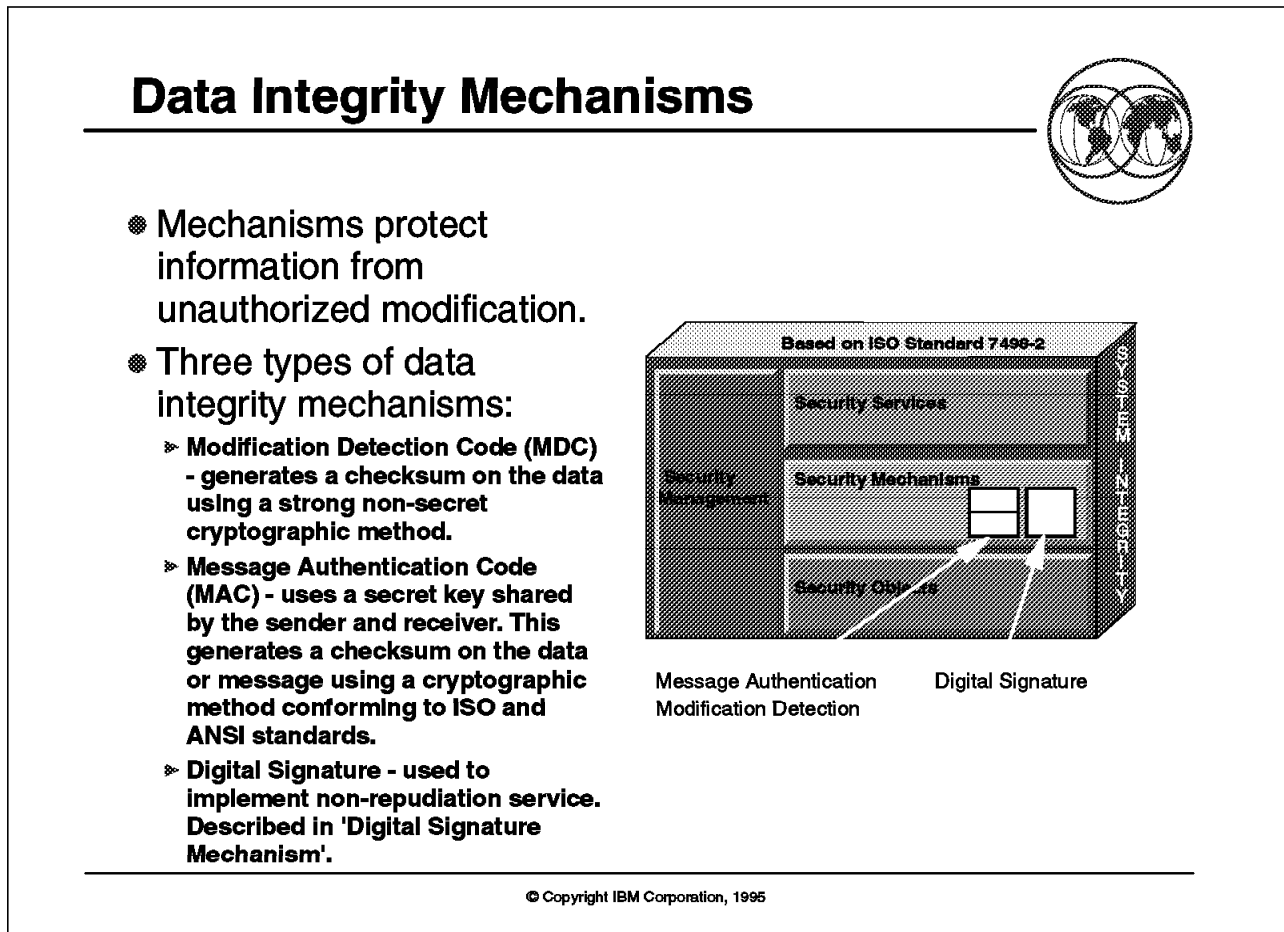


Figure 27. Data Integrity Mechanisms

Key Points

The data integrity services are dependant on encryption mechanisms for modification detection, message authentication and digital signatures.

Presentation Script

Data integrity mechanisms protect information from unauthorized modification. All data integrity mechanisms are based on the principle of redundancy. That is, given an original data object, a data integrity object is calculated on the original data. Typically, the original data object and the data integrity object are kept together.

Mechanisms such as a Cyclic Redundancy Code (CRC) check or a parity field check, which are appropriate to detect accidental modification of data, are relatively fast and easy to compute. However, a CRC or parity field check involve no secret quantity, and so these methods are insufficient by themselves to thwart deliberate modification of data.

Cryptographic methods must be used when there are concerns about the deliberate modification of data. There are three cryptographic methods available:

- Modification Detection Code (MDC) also known as a message digest. An example is MDC-2 and MDC-4 supported by CCA products.
- Cryptographic checksum based on a symmetric key algorithm. An example is the DES-based Message Authentication Code (MAC) supported by CCA products.
- Digital Signature based on a public key algorithm. An example is the RSA-based digital signature supported by CCA PKA products.

There are three types of data integrity mechanisms that are strategic

- The first is a modification detection mechanism. This cryptographic mechanism requires no secret key. The modification detection mechanism generates a checksum on the data using a cryptographic method.
- The second is a message authentication mechanism. This cryptographic mechanism uses a secret key shared by the sender and receiver. The message authentication mechanism generates a checksum on the data or message using a cryptographic method conforming to ISO and ANSI standards.⁴
- The third is a digital signature generation and verification mechanism. As digital signatures additionally provide a nonrepudiation capability, they are described in 2.3.14, “Digital Signature Mechanism” on page 59.

Modification Detection Code (MDC) Mechanism: A Modification Detection Code (MDC) or message digest is a checksum calculated using a strong non-secret cryptographic one-way hash function. A function is called a cryptographic one-way function if it is easy to compute in one direction but is very difficult or infeasible to compute in the other direction. That is, it is easy to compute the hash from the data but, for practical purposes, infeasible to compute the data from the hash (or equivalently to compute any data that, when hashed, will produce a value equal to a given hash value).

There are many uses for an MDC. For example, one may wish to load a large program into a system but want assurance that the program has not changed (for example, by a computer virus). If the creator of the program calculates an MDC on the program and publishes the value in widely distributed fora (such as a newspaper), anyone can recover the well-known MDC and compare it for equality with the MDC just calculated on the program. A similar example is the data reduction problem; that is, one has a large amount of data that needs integrity and what is desired is a calculation on the data that results in a relatively small amount of data whose integrity is easier to protect.

Message Authentication Code (MAC) Mechanism: The MAC is cryptographically derived using a secret key shared by the sender and recipient and is sometimes delivered (in encrypted form) with the data being protected. A MAC key relationship is established between a message originator and message recipient. The originator constructs a message and then using the appropriate MAC key generates a MAC value that is appended to the message. The recipient, using the same MAC key, generates a new MAC value and compares this to the original MAC value appended to the message. If the two MAC values are

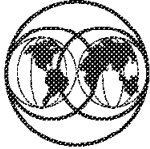
⁴ ISO 8730 Banking - Requirements for Message Authentication (Wholesale). The ANSI X9.9 standard is required by most financial customers for wholesale and retail banking. The emerging electronic data interchange (EDI) Message Authentication Code standard is expected to be consistent with the ANSI Message Authentication Code standard.

equal, two things have been demonstrated: 1) the originator of the message has the authorization to send the message since the originator possesses the right MAC key, 2) the content of the message has not been altered. When the recipient is satisfied with the message authentication and content, an acknowledgement message, perhaps using a different MAC key, is sent to the originator. The originator processes the acknowledgement message and satisfies any content and authenticity questions by repeating the same process that was used by the recipient. If the acknowledgement message passes the MAC test, the originator has proof of receipt.

The CCA implementation of the MAC mechanism makes use of control vectors that permit a MAC key to be generated in two forms: a MAC generation key and a MAC verification key. A MAC generation key allows a MAC to be generated whereas a MAC verification key allows a MAC to be verified but not generated. Thus, the CCA DES-based implementation simulates attributes of a public key system.


2.3.13 Non-Repudiation Service

Non-Repudiation Service



- The non-repudiation service provides:
 - ▶ Proof of origin of data
 - ▶ Proof of delivery of data
 - ▶ Proof of submission of data
 - ▶ Proof of transport of data
- Non-Repudiation can:
 - ▶ Protect a recipient against the false denial of an originator that the data has been sent
 - ▶ Protect an originator against the false denial of a recipient that the data has been received
- Non-repudiation is implemented by cryptographic mechanisms

Non-Repudiation
Proof of origin or delivery



© Copyright IBM Corporation, 1995

Figure 28. Non-Repudiation Service

Key Points

Non-repudiation services provide proof of data origin and delivery.

Presentation Script

The non-repudiation⁵ security facility is an encryption-based mechanism that provides the following functions:

- Proof of origin of data
- Proof of delivery of data
- Proof of submission of data
- Proof of transport of data

The non-repudiation service is different from the data integrity service (per the ISO 7498-2 guideline). Non-repudiation is critical for electronic data interchange (EDI) security and thus is a strategic element of the architecture. The digital signature mechanism is the principal implementation of a non-repudiation service.

⁵ Non-repudiation is defined by ISO/IEC CD 13888-1, *Information Technology - Security Techniques - Non-repudiation; Part 1: General Model*.

2.3.14 Digital Signature Mechanism

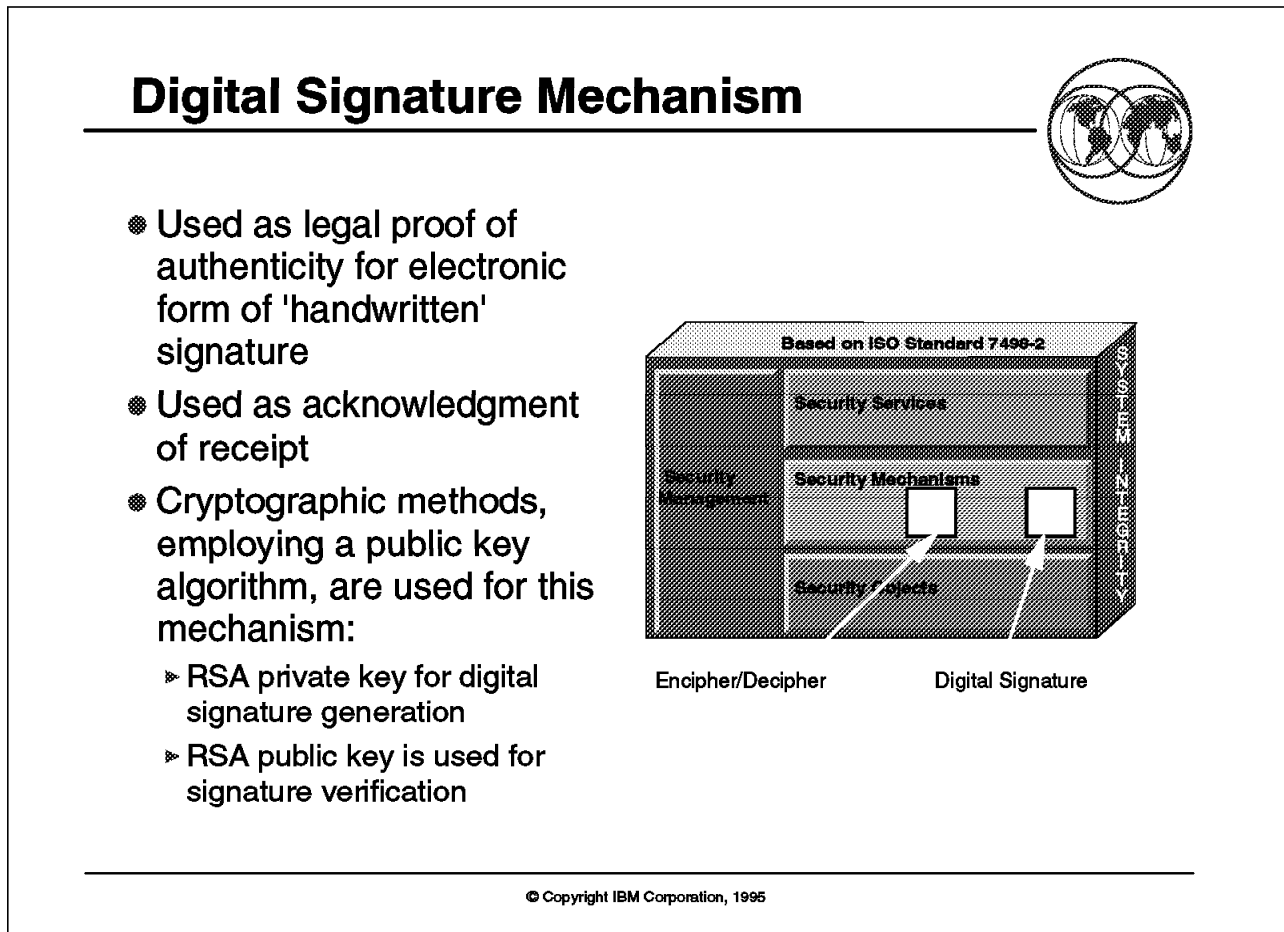


Figure 29. Digital Signature Mechanism

Key Points

Non-Repudiation services are implemented by digital signature mechanisms, such as the RSA Public Key Algorithm.

Presentation Script

The technique of digital signature can be used to implement the non-repudiation service. On the emerging information highway, the digital signature replaces the handwritten signature as a legal proof of authenticity. It may be used to provide for proof of origin, proof of delivery, proof of submission and proof of transport. A digital signature is used directly to provide proof of whom the data sender was. A digital signature is used to sign an acknowledgement "receipt" for the latter three proofs. Cryptographic methods are employed in using this technique, and support is provided by the IBM Common Cryptographic Architecture Public Key Algorithm.

RSA Public Key Algorithm: The Rivest Shamir Adleman (RSA) public key algorithm is based on the difficulty of the factorization problem. The factorization problem is to find all prime factors of a given number n . The factorization problem is believed by mathematicians to be hard when n is sufficiently large (for RSA, n is typically 512 bits or more) and when n is the product of a few large primes (for RSA, n is the product of 2 large primes).

The RSA algorithm is used in ISO standard 9796 Digital Signatures and is in draft ANSI X9.31 Part 1 Digital Signatures. The RSA private key is used for digital signature generation, and the RSA public key is used for digital signature verification. The size of an RSA digital signature is typically 512 bits, although for some applications the size may be up to 1024 bits. A larger digital signature has more security but takes longer to generate and verify.

RSA is also used in draft ISO standard 11770 Key Management using Asymmetric Techniques and in draft ANSI X9.44 RSA Key Transport. The RSA public key is used for symmetric (such as DEA) key encryption and the RSA private key is used for symmetric key recovery. The size of an RSA-encrypted symmetric key is typically 512 bits.

Digital Signature Standard: The NIST Digital Signature Standard (DSS) public key algorithm is based on the difficulty of the discrete logarithm problem. The discrete logarithm problem is to find x given a large prime p , a generator g and a value $y = (g^{**x}) \bmod p$, where $**$ represents exponentiation. A generator g is a value such that $g^{**x} \bmod p$ generates all values in the set $(1,2,\dots,p-1)$ as x is incremented from 1 to $p-1$. This problem is believed to be very hard when p is sufficiently large (for DSS, p is 512 bits or more) and x is a sufficiently large random number (for DSS, x is 160 bits).

DSS is defined in NIST FIPS 186 Digital Signature Standard and is in draft ANSI X9.30 Part 1 Digital Signature. The DSS private key is used for digital signature generation and the DSS public key is used for digital signature verification. The size of a DSS digital signature is always 320 bits.

2.3.15 Security Management, Audit and Policy

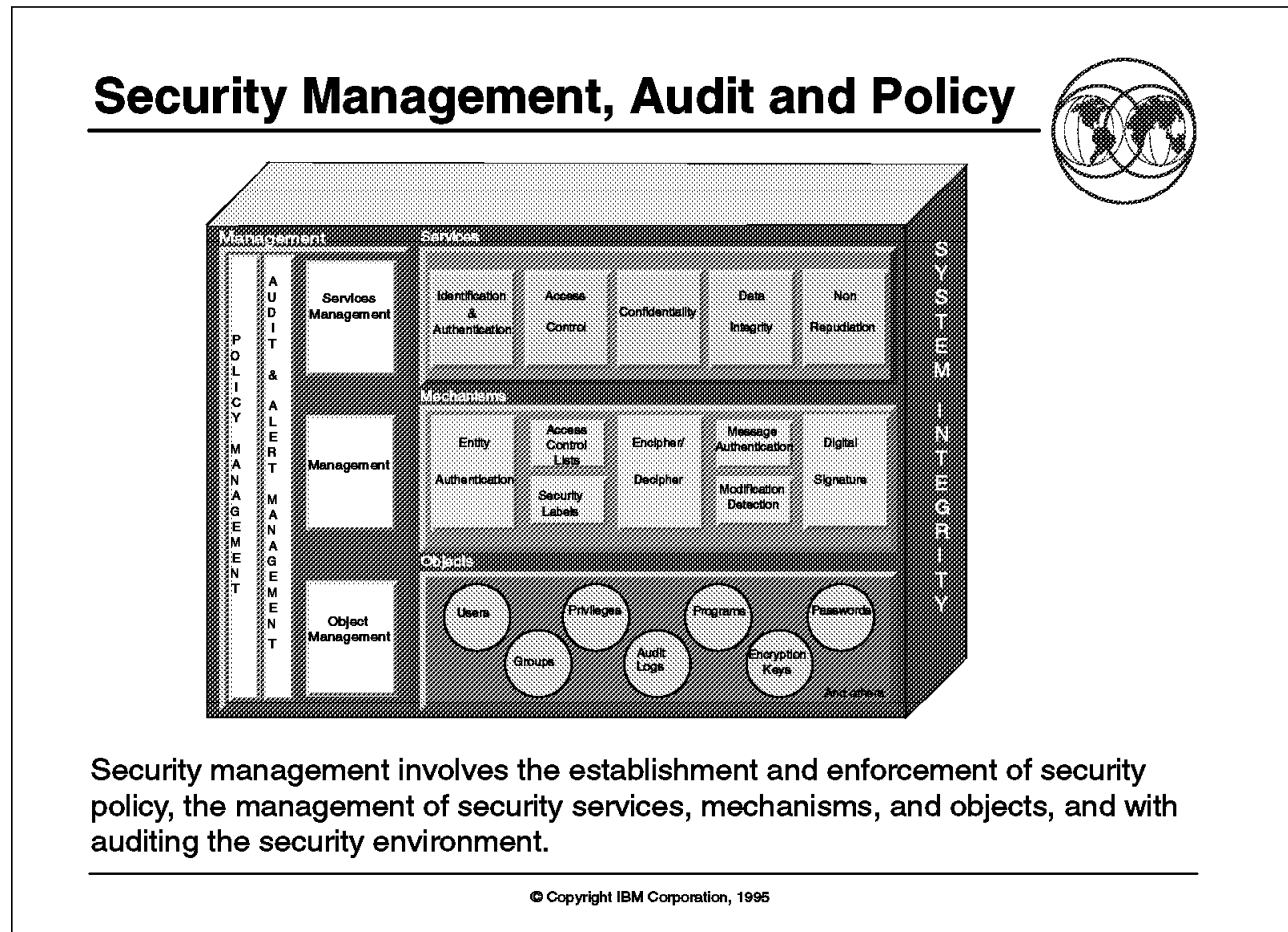


Figure 30. Security Management, Audit and Policy

Key Points

- Security management is defined as part of the IBM SystemView Business Discipline.
- Security Management is the administration, control and review of an enterprise's security policy.
- Security managers make use of procedures and system security services to implement policies consistent with the organization's objectives.
- System audibility can provide checks and balances on system users, administrators, and operators.

Presentation Script

Security management involves the establishment and enforcement of security policy; the management of security services, mechanisms, and objects; and the auditing of the security environment. Today, in many cases, administrators must perform administrative tasks through multiple interfaces via multiple systems and subsystems. They are looking for a way to perform these tasks through a single interface without having to log on to multiple systems and subsystems. In addition, they want to be able to structure their security management around their business management organization. That is, some businesses need a

centralized management solution, others need a distributed solution, and others need some combination of the two.

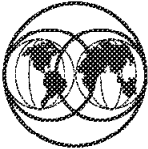
To protect against the generic set of security threats in the open environment, the ISO OSI Security Architecture Standard has specified a set of generic security services, a set of security mechanisms to implement those services, and an outline of security management functions to enforce the system security policies. Security management is a key component of overall system management, being one of the set of common management functions specified in the ISO OSI Management Standard. The other common management functions are configuration management, performance management, fault management, and accounting management.

Security management is a critical element of the IBM Security Architecture. It relates to all security services, mechanisms, and objects. In addition, the move toward a distributed system environment requires that a solution for security management be cross system in nature.

The strategy for security management calls for tools that will simplify the administrative tasks and provide a single system image of an organization's security systems. The approach for security management is to follow the strategic systems management approach that has been defined by the IBM SystemView Framework.

2.4 IBM Security Architecture Summary

IBM Security Architecture Summary



- System Integrity is required to ensure that Security Services based on ISO Standard 7498-2 are effective.
- Identification and authentication of all users and programs is the minimal base security service required. Most other services and the implementation of security policies are dependent on this service.
- Managed access control services are required in a centralized and distributed environment to ensure that resources are protected consistently.
- Confidentiality and Data Integrity services are essential, especially when using a network and distributed environment.
- Non-repudiation service is a major business requirement for Electronic Data Interchange (EDI) and the Internet.
- Security Management and Audit will move from System scope to Enterprise scope.
- Applications will invoke security mechanisms, using standard interfaces, to meet organizational policy.

© Copyright IBM Corporation, 1995

Figure 31. IBM Security Architecture Summary

Key Points

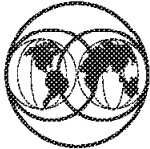
In order to implement effective enterprise-wide security, an installation needs to provide the fundamental services in IBM's security architecture.

Presentation Script

IBM's Security Architecture provides a set of security services, mechanisms, objects, and security management to provide a full set of security capabilities for user identification, authentication, access control, confidentiality, data integrity, non-repudiation, security administration and auditing, which support an enterprise's security policy. These facilities are all based on ISO Standard 7498-2.

2.5 IBM's Ongoing Commitment

IBM's Ongoing Commitment



- ❖ Security standards, interfaces and architectures are continuously being defined:
 - Framework - ISO
 - Mechanisms - ISO, ANSI
 - Protocols - X9, X12
 - Interfaces - X/Open, OSF, OMG, IETF, IEEE
 - Criteria - X/Open, NCSC, ITSEC, NIST
- ❖ Major IBM commitment to participate, contribute, adopt and implement these standards. For example:
 - Cryptography products supporting multiple platforms and encryption algorithms:
 - Data Encryption Standard (DES)
 - Public Key Algorithm (PKA) - RSA
 - Commercial Data Masking Facility (CDMF)
 - Open Edition on MVS
 - RACF enhancements to support Open Edition

© Copyright IBM Corporation, 1995

Figure 32. IBM's Ongoing Commitment

Key Points

IBM has an ongoing commitment to participate, contribute, adopt and implement the international security standards in the current IBM security products.

Supporting these security standards provides consistent interfaces that allow interoperability in multi-vendor open, client/server distributed computing environments.

IBM has adopted and implemented some of these standards in the current product line.

Presentation Script

Standards: Efforts are being made to incorporate the various security standards into the IBM strategy. However, most of the standards work has yet to mature. Given customer concern with providing security in mixed (multi-vendor) environments, it is important that products conform to open systems standards for security functions. Because there are multiple standards bodies at work defining different facets of security, IBM will encourage, through active participation, convergence to a single set of coherent standards. IBM has a continuing involvement with ISO, Open Systems Foundation (OSF**) and X/Open.

ISO is guiding many efforts to define the protocols that support the security architecture. A set of standards is being developed in various ISO work groups that address upper and lower layer models, OSI security management framework, security services framework, and OSI security services definition and protocol specification.

In addition to the ISO standards efforts, there are a number of other groups preparing security standards. Among these are:

- American National Standards Institute (ANSI)
- European Computer Manufacturers Association (ECMA)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Telegraph and Telephone Consultative Committee (CCITT)
- National Institute of Standards and Technology (NIST)
- Internet Engineering Task Force (IETF)
- Open Software Foundation (OSF)
- X/Open

X/Open is an independent world-wide, open systems organization who's mission is to bring users greater value from computing in open systems. X/Open's strategy is to combine existing and emerging standards into an open system environment which is:

- Comprehensive
- Integrated
- Of high value
- Usable

X/Open Specifications are:

- Common Application Environment (CAE) Specifications

CAE specifications are the stable specifications that form the basis for X/Open-branded products. These specifications are intended to be used widely within the industry for product development and procurement purposes.

Anyone developing products that implement an X/Open CAE can enjoy the benefits of a single, widely supported standard.

- Preliminary Specifications

These specifications, which often address an emerging area of technology and consequently are not yet supported by multiple sources of stable conformant implementations, are released in a controlled manner for the purpose of validation through implementation of products. A preliminary specification is not a draft specification. In fact, it is as stable as X/Open can make it, and on publications has gone through the same rigorous X/Open development and review procedures as a CAE specification.


Implementation of Standards: Examples of where IBM has incorporated standards into products include:

- Cryptography products supporting multiple platforms and encryption algorithms:
 - Data Encryption Standard (DES)
 - Public Key Algorithm (PKA) supporting RSA
 - Commercial Data Masking Facility (CDMF)

- Open Edition on MVS
- RACF enhancements to support Open Edition

2.5.1 Standards, Interfaces and Architectures

Standards, Interfaces and Architectures



IBM is working closely with acknowledged consortiums world wide in helping develop and define key Standards, Application Interfaces and Architectures:

- **GSS-API (Generic Security Service API) - International Engineering Task Force (IETF)**
 - ▶ X/Open intends to endorse this standard. Common Application Environment (CAE) Specification expected late 95. Work commenced on this standard in 93/94.
- **GCS-API (Generic Cryptographic Service API) - X/Open**
 - ▶ X/Open intends to publish a Preliminary Specification by late 95 and a company review draft (public) in 96. Work commenced on this standard in 94.
- **GAS-API (Generic Audit Service API) - X/Open**
 - ▶ X/Open intends to publish a 2nd draft 3Q 95, and a Preliminary Specification by early 96. Work commenced on this standard in March 95.
- **SM-API (System Management API) - X/Open**
 - ▶ Proposal has been put forward. Resources are yet to be assigned to this standard by X/Open Consortium.
- **AC-API (Access Control API) - X/Open**
 - ▶ No proposal has yet been formally submitted.

© Copyright IBM Corporation, 1995

Figure 33. Standards, Interfaces and Architectures

Key Points

IBM is working closely with many standards organizations to define standard consistent security application programming interfaces for security services, access control, cryptography, audit and systems management.

Presentation Script

GSS-API: Purpose - to provide a standard API to certain communication oriented security services.

Implementation of GSS-API:

- Together with cryptographic algorithms and protocols, permits callers portability and interoperability
- Counters a range of vulnerabilities that may affect the security of communication between applications in open networks

GSS-API Goals:

The GSS-API design assumes and addresses several basic goals, including:

- Mechanism independence

The GSS-API defines an interface to cryptographically-implemented strong authentication and other security services at a generic level that is independent of particular underlying mechanisms. For example, services provided by GSS-API can be implemented by secret-key technologies (for example, Kerberos), or public-key approaches (for example, X.509).

- Protocol environment independence

The GSS-API is independent of the communication protocol suites with which it is employed, permitting use in a broad range of protocol environments.

- Protocol association independence

The GSS-API's security context construct is independent of communication protocol association constructs. This characteristic allows a single GSS-API implementation to be utilized by a variety of invoking protocol modules on behalf of those modules' calling applications. GSS-API services can also be invoked directly by applications, wholly independent of protocol associations.

GCS-API: Purpose - to cover services to support Cryptographic Aware callers.

Interface specification is to be provided for use by programmers who develop applications that rely on:

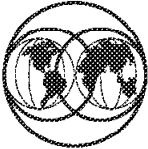
- General application cryptographic services
 - Integrity checkvalue generation and verification
 - Data encipherment and decipherment
 - Production of irreversible hash of data
 - Generation of random numbers
 - Inquiry of available keys and key related data
- Key management services
 - Generation, derivation and deletion of key
 - Export, import of keys
 - Storage and retrieval of keys
 - Archive and retrieval of keys

GAS-API: High-level requirements include:

- Support of stand-alone and distributed systems
- Define what data should be recorded
- Support integrity, confidentiality and separation of duties
- Define standard format for security event messages
- Meet user group requirements for consistency, usability and configurability

2.5.2 Standards, Interfaces and Architectures (continued)

Standards, Interfaces and Architectures (continued)



- **OSSA (Object Security Service Architecture) - Object Management Group**
 - ▶ IBM submitted a proposal in 94.
- **MSFR (Minimum Security Functionality Requirements) - NIST**
- **XBSS (X/Open Baseline Security Services) - X/Open**
 - ▶ Security Branding Draft available for Company Review. CAE specification expected late 95. Work commenced on this in 93.

© Copyright IBM Corporation, 1995

Figure 34. Standards, Interfaces and Architectures (continued)

Key Points

IBM is working closely with many standards organizations. IBM played a leadership role in helping to define X/Open's XBSS Security Branding process and the OMG Object Security Service Architecture.

Presentation Script

OSSA: IBM submitted the Object Security Service Architecture proposal to the Object Management Group in 1994. It is currently under review.

MSFR and XBSS: Industry concerns over the lack of harmony among various national evaluation criteria and their emphasis on the security needs of the military/intelligence communities have led to the development of sets of security requirements by commercial organizations.

In 1990 a document called the Commercial International Security Requirements (CISR) was published by Ken Cutler of The American Express Travel Related Services and Fred Jones of the Electronic Data Systems Corporation. The CISR was adopted by the International Information Integrity Institute (I-4). Somewhat in parallel, Bellcore was developing its Standard Operating Environment Security

Requirements so that all system procurements could specify a consistent level of security. These two documents were used by the National Institute of Standards and Technology (NIST), along with the Orange Book functionality criteria, to produce the Minimum Security Functionality Requirements (MSFR) for commercial systems. The MSFR was to be published as a FIPS but instead became absorbed into the functionality requirements part of the Federal Criteria and subsequently the Common Criteria.

Following the publication of the MSFR, the European Computer Manufacturers Association (ECMA) derived the Commercially Oriented Functionality Class (COFC) as an ECMA Standard to be used as a sample Functionality Class for evaluations under the ITSEC.

Recently the X/Open Security Working Group has been working on the concept of extending its software branding process to perform security branding. Security branding would initially be limited to XPG3 or XPG4 compliant systems and would be based on the X/Open Baseline Security Services (XBSS), which is defined in the form of the functionality part of a Protection Profile and built from the security functionality components defined in the Federal criteria. XBSS is defined as the minimum security services needed by interconnected commercial systems. These services allow installations to run secure systems by default and implement reasonable security policies to protect their assets against minimal risks at reasonable cost. The assurance gained from an X/Open Security Branded system would be based on supplier testing and declaration of compliance with XBSS requirements, backed up by the warranty contained in the Trade Mark Licensing Agreement (TMLA) entered into with X/Open.

The X/Open Security Branding process has the potential of being much shorter and cheaper than a government-sponsored formal evaluation, yet should meet the security needs of the majority of commercial users. The European Security Forum and the I-4 are strongly supportive of the X/Open initiative and are working closely with X/Open to ensure that the effort is successful. The Preliminary Specification for XBSS underwent X/Open Company Review in April and May of 1995, and, should the X/Open business considerations be satisfied and the Security Branding process be successfully created, trial Security Branding may begin in 1996.

IBM has played an active role in critiquing the MSFR and working with ECMA and X/Open in the creation of the COFC and the XBSS. IBM is thus well positioned to address the security needs of commercial systems through these standards, should our users express sufficient interest.

2.6 Related Strategies and Architectures

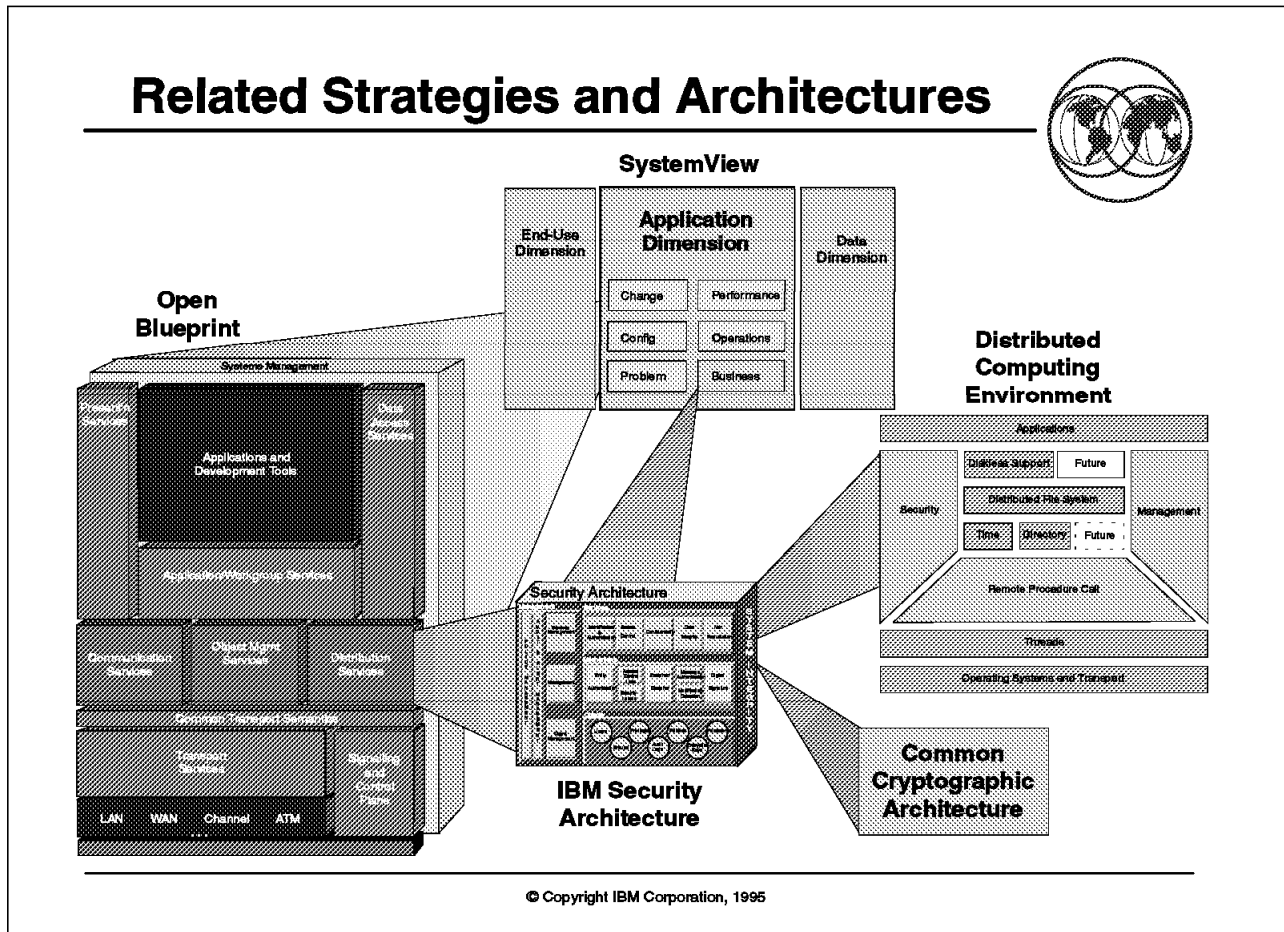


Figure 35. Related Strategies and Architectures

Key Points

This foil depicts the structure of the IBM's Security Architecture with respect to other IBM strategies and architectures.

Presentation Script

This chapter presents overviews of the role security plays in the key IBM strategies and architectures including:

- IBM Open Blueprint
- DCE Security Services
- IBM Object Oriented Programming Security
- IBM System Management Strategy
- IBM Information Warehouse Architecture
- IBM Security Evaluation Strategy

2.6.1 IBM's Open Blueprint

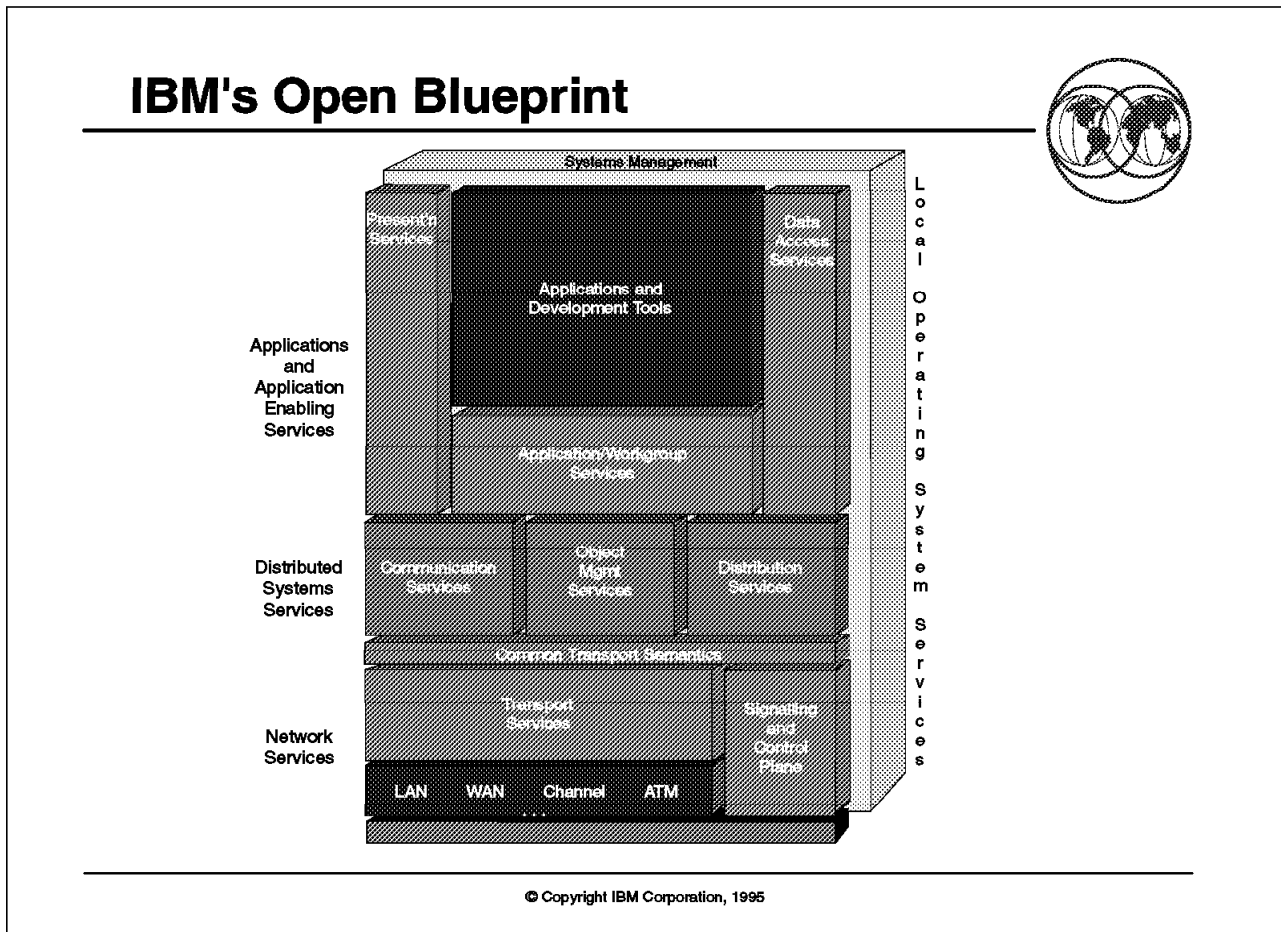


Figure 36. IBM's Open Blueprint

Key Points

This picture depicts the components of Open Blueprint. The Security Service is a key component of the Distribution Services which is based on the DCE security standards.

Presentation Script

The Open Blueprint is a standards-based architecture that defines the services required by applications in a distributed multivendor environment.

The Open Blueprint addresses the challenges of the open environment by viewing a system as part of a distributed network and viewing the network as if it were a single system.

The Open Blueprint serves four major roles:

- It helps customer develop their own architecture and organize products and applications in an open, distributed environment.
- It informs customers, software vendors, consultants, system integrators and service providers about IBM's directions for product and solutions.

- It guides developers as they meet customers' needs by supplying products and solutions that include the appropriate functions and that can be integrated and can interoperate with other installed products.
- It provides a context for the incorporation of new technologies into a distributed environment.

The structure of the Open Blueprint allows the network of operating systems to function as a unit, as a *network operating systems*. A network operating system is made up of multiple systems that are separated from each other and are connected by a communication network. In this network operating system, each individual system logically contains the services briefly described below. However, it is not necessary for each individual system to contain all the services included in the Open Blueprint.

Just as an operating system provides the management of resources on a single system, a network operating system provides for the management across the network of the same types of resources: files, databases, printers, transactions, software packages, documents, jobs, and so on.

As depicted in the foil, there are several sets of resource management services in the Open Blueprint:

Network Services

- *Common Transport Semantics* support protocol independent communication in distributed networks.
- *Transport Services* provide the protocols for transporting information from one system to another, such as SNS/APPN, TCP/IP, OSI, NETBIOS, and IPX.
- *Subnetworking* provides functions dealing with specific transmission facilities, such as LANs, WANs, channels, Asynchronous Transfer Mode (ATM) and emerging technologies such as wireless.
- *Signalling and Control plane* provides the ability to establish subnetwork-specific connections.

Distributed System Services

- *Communication Services* provide mechanisms for parts of a distributed application or resource manager to talk to each other.
- *Object Management Services* provide transparent access to local and remote objects.
- *Distribution Services* assist the communication between parts of distributed applications and resource managers by providing common functions such as a directory and security.

The *Security Service* protects network resources from unauthorized use by registering users and their authorization levels, by authenticating users, and by auditing access.

Application Enabling Services

- *Presentation Services* define interaction between applications and the user.
- *Application/Workgroup Services* are common functions, such as mail, which are available for use by all applications.

- *Data Access Services* allow applications and resource managers to interact with various types of data.

System Management: provides facilities for a system administrator or automated procedures to manage the network operating system.

Local Operating System Services: operate within the confines of a single system in a network. Examples of local services are managing memory, dispatching work, and local security logon.

Development tools: help the application developer implement distributed applications that uses standard interfaces.

The Open Blueprint provides guidelines for the integration of multivendor systems and the simplification of the more cumbersome aspects of distributed computing, such as multiple logons, multiple passwords, and unique application directories for locating resources. Products that align with the Open Blueprint provide designated interfaces and protocols.

The Open Blueprint includes interfaces and protocols from IBM and other industry sources. Those from industry sources are broadly accepted standards. Many of these standards are the same ones included in X/Open's Distributed Computing Services (XDCS) Framework and OMG's Common Object Services Specifications (COS).

The Open Blueprint describes techniques for building an open, heterogeneous, distributed system that is extensible by alternate component implementation and by support for evolving new technologies and functions. For example, the Open Blueprint currently supports three models for interprocess communications: Conversational, Remote Procedure Call (RPC), and Messaging and Queuing. If a fourth model were to be developed, it will be evaluated for inclusion.

Open Blueprint Security: In earlier centralized systems, the operating system authenticated the users' identities and authorized access to resources. Individual workstations in a network are not necessarily secure. Therefore, in a distributed environment, security operations must be performed by an independent set of services. Security in a distributed environment presents additional challenges, such as preventing eavesdropping, impersonation, and forgery.

The Open Blueprint security service specification lets administrators register users and resource managers, provides for the mutual authentication of client and servers, and enables resource managers to provide access to resources only to authorized users. The Open Blueprint security service also defines services for auditing user activity. These services include DCE specifications and incorporate and expand on the Kerberos specification from MIT.

These security services meet relevant X/Open and POSIX specifications.

For more information about Open Blueprint security, order *Security in the Open Blueprint* from the IBM Open Blueprint Reference Library (SBOF-8702).

2.6.2 DCE Security Services

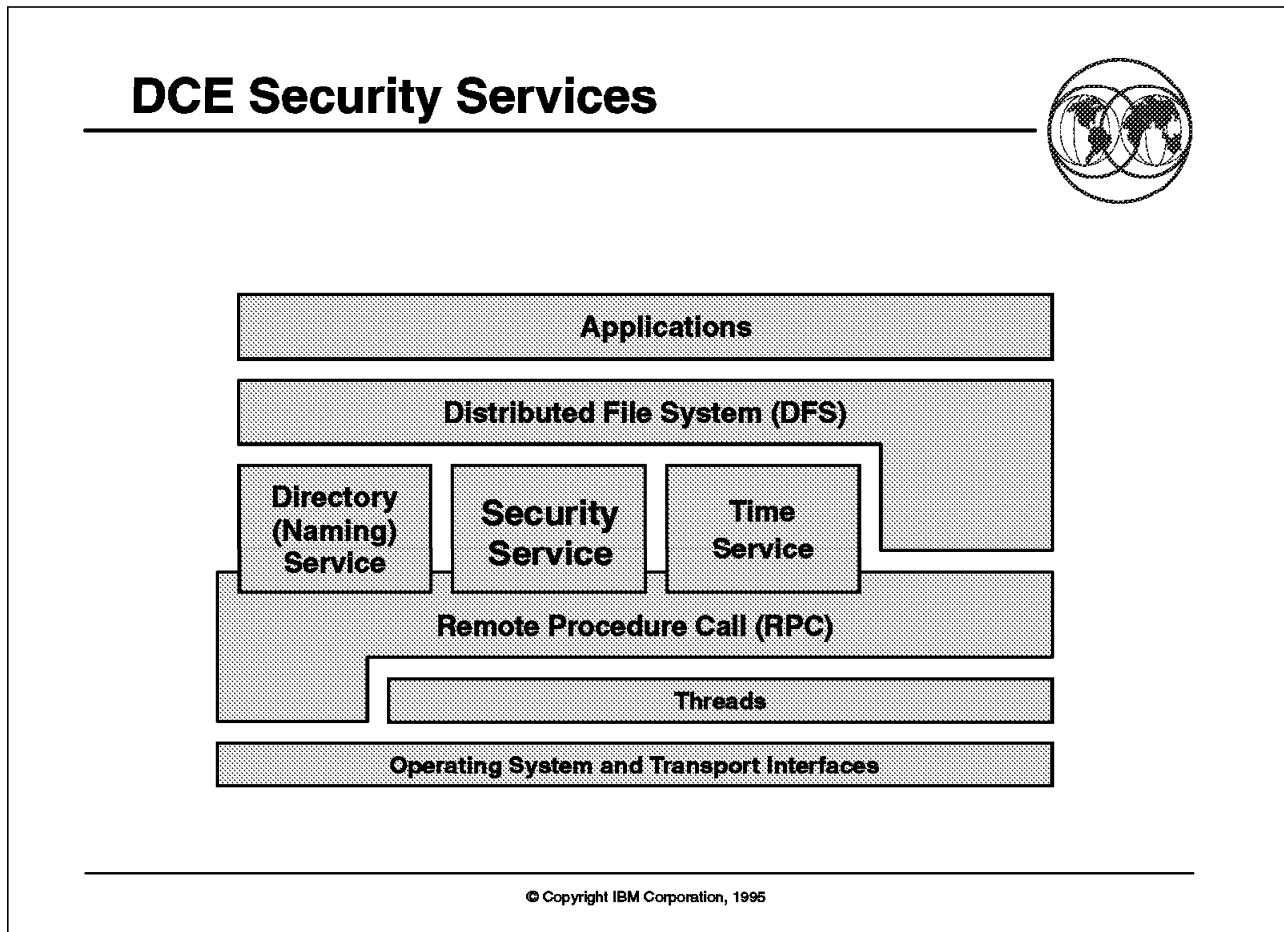


Figure 37. DCE Security Services

Key Points

- This foil depicts the OSF DCE architecture structure.
- DCE provides tools and services for distributed application support.
- DCE provides interoperability and portability across heterogeneous platforms.
- Security services support user identification, privacy/integrity of communications, access control and auditing.
- IBM is a leader in providing DCE technology in MVS, VM, AIX, OS/400 and OS/2.

Presentation Script

DCE provides the services that allow a distributed application to interact with a collection of heterogeneous computers, operating systems, and networks as if they were a single system. DCE has achieved wide acceptance in the industry. Because DCE technology was developed by Open Software Foundation (OSF), many of the world's leading software manufacturers are working on implementing DCE on their respective platforms. IBM is a leader in providing DCE services.

DCE's set of services is organized into two categories: *distributed programming facility* and *distributed services*.

The distributed programming facility includes:

- Remote procedure call
- Directory service
- Time service
- Thread service
- Security service

The distributed services include:

- Distributed file service
- Diskless support

DCE Security Service: To prevent unauthorized access to resources in a distributed environment, distributed services and applications must be able to securely identify users, guarantee the integrity and privacy of communications, and control access to resources in an orderly way. The distributed security mechanism provided in DCE not only performs these functions, but also allows for the distributed administration of the security network.

The DCE Security Service is comprised of several parts:

- The Authentication Service
- The Privilege Service
- The Registry Service
- The Access Control List Facility (ACL)
- The Login Facility
- The Audit Service
- The Key Management Facility
- The Principal ID Mapping Facility

For more information about DCE Security Services, refer to Chapter 4, "DCE Security" on page 111.

2.6.3 Object Oriented Security

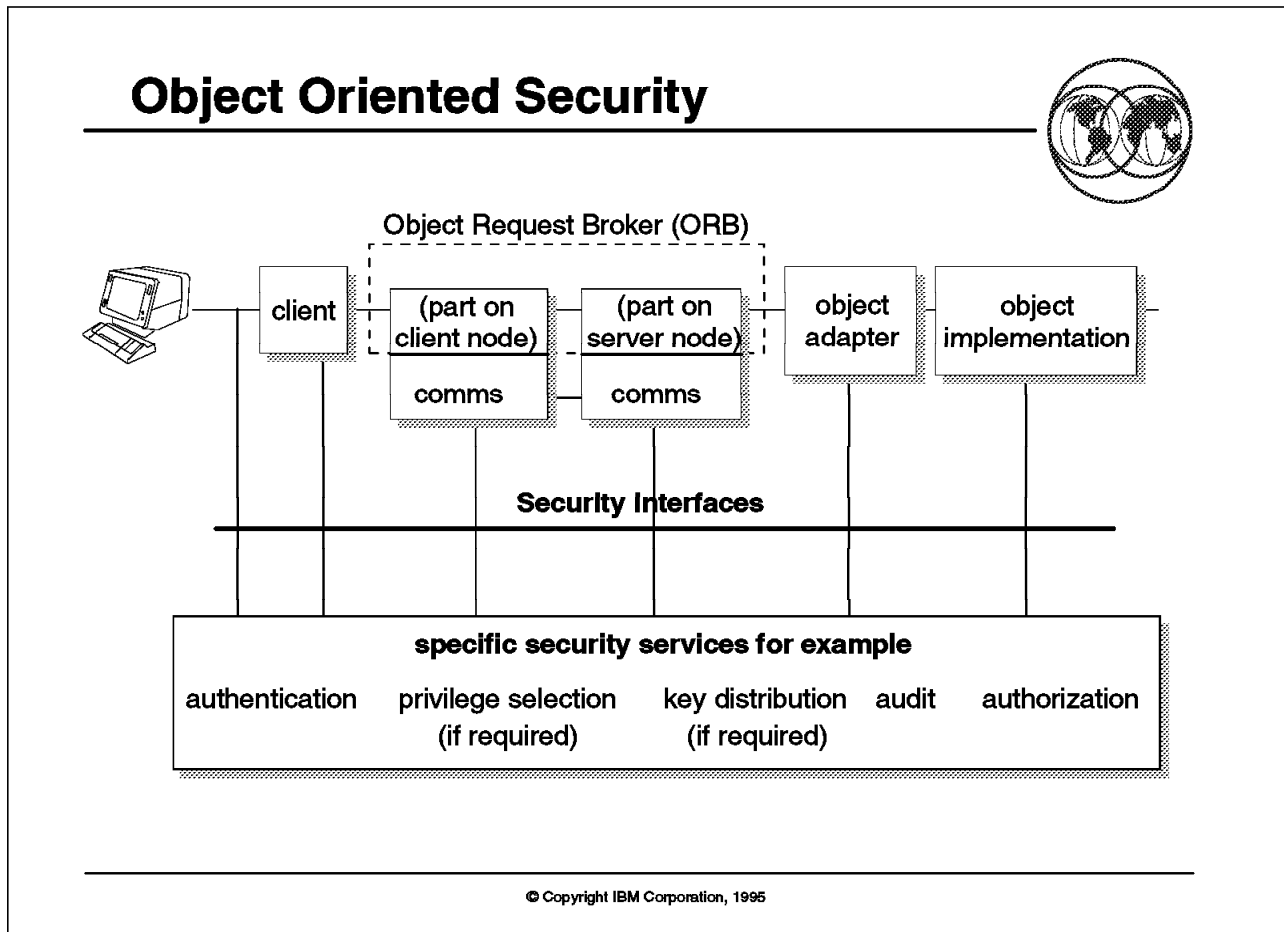


Figure 38. Object Oriented Security

Key Points

The foil depicts the logical flow of a user signing-on and then invoking objects, and how object system components use the security facilities.

IBM participates in the OMG security standards organization to develop the System Object Model and Distributed SOM.

Presentation Script

For many years, the programming community has been trying to improve the efficiency of the program development process. This objective could finally be reached through the use of Object Oriented Programming (OOP). The IBM strategy is to implement object oriented programming support on all of its strategic platforms in an interoperable and portable manner.

Overview of Object Systems: Some of the basic concepts of object-oriented computing are:

- An *object* is an entity in which we store *data* and *methods* (or programs) that process the data.

- An *object type* is a category of object of which an object is an *instance*.
- A *class* is a software implementation of an *object type* that specifies the *data structure* for each object in the class, and the permissible *methods* that can be invoked as a unit of work on the objects.
- *Encapsulation* means that the objects in a class can be manipulated only by the methods defined for that class.
- Objects can be built of other objects to produce complex objects that can be considered as a whole.
- Objects send *requests* to other objects to carry out an indicated operation and return the result.
- Class hierarchies may be used to build objects out of pre-existing objects by inheriting and reusing some or all of the data types and methods of these classes.

Overview of Security Architecture in Object Systems: In an object system environment the primary security requirement is to control access to objects. This requirement implies that users wishing to gain access to an object must be properly authenticated with their access rights established through identity, group membership, role definition, or privileges. At the same time, the object that the user or client wishes to access must have associated with it, some indication of the identification, group, role or privilege of legitimate users or clients.

When Object Oriented Programming is implemented within a single address space, then the fact that a user is authorized to operate within that space may be sufficient, such as in the case of early releases of SOM (IBM's System Object Model - the framework of IBM OOP offerings). Later versions, however, will include support for persistent objects, where the objects may be saved in a local shared file system, DB/2, or IMS, requiring some object access control.

When the user is executing from a client program in a different address space, or from a different node or computer domain, as in the case of DSOM (Distributed SOM), then object access control may become a requirement. Furthermore if the client/object message communication is via an untrusted network, then the questions of message origin authenticity, message integrity, and confidentiality become important.

Thus Object Oriented Programming DSOM security has much in common with security in distributed computing environments, and it is more desirable to use the security services of DCE for those enterprises that use DSOM within a DCE infrastructure. If security services other than those provided by DCE's Kerberos are to be used, then GSS-API, the generic security service interface in DCE 1.1, must be used to ensure application portability.

Where integration with DCE is not possible, then GSS-API will be used to invoke local platform services.

Security Requirements in Distributed Object Systems: A consortium of vendors known as the Object Management Group (OMG) is cooperating on a White Paper on security requirements for object programming.

The following is a summary of this White Paper on Security requirements:

- A consistent model facilitating application portability for new and legacy systems in distributed environments
- Scalable from small local systems to multiple large systems
- Business justifiable in terms of human and machine resources required to use and manage, when measured against security benefits
- Flexible in terms of level of functionality required to implement a range of security policies, in order to minimize overheads
- Compliant to government regulations and other standards and developed in a controlled and formal manner
- Portable to environments that support different security policies using generic security services for mechanism independence
- Supportive of object interoperability with systems that support different security policies, or none at all, or across heterogeneous systems using different communication protocols or security services
- Easy enough to set up, manage and use

Security Functional Requirements:

The primary security functional components required in an object system are at least the following:

- Identification and authentication
- Authorization and access control
- Security auditing
- Secure communication
- Encryption
- Secure administration

IBM Object Oriented Programming Security Solutions: IBM and Tivoli Systems Inc. have proposed an architecture to OMG, as have several other vendors. OMG is evaluating the various proposals and working toward an architecture that incorporates the features most common to these proposals that can gain a majority vote of approval.

IBM's proposal has been formulated to allow for compatible and interoperable security on all IBM OOP platforms (AIX/6000, MVS/ESA, OS/2 and OS/400 and the Enterprise Server), and a primary objective is that the architecture should be generic to be acceptable to non-IBM platforms and operating systems.

With respect to security solutions, implementation is being coordinated by the IBM Object Services Technology Center (OSTC)

A Simple Security Solution: There is a clear need to provide security solutions for non-DCE as well as DCE-based configurations. We will call the non-DCE solution the Simple Security Solution because it is based on two-party authentication rather than the three-party authentication of DCE.

Simple solutions can be used where the client-server communication link is private and trusted and where all users, once authenticated and authorized to access an application server, may access all objects in that server's class libraries. A simple security solution requires user identification and

authentication, using native security facilities via a generic security service interface, such as GSS-API.

A key requirement of simple security solutions is to utilize host specific security services via a generic API in order to conserve application portability and to allow any client-server platform combination.

A second key requirement of simple security solutions is that they must be implemented in such a way as to not preclude easy migration to a DCE-based security solution. This may be achieved by utilizing a generic security service interface such as GSS-API.

DSOM Security - A Comprehensive Solution: For DSOM implementations, integrated within a DCE infrastructure, authentication will be achieved using the three-party scheme provided by DCE.

The simple security solution limits authorization services to the determination of the right of a client to access a service application residing on a server.

Authorization for fine grain object/method/class library access control is complex for Object Oriented Programming in distributed environments, because in the Object Oriented Programming world, access rights are more than simply read, write, and execute; they can be anything that makes sense for the function performed by a particular method. In fact, they are role oriented.

Thus the access rights associated with the various methods that comprise various classes need to be defined and tabulated. They are called the Method Required Access Rights (MRAR). Also, the rights for users and groups of users to access particular methods also need to be defined and tabulated. They are known as the Capability Access Rights (CARs). These requirements could result in huge matrices of rights information and costly computation at run time. So significant savings can be achieved by assigning objects to object groups and associating Access Control Factors (ACFs) with those groups. Thus users or user groups can have their CARs defined in terms of ACFs: a set of capability rights to use against any objects in a particular object group.

The right of a client (on behalf of a user) to perform a method request on an object is then determined by testing that the MRARs are contained in the client's CARs.

This architecture is still in the process of evolution, but the challenges are understood, and a generic model is emerging as part of the joint IBM/OMG efforts to gain consensus.

2.6.4 System Management (SystemView)

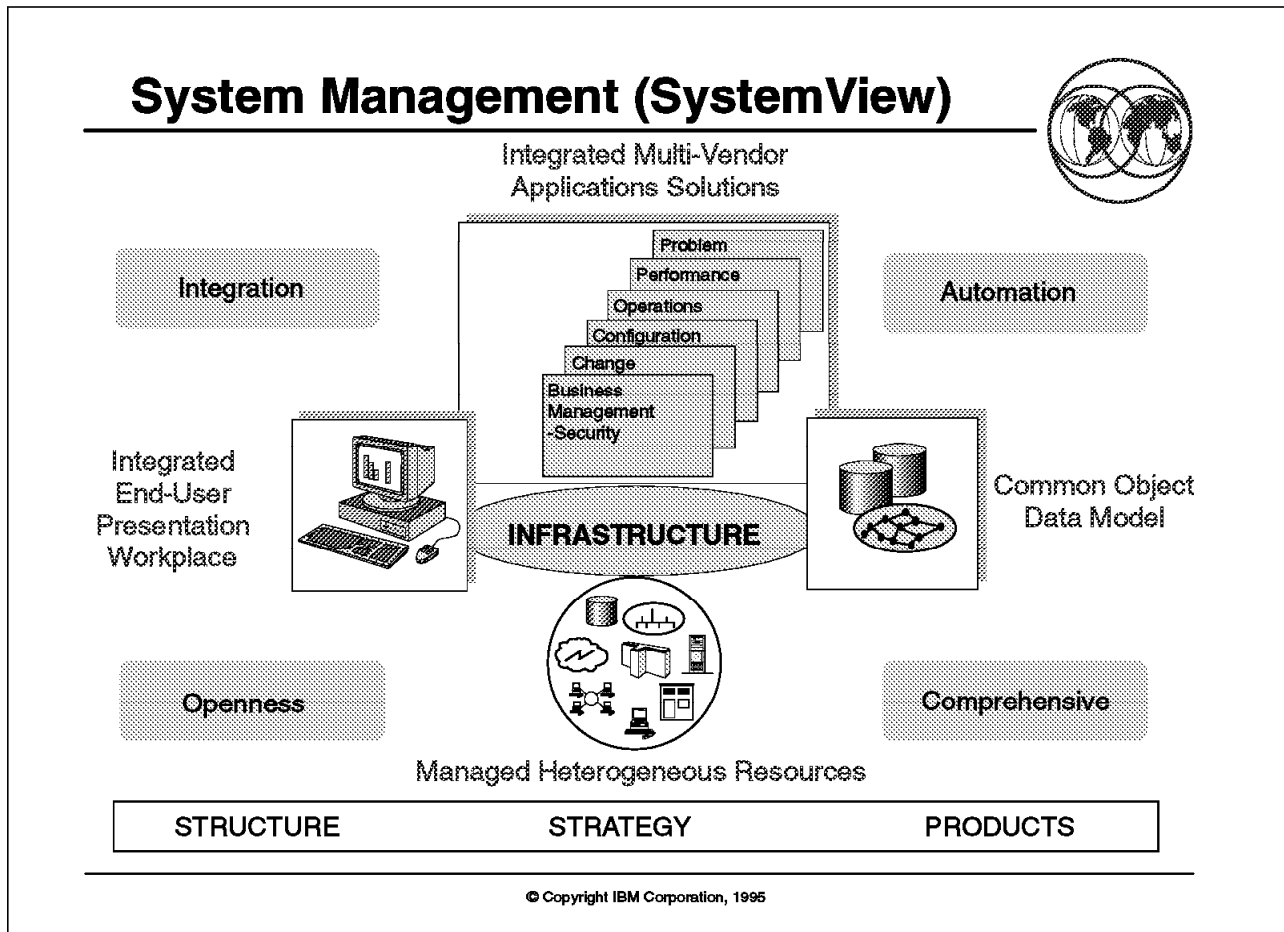


Figure 39. System Management (SystemView)

Key Points

This foils depicts the four dimensions in the SystemView structure, tied together by an infrastructure. Security is part of the business management dimension.

Presentation Script

SystemView is IBM's solutions to the customers' problems managing their increasingly complex multi-platform, multi-vendor, heterogeneous networked information technology environments. While it was once a conceptual framework to position systems management products, today is an evolving open, object oriented, standard based architecture supported by a set of products and services providing integrated solutions to customers' systems management problems.

IBM has based the SystemView structure on existing and emerging standards. It is open in order to allow portability and flexibility in extending systems management to the various proprietary platforms and operating systems by enabling multi-vendor management.

The SystemView structure has four dimensions, tied together by an infrastructure:

- The *End Use Dimension* or “integrated end-user presentation workplace” describes the services and application program interfaces (APIs) for providing a user interface to system management.
- The *Application Dimension* or “integrated multi-vendor applications” prescribes applications to automate management of all general system resources such as databases, networks, storage, systems, applications, and administrative resources.

The Application Dimension includes six disciplines:

- Business Management
 - Change Management
 - Configuration Management
 - Operations Management
 - Performance Management
 - Problem Management
- The *Data Dimension* or “shared data” describes and supports the data needs of systems and networks, allowing sharing of systems management data among all SystemView components.
 - The *Managed Resource Dimension* or “managed heterogeneous resources” describes the integration of the resources, assisting in producing systems management applications that can be shared across multiple resources of similar types.
 - The *SystemView Infrastructure* defines the techniques, standards, and services that enable interactions and exchanges among all elements of the SystemView structure. It includes protocols, common services, APIs, and other technology selections.

IBM’s goal for SystemView includes four objectives for the implementation of its dimensions, disciplines, and infrastructure:

- End-to-end management
- Open access
- Integrated application and services
- Automation

Security Management with SystemView: SystemView’s Security Management function is focused on performing security administration tasks and providing a single system image of the entire security system. Other security functions are provided by applications and operating systems using the functions included in the operating system themselves, or in the SystemView infrastructure. These services are basically identification and authentication, access control, confidentiality, data integrity and non-repudiation.

The basis for providing SystemView Security Management will be the Distributed Security Manager family.

For more information about SystemView and IBM products, see Chapter 9, “Security Management” on page 199.

2.6.5 Information Warehouse

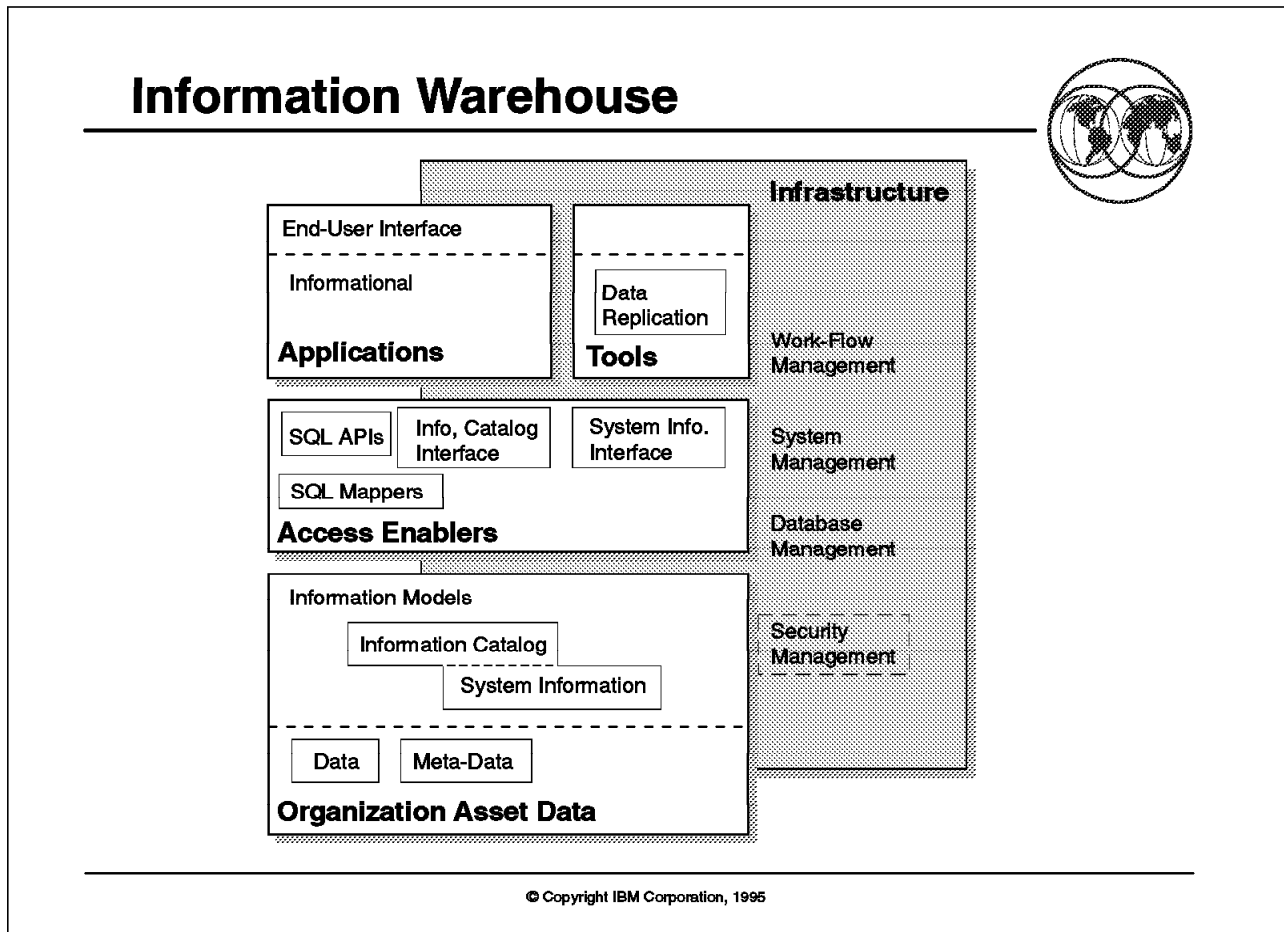


Figure 40. Information Warehouse

Key Points

This foil shows the general structure of the Information Warehouse Architecture. Security management is part of the common services offered by the infrastructure.

Presentation Script

The IBM Information Warehouse (IW) architecture provides a unifying and technical approach for building products and services that interoperate with each other to make it easy for customers to access data anywhere in their enterprises.

The Information Warehouse provides a lot of capabilities in support of informational applications and their end users (known as knowledge workers):

- Information provided to end users about what data is available and how to access them
- A programming interface to formatted relational and non-relational data to facilitate the development of informational applications
- Location-transparent direct access to herogeneous data

- Periodic extracts of heterogeneous data (typically into relational tables) for access by multiple end users
- Creation and refresh of reconciled and derived data
- Update of reconciled or derived data via data changes
- Distribution of data to multiple locations
- Integration of the administration of the above capabilities

The Information Warehouse architecture is composed of five major components, each corresponding to a box in the IW architecture foil:

- *Applications*

This box shows informational application with an end-user interface. The IBM Visualizer family of products is an example of such applications. It enables business professionals to access and analyze data in an IW implementation, bringing them to the end user for preplanned reporting and for active data analysis. The most relevant area of security for an informational application is identification and authentication. The informational application must be able to identify an end user and pass that information on to the database management systems that own the data to be accessed. The Visualizer products perform identification and authentication, and authorization functions through the native operating system and the database management systems.

- *Tools*

This box shows generalized data replication tools used for moving/transforming data among the variety of organization asset data defined in the IW architecture (for instance, real-time data, and reconciled, change or derived data). These tools include extractors, loaders, file transferers, data converters, and so on. The IBM DataHub product and the IBM Data Replication family of products work together in support of data replication management in an IW implementation. The DataHub product is a database administration tool that provides an interface with single point of control for administering relational databases un an enterprise. The native operating systems and the management systems on which DataHub is running are used to perform the identification and authentication, and authorization functions for DataHub administration requests.

- *Access Enablers*

This box provides access to the organization asset data by informational applications and tools via the SQL application programming interface. The DB2 family is an example of products that support the SQL application program interface. They support a common set of SQL calls and extensions to support specific characteristics of that DB2 product on the specific operating system the DB2 product runs on. DataJoiner is an example of a product for accessing both relational and non-relational databases.

- *Organization Access Data*

This box is composed of two elements: "data" and "meta-data." "Data" is the storage for the actual real world data, and "meta-data" is the storage for the models of the data (Information models). The information models contain the information catalog and system information, which are key components of the IW architecture. The physical data is stored on a variety databases, relational and non-relational. The DB2 family of products are examples of relational databases that provide storage for and organization's asset data.

The IBM DataGuide is an example of product that provides the “meta-data.” It helps informational workers find the right data using a graphical user interface. Identification and authentication, and authorization still rely upon the native operating system and the database management systems.

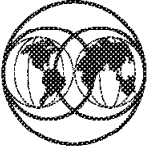
- *Infrastructure*

This box contains the components used at or by the other components previously described. The functions available are:

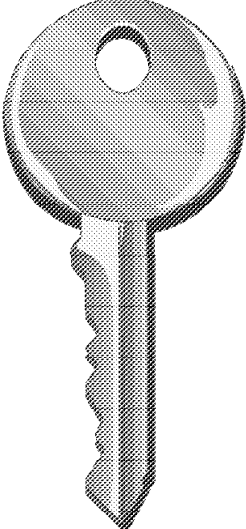
- Work-Flow Management
- System Management
- Database Management
- Security Management

2.6.6 IBM Common Cryptographic Strategy

IBM Common Cryptographic Strategy



- Fundamental to all Security Services
- Common Cryptographic Architecture (CCA)
 - ▶ Common API for Multiple Platforms:
 - Authentication
 - Confidentiality
 - Data Integrity
 - Non-Repudiation
 - Key Management
 - PIN Management
 - ▶ Supports Multiple Encryption Algorithms:
 - Data Encryption Standard (DES)
 - RSA Public Key Algorithm (PKA)
 - Commercial Data Masking Facility (CDMF)



© Copyright IBM Corporation, 1995

Figure 41. IBM Common Cryptographic Strategy

Key Points

This foil shows the “key” services provided by the IBM Common Cryptographic Architecture, which supports the DES, CDMF, and PKA algorithms to provide consistent cryptographic services across the IBM platforms.

Presentation Script

Today, the risk of losing the competitive advantage and market share through industrial espionage or from not protecting sensitive information, is increasing steadily. Not only is confidentiality important, but also the integrity of information. Commercial enterprises send contracts, private documents, money orders, and so on across communications networks. Prior to the electronic age, paper, signatures, and seals were used to guarantee the integrity of a document. Now, with electronic communication of information, new technological security mechanisms are required.

Cryptography is the only known practical method of protecting information transmitted electronically through communications networks. It can also be an economical way to protect stored information.

The use of cryptography provides many data handling capabilities such as data confidentiality, data integrity, authentication, and electronic signatures.

The IBM Common Cryptographic Architecture defines a set of cryptographic functions, external interfaces, and a set of key management rules. These provide a consistent, end-to-end cryptographic architecture across different IBM platforms such as MVS, VM guests, AIX, OS/400, S/88, OS/2, and DOS.

The Common Cryptographic Architecture defines services for:

- *Data Integrity*
- *Data Confidentiality*
- *Non-Repudiation*
- *Personal Authentication*
- *PIN Management*
- *Key Management*

The IBM Transaction Security System and the IBM Integrated CRyptographic Facility (IBM ICRF) with its supporting Integrated Cryptographic Services Facility/MVS (ICSF/MVS) conform to the IBM CCA Application Programming Interface (API).

Cryptographic Algorithms: Cryptographic algorithms are categorized as either symmetric key (secret key) or asymmetric key (public key) algorithms with different usage attributes, security capabilities and performance characteristics.

In a symmetric key algorithm, both the sender and the recipient know the single secret key and must maintain the integrity and confidentiality of the key value. Examples of symmetric key algorithms are the Data Encryption Algorithm (DEA) and the exportable Commercial Data Masking Facility (CDMF).

An asymmetric algorithm has a unique pair of keys consisting of one public key, which can be known by everyone, and one private key that is kept in the secure environment of the owner. A digital signature can be created using the private key such that this digital signature can be verified by everybody who knows the appropriate unique public key, but it cannot be recreated without access to the private key. Examples of asymmetric key algorithms are the Rivest Shamir Adleman (RSA) algorithm and the Digital Signature Standard (DSS).

IBM Cryptographic Strategy: The IBM Cryptographic Strategy is to provide cryptographic products driven by the requirements of the market, which are standards-compliant, open-systems solutions, capable of exploiting the advantages of both symmetric and asymmetric cryptography. IBM is very active in the standards arena and in the X/Open working group designing the Generic Cryptographic Services Application Programming Interface (GCS-API).

For further information about Cryptography refer to Chapter 6, "Cryptographic Security" on page 149.

2.6.7 Security Evaluation Strategy

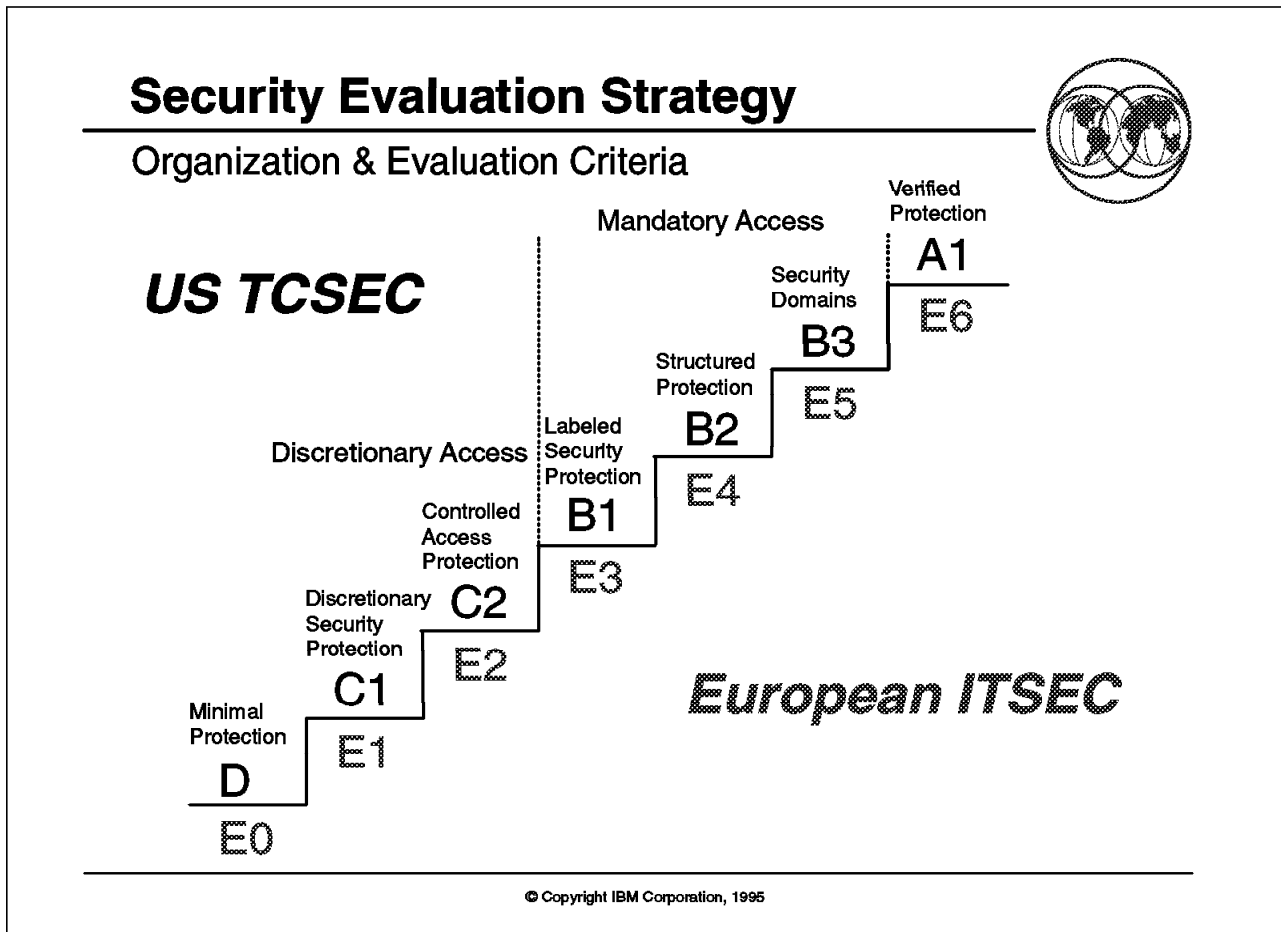


Figure 42. Security Evaluation Strategy

Key Points

This foil shows the TCSEC security criteria, the evaluation classes and the intended correspondence between them and the ITSEC classes.

The following IBM products have been evaluated or designed to meet the given evaluation classes:

- MVS/ESA with RACF evaluated at B1
- VM/SP with RACF evaluated at C2
- VM/ESA with RACF designed to meet B1
- OS/400 evaluated at C2
- AIX/6000 designed to meet C2
- PR/SM evaluated at E4
- CMW for AIX evaluated at E3

Presentation Script

US TCSEC or “Orange Book” criteria: The US DoD was the first institution to investigate the risks arising from using IT, and they came up with a set of criteria developed to serve several purposes:

- To provide a standard to manufacturers regarding what security features were to be built into their new and planned commercial products
- To provide DoD components with a measure by which to evaluate the degree of trust that could be placed in computer systems for the secure processing of classified or sensitive information
- To provide a basis for specifying security requirements in government purchasing specifications

The TCSEC criteria are divided into four divisions: D, C, B, and A, that are ordered in a hierarchical manner, with the highest division, A, being reserved for systems providing the most comprehensive security. Within divisions C and B there are several subdivisions known as classes. The classes are also ordered in a hierarchical manner, with systems representative of division C and lower classes of division B being characterized by the set of computer security mechanisms that they possess. Assurance of correct and complete design and implementation for these systems is gained mostly through testing the security-relevant portions of the system, which are known as Trusted Computer Base (TCB).

Systems representative of higher classes in division B and division A derive their security attributes more from their design and implementation structure. The assurance that the required features are operative and correct under all circumstances is gained through progressively more rigorous analysis during the design process.

European ITSEC criteria: The ITSEC is the harmonized version of the national criteria of France, the Netherlands, the United Kingdom, and Germany. Essential elements from the Orange Book were taken as the basis for ITSEC, but there are some aspects in the European criteria that are not mentioned in the TCSEC criteria. While the Orange Book mainly addresses the “confidentiality,” the notions of “integrity” and “availability” were enhanced in the ITSEC criteria.

IBM’s approach: IBM’s approach to formal government managed evaluations of security products is based strictly on the business case for each candidate product and the countries in which the highest demand for a product can be demonstrated. If a European Community country shows a demand for an E3 evaluation, then IBM will conduct an ITSEC based evaluation in that country. If a sufficient demand for a B1 level product is found among U.S. government agencies and aerospace contractors, then IBM will request a TCSEC based evaluation.

In other cases, users will expect the systems they purchase to include the basic security features, but will not require formal evaluation. In this case, IBM will announce that the product will meet C2 functionality requirement, but without formal evaluation.

The IBM products that have been evaluated or designed to meet the evaluation classes are:

- MVS/ESA with RACF evaluated at B1

- VM/SP with RACF evaluated at C2
- VM/ESA with RACF designed to meet B1
- OS/400 evaluated at C2
- AIX/6000 designed to meet C2
- PR/SM evaluated at E4
- CMW for AIX evaluated at E3



Figure 43. Platform Security

3.1 Platform Security Support Overview

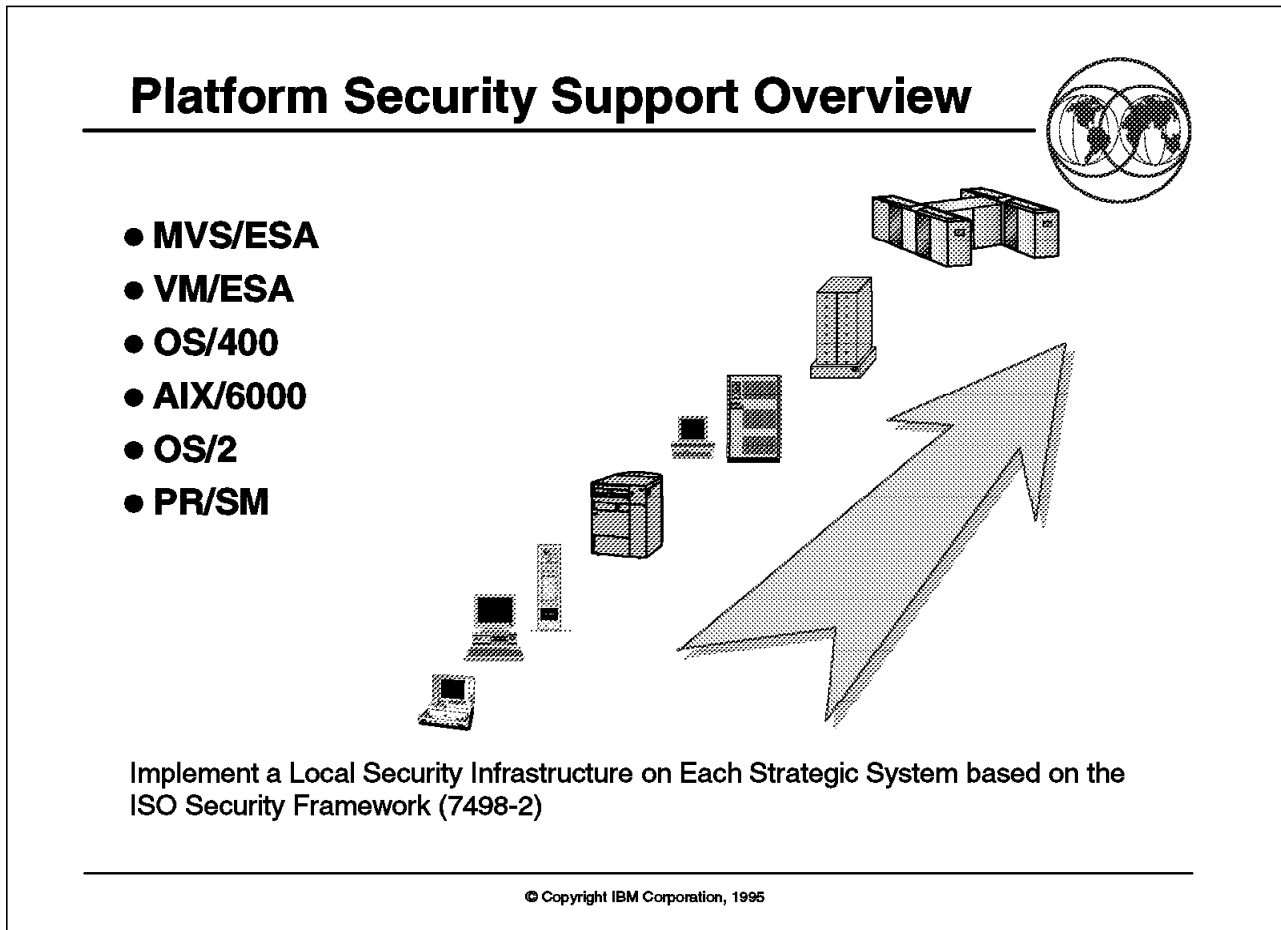


Figure 44. Platform Security Support Overview

Key Points

IBM's strategy is to implement a local security infrastructure on each strategic platform based on the IBM Security Architecture.

This chapter summarizes the security available on the key system platforms including: MVS, VM, RACF, SAF, OS/400, AIX/6000, OS/2 and PR/SM.

3.2 MVS/ESA

3.2.1 MVS/ESA and RACF

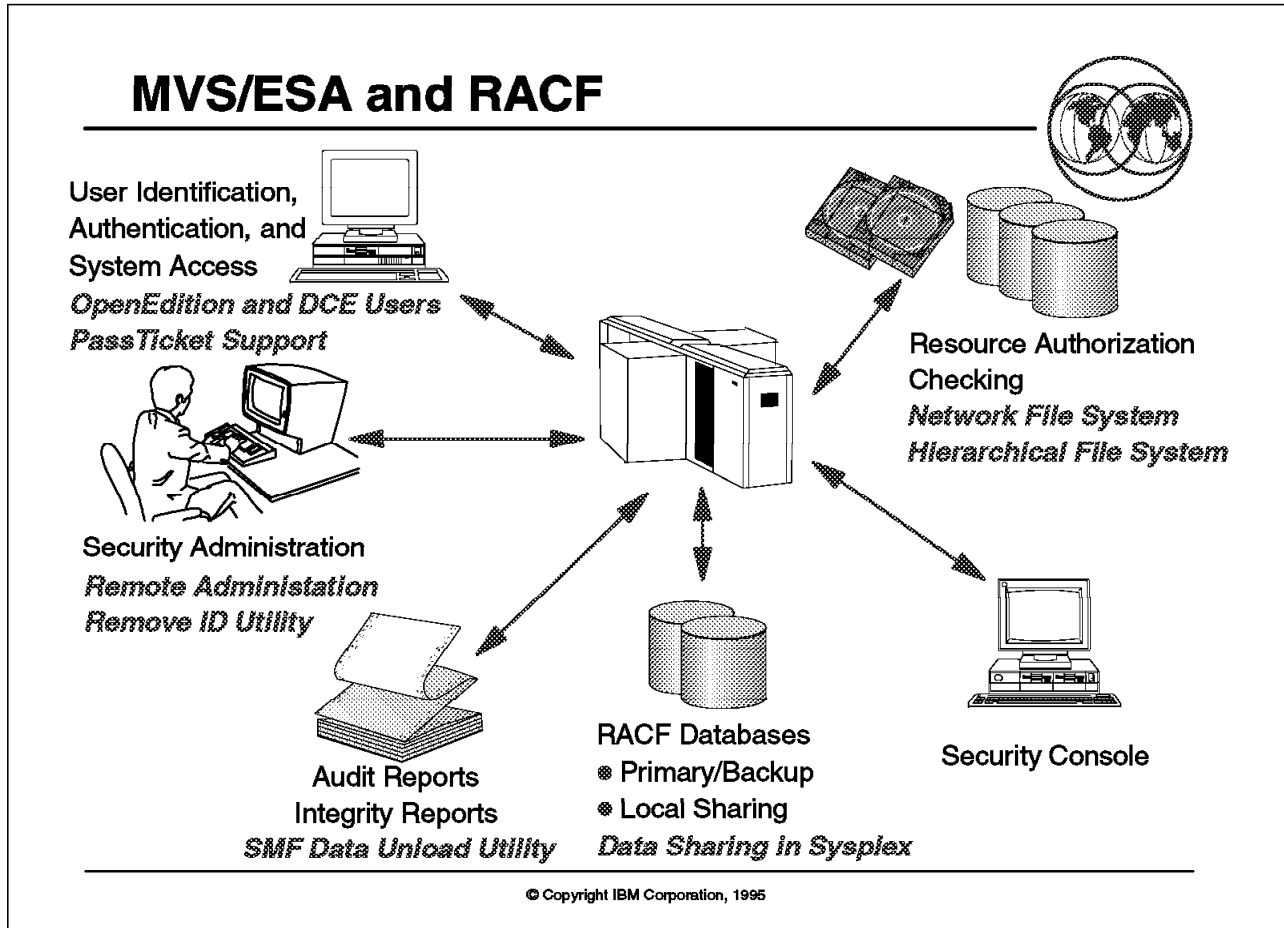


Figure 45. MVS/ESA and RACF

Key Points

MVS offers operating system integrity and system services upon which RACF builds enhanced security services.

Presentation Script

The MVS operating system has many characteristics and features to provide a secure environment, which include:

- *System Integrity*

MVS has supported system integrity since 1973 when IBM began to accept APARs for MVS system integrity failures. System integrity helps ensure that system security cannot be bypassed, and so it is vitally important to a system. It mainly consists of the limitations of what an unauthorized application program can accomplish. So, unauthorized programs cannot:

- Bypass store or fetch protection (for example, reading or writing into others users' areas)
- Bypass OS password, VSAM password, or RACF checking

- Obtain control in an authorized state: for example:
 - Running an authorized program with the capability of obtaining a system protection key in the range 0-7, and/or
 - In supervisor state, and/or
 - With Authorized Program Facility (APF) authorization

- *Private Address Space*

In MVS, the virtual storage consists of a system area, a common area and a private area. MVS prevents a user from violating another user's address space. Furthermore, before allocating real storage, MVS clears the storage's residual data, in order to prevent access of its previous contents.

Identification and Authentication

RACF identification and authentication allows MVS to identify users requesting access to the system. Flexibility has been provided in the method of authentication, which can be by traditional password or via "PassTicket." This PassTicket is a dynamically generated password substitute that allows authentication to occur outside RACF, such as within a LAN Server, for example with the NetSP Secured Logon Coordinator product or with smartcards. RACF also intends to interoperate with DCE Kerberos and the DCE Registry. When MVS works in combination with RACF and Netview Access Services (NV/AS), a single signon point is provided for terminal users to access multiple applications and systems. MVS supports seven character user IDs and optional RACF group IDs. RACF also provides support for LU6.2 sessions and authentication of remote RJE/RJP station user IDs. For transaction driven applications with application programming involvement, workstation users can be authenticated via PIN, signature dynamics, and IBM Personal Security Card.

- *Access Control Check*

MVS also provides for access control to objects that it manages. It uses either RACF or an equivalent product in performing the checks. The MVS resources that can be protected include data sets, transactions, spool files, programs, operator commands, messages, hiperbatch, APPC transaction programs, printers, physical devices (such as card readers and tape drives), SYSOUT data, and many others.

- *Confidentiality and Data Integrity*

Confidentiality and data integrity in MVS uses access control to protect the resources within the system, and encryption to protect sensitive information for network communication security. MVS has several cryptographic products such as the Integrated Cryptographic Feature (ICRF), Integrated Cryptographic Service Facility/MVS (ICSF), and Transaction Security System. On MVS the two main control policies for supporting confidentiality of information resources are Discretionary Access Control (DAC) through RACF access control list checking, and Mandatory Access Control (MAC), through RACF security levels and categories.

- *Auditing*

MVS ensures that appropriate audit records are recorded. Your installation can define the security relevant events needed for an audit trail (such as identification/authentication of users, access to resources, deletion of resources, actions of privileged users, and so on). A number of logging

facilities exist, such as the system log, system trace records, Generalized Trace Facility, SMF records, and many others.

The RACF Data Security Monitor (DSMON) and the RACF Data Base Unload Facility are tools to create reports reflecting the current status of the operating system security environment.

RACF is closely integrated with, and provides security support for the latest software IBM facilities, such as the ES/9000 coupling facility, Open Edition MVS, MVS APPC support, MVS Version 5 and CICS Version 4.

RACF's architecture in conjunction with MVS/ESA lets you implement security as you wish, either immediately at the desired target level, or incrementally, starting with a low level and then growing to the desired level.

RACF also allows multiple MVS and VM systems to share user profiles and resource definitions by sharing the RACF database. This simplifies security management and administration across multiple-system environments.

A Trusted Computer Base (TCB) based on MVS/ESA with RACF was rated at the B1 level. IBM continues to announce that subsequent versions of MVS are designed to meet B1 criteria.

For additional MVS or RACF security information, refer to the following publications:

- *MVS/ESA Planning: B1 Security*, GC28-1440
- *MVS Planning: Security*, GC28-1439
- *RACF General Information*, GC23-3723
- *RACF Planning: Installation and Migration*, GC23-3736

3.2.2 MVS/ESA Open Edition

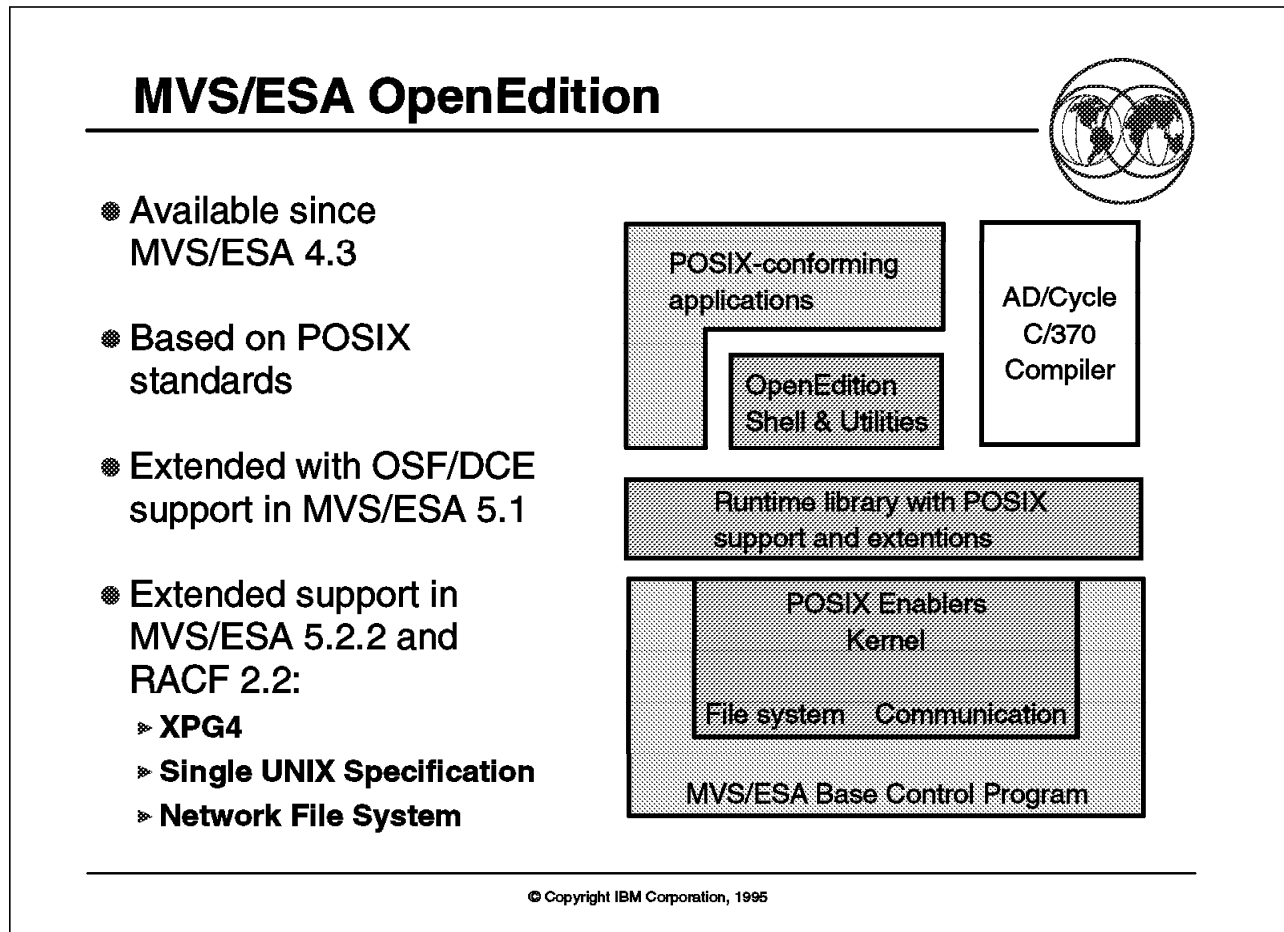


Figure 46. MVS/ESA Open Edition

Key Points

This foil depicts the MVS Open Edition structure and the product enhancements.

RACF supports POSIX file access control checking.

Presentation Script

MVS OpenEdition addresses the need for open systems and provides an environment that enables the development of portable applications. OpenEdition support has been available since MVS/ESA 4.3. The functions delivered in MVS/ESA 5.2.2 are a further step toward MVS/ESA being branded as a UNIX system. RACF continues to assist in this effort, being continuously enhanced to provide the ability to maintain traditional system security.

Support for X/Open XPG4 base branding requirements and for a significant set of the functions defined by XPG4.2 Single Unix Specification have been added.

The features of MVS OpenEdition fit between application programs and the existing services of MVS/ESA. POSIX-compliant application programs include C language POSIX 1003.1 functions. These functions, after being recompiled with the C/370 (or equivalent) compiler, result during program execution in calls to the function routines, which perform some of the function, while for the other

functions, the library routine in turn invokes MVS OpenEdition services or basic MVS services.

In addition, applications can invoke shell scripts, which in turn invoke shell utility programs. Some of these programs make operating system requests and thus are seen from the operating system as applications.

The MVS support for the OpenEdition MVS services feature provides the new control program services for POSIX 1003.1 process management, file system management (to support the new file system type called hierarchical file system, "HFS"), and communication.

3.3 VM/ESA and RACF

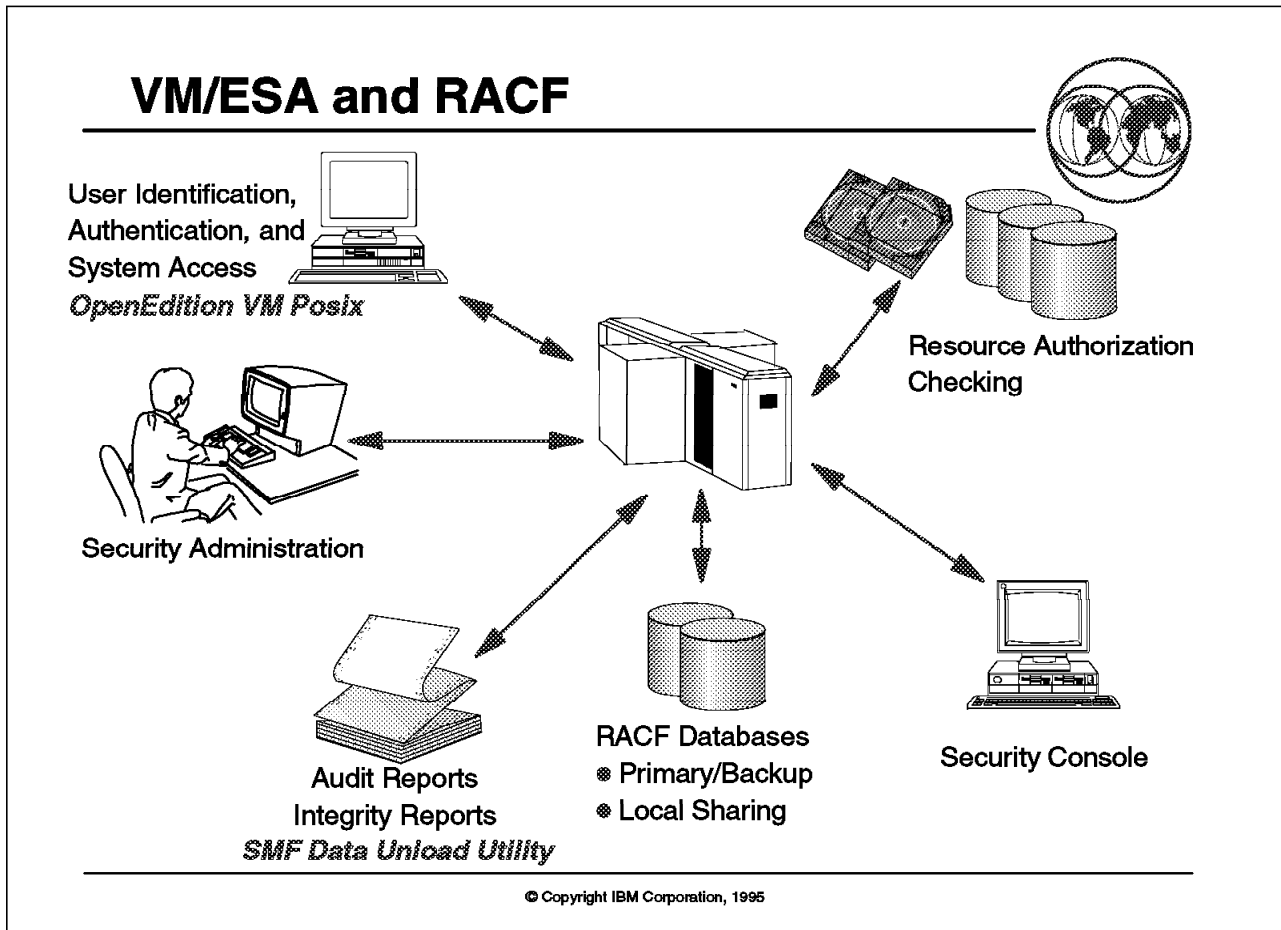


Figure 47. VM/ESA and RACF

Key Points

RACF provides extended security for the VM environment.

Presentation Script

The VM operating system has many system integrity and security features. VM/ESA exploits the System/390 architecture in several ways:

- Addresses in a virtual machine are *virtual* addresses, and they have no meaning outside the virtual machine in which they are generated and used. So it is impossible for one user to access an address space of another user unless the owner allows the other user to do so.
- All channel program addresses are translated, except those started via DIAGNOSE X'98' and V=R machines. VM/ESA will identify the storage device and perform the I/O operation on behalf of the virtual machine.
- Every virtual machine runs in interpretive-execution mode, which processes most privileged and non-privileged instructions and address virtual storage translation without intervention of VM/ESA.

Other VM/ESA native features are:

- Unique user identification and authentication
- Clearing temporary disk space
- Journalling the LOGON, AUTOLOG, XAUTOLOG and LINK commands
- Automatic deactivation of restricted passwords
- Suppressing passwords entered on command line
- Shared user capability

VM/ESA V2 extends its interoperability to DCE-compliant systems. This DCE support is based on OSF's DCE Version 1.02 and provides DCE Security Service support: authentication, authorization, and communication integrity.

RACF's architecture in conjunction with VM/ESA lets your installation implement security as you wish, either immediately at the desired level, or incrementally, starting with a low level and then growing to the desired level. At the same time, RACF provides you with consistent administrative and technical support for the security administrators and auditors.

RACF also allows multiple MVS and VM systems to share user profiles and resource definitions by sharing the RACF database. This simplifies security management and administration across multiple-system environments.

The RACF functions available in a VM/ESA environment are:

- Security administration
- User identification and authentication and system access
- Resource authorization checking
- Security relevant event monitoring & auditing
- Integrity reporting

VM/ESA 2.1.0 with RACF 1.10 for VM will provide support for Open Edition VM POSIX 1003.1 level of function.

VM/SP with RACF has been evaluated at the C2 level.

VM/ESA with RACF was designed to meet B1 requirements.

3.4 System Authorization Facility (SAF)

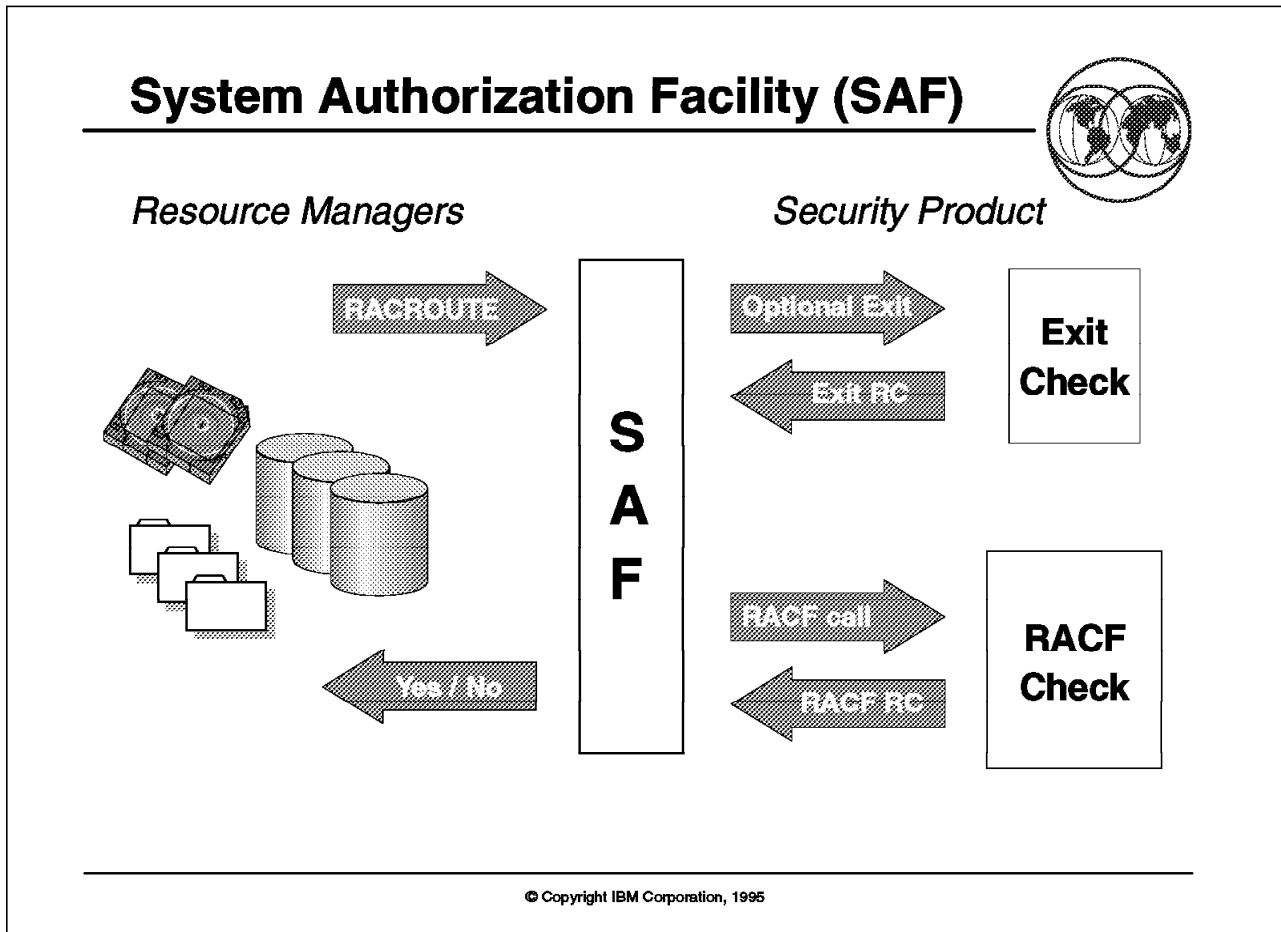


Figure 48. System Authorization Facility (SAF)

Key Points

This foil depicts the flow of the System Authorization Facility (SAF) interface, available on MVS and VM systems.

SAF provides a common security control point for routing checks to a security product such as RACF.

Presentation Script

The System Authorization Facility (SAF) supplies the primary MVS and VM system security interfaces for invoking user authentication and access control services. System, subsystem and program product resource managers invoke security services through SAF at critical security processing spots known as "control points."

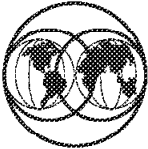
SAF provides a routing service that examines the request, invokes optional customer exit routines, and then optionally invokes RACF, or a compatible security product to process the request if it is not one the SAF can process itself.

A key advantage of the SAF function over other designs is that it provides a centralized security processing point within the system. Applications, resource

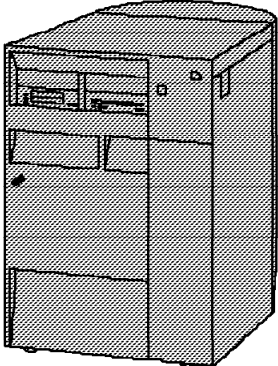
managers, and MVS itself may invoke the security product through SAF to provide consistent security processing, without having to imbed the actual processing in the application itself. This single SAF interface encourages the use of common control functions shared across products and systems.

SAF provides interfaces for both MVS and VM environments supporting the RACROUTE macro to request the authentication of a user or to make decisions when a user attempts to access a resource. The RACROUTE macro is also used to retrieve information about user or resource definitions from the security product, or to update the information in the security database. In the MVS environment, SAF also supports callable service routines that are used by Open Edition MVS to provide UNIX-style security functions.

OS/400



- **OS/400 has completed the formal evaluation for C2 security certification with an integrated database**
- **Security built into the system architecture**
- **Different security levels selectable:**
 - ▶ **No protection**
 - ▶ **Sign-on security**
 - ▶ **Resource security**
 - ▶ **Resource security with system integrity**
 - ▶ **Resource security and enhanced system security**



AS/400

© Copyright IBM Corporation, 1995

Figure 49. OS/400

Key Points

OS/400 security is integrated into the OS/400 hardware and software, offering selectable levels of installation security.

The OS/400 has completed formal evaluation by the U.S. Government for C2 Certification with an integrated database.

Presentation Script

Security is built into the system architecture. This means that there are security functions integrated in the operating system software and hardware so that you do not need to purchase software to secure your system.

In the OS/400 operating system, you can choose one of five different security levels:

- No Protection (Level 10)
 - The system does not enforce security. Anyone can sign on to the system.
- Signon security (Level 20)

The system requires a user ID and password. By default, all users are given access to all objects on the system.

- Resource security (Level 30)

User IDs and passwords are required to sign on. Users are required to have authority to objects to access them. That is, resource security is enforced.

- Resource security with system integrity (Level 40)

Level 30 security plus system integrity. Users can not directly access system objects without going through published interfaces. Integrity is enforced in the operating system and through hardware storage protection.

- Resource security and enhanced system integrity (Level 50)

Level 40 security plus protection of more system interfaces. Security level 50 is intended for AS/400 systems with high security requirements. This level is designed to meet C2 security requirements as defined by the U.S. Government TCSEC.


The OS/400 has completed formal evaluation by the U.S. Government for C2 Certification with an integrated database.

For definition of the TCSEC security levels see 2.6.7, "Security Evaluation Strategy" on page 88.

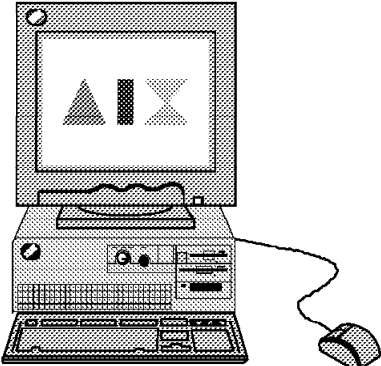
For additional OS/400 security information, refer to the following publications:

- *AS/400 Security -- Basic*, SC41-3301
- *AS/400 Security -- Reference*, SC41-3302
- *Guide to Enabling C2 Security*, SC41-0103
- *An Implementation Guide for AS/400 Security and Auditing*, GG24-4200

AIX/6000



- **Hardware Key Lock**
- **AIX/6000 is designed to meet C2 security functions:**
 - ▶ **User Identification and Authentication**
 - ▶ **Access Control List (ACL)**
 - ▶ **Object Reuse**
 - ▶ **Audit**
 - ▶ **System Architecture**
 - ▶ **System Integrity**
- **Application Security:**
 - ▶ **DCE**
 - ▶ **CICS/6000**
 - ▶ **DB2/6000**



© Copyright IBM Corporation, 1995

Figure 50. AIX/6000

Key Points

AIX Version 3.2 and AIX Version 4 for the RISC System/6000 currently offer security policies and mechanisms for user authentication, password complexity, user/port access controls, access control lists, auditing, trusted path, system integrity, and user-resource limitations.

AIX/6000 is a secure system offering traditional UNIX type security, DCE security, and ACL enhancements to support C2 functions.

Presentation Script

AIX Version 3.2 and AIX Version 4 for the RISC System/6000 currently offer security policies and mechanisms for user authentication, password complexity, user/port access controls, access control lists, auditing, trusted path, system integrity, and user-resource limitations.

Hardware Key Lock: AIX/6000 can be ordered with a hardware Key Lock. This Key Lock has three positions:

- Secure

The system is not able to boot, from hard disk or from any other device like floppy, CD, or tape.

- Normal

The system is able to boot from the hard disk only. This is the most common position.

- Service (Maintenance)

The system tries to boot from removable devices like floppy, CD, or tape. If the system cannot find any removable boot device, then the diagnostic software from the hard disk will be loaded.

AIX/6000: AIX/6000 is designed to meet the National Computer Security Center (NCSC) Trusted Computer System Evaluation Criteria (TCSEC) Class C2, with additional support exceeding C2 for extended granular access control, configurable identification and authentication, and system integrity checking mechanisms. For definition of the TCSEC security levels, see section 2.6.7, “Security Evaluation Strategy” on page 88.

The security functions offered by AIX/6000 are:

- Identification and Authentication

AIX uses standard password authentication. Encrypted passwords and other security relevant user information are kept in a directory that is not accessible to ordinary users.

- Access Control Lists (ACL)

AIX uses a combination of traditional UNIX mode bits and an Access Control List (ACL) mechanism. An AIX ACL allows the user to restrict or permit access for individual users, groups or combinations of users and groups. The access permission bits (and the ACLs, if present) are modifiable only by the owner of the file or directory.

- Object Reuse

Storage objects are objects that can be read-from and written-to by non-privileged users and are accessed through kernel system calls. The identified storage objects on AIX are filesystem objects, heap data (malloc'd memory), a process's memory address space, shared memory segments and sockets.

- Audit

AIX has the capability of creating an audit trail of security relevant events. The auditable events are generated by preselection of user/event combinations that can be configured by the system administrator. The audit trail is kept (by default) in a directory that is not accessible by ordinary users.

- System Architecture

All processes in AIX reside in their own address space. A non-privileged process may not read or write outside of its own address space. Segment registers, which define these address spaces, are modifiable only by the kernel. Other, non-memory TCP resources are protected from unauthorized access by discretionary access control.

- System Integrity

The RISC System/6000 performs an extensive Power On Self Test (POST) each time the system is cold booted to check the proper functioning of its hardware and firmware.

Application Security: Some applications have additional application dependent security functions such as DCE (for more information about DCE see Chapter 4, “DCE Security” on page 111 and 2.6.2, “DCE Security Services” on page 75), DB2/6000 and CICS/6000. (In Chapter 5, “Application Security” on page 123 you will find some additional information about DB2 and CICS)

AIX (IBM E3/CMW): IBM E3/CMW for the AIX operating system is a multi-level secure workstation operating system that is based on AIX/6000 V3.2.5. It is designed to meet E3 (ITSEC) and B1 (TCSEC) with selected functionality from the B2 and B3 level. For definition of the TCSEC and ITSEC security levels, see section 2.6.7, “Security Evaluation Strategy” on page 88.

The IBM E3/CMW for the AIX operating system is only available from IBM UK. For detailed information about this operating system you have to contact IBM UK.

Additional Information: For additional information on AIX 4 security see the *AIX 4 Security White Paper* from the EMEA AIX Security Center of Competence available through WWW at <http://w3.munich.ibm.com/CoC-Security/>.

3.7 OS/2

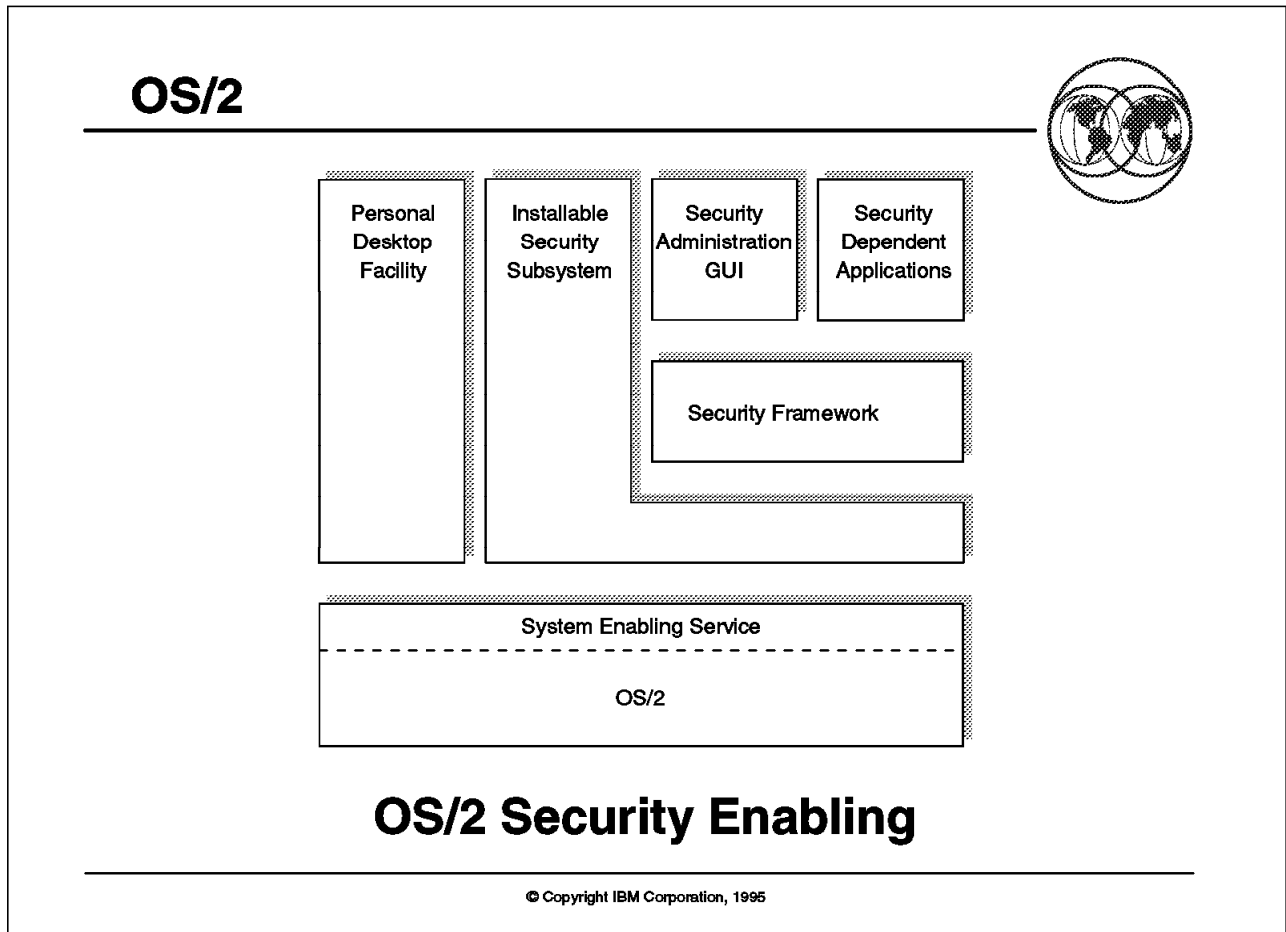


Figure 51. OS/2

Key Points

OS/2 provides a security structure with security interfaces that enable installable security subsystems on the platform.

Presentation Script

The OS/2 security enabling strategy addresses a diverse set of workstation security requirements that includes a wide range of security services from simple restricted shell protection to C2 level operating system security capability, compatibility with a wide variety of existing DOS/Windows security products, single signon, and centralized security administration in a heterogeneous distributed computing environment.

These diverse security requirements are addressed by enabling an external security component (Installable Security Subsystem) to enforce security policies that satisfy specific customer security requirements. The ISS may be provided as part of an ISV security product, an IBM product, or a customer application.

The OS/2 security enabling strategy is dependent on the following OS/2 security enabling features:

- The OS/2 Security Enabling Services (SES) enable an ISS to provide operating system security services such as user identification and authentication, resource access control, multi-user and trusted program support, and single signon.
- The OS/2 Personal Desktop Facility (PDF) enables serial sharing of an OS/2 workstation by supporting multiple personal desktops and facilitates system management by enabling restriction of user interface operations. In addition, PDF enables an ISS to integrate its security services with PDF services.
- The OS/2 Security Framework and the OS/2 Security Administration GUIDE enable customer applications and users to communicate with security service providers (such as an ISS) through standardized interfaces.

The OS/2 security strategy also includes working with security product ISVs to develop security products for OS/2 that exploit and support SES, PDF, the Security Framework, and the Security Administration GUI.

The code for OS/2 2.11 Security Enabling services went Gold Master on August 29, 1995. It is available on the PCCBBS Bulletin in Retain (Retain info #II0887).

The security objectives of Warp for Intel and Warp for PowerPC include:

- Provide users with a secure operating system environment that scales easily and has uniform management “look and feel” from stand alone systems to full client/server environment
- Build on industry standards such as DCE security and OMG Object Oriented security
- Provide for seamless growth with single signon support capability at all levels
- Build on and maximize capability with the SES security programming interfaces integral to the OS/2 Security Strategy
- Provide flexibility in support of security policy/management software in DOS, Windows and OS/2 environments
- Produce a design and implementation that will support the pursuit of a C2 evaluation.

3.8 Process Resource/Systems Manager

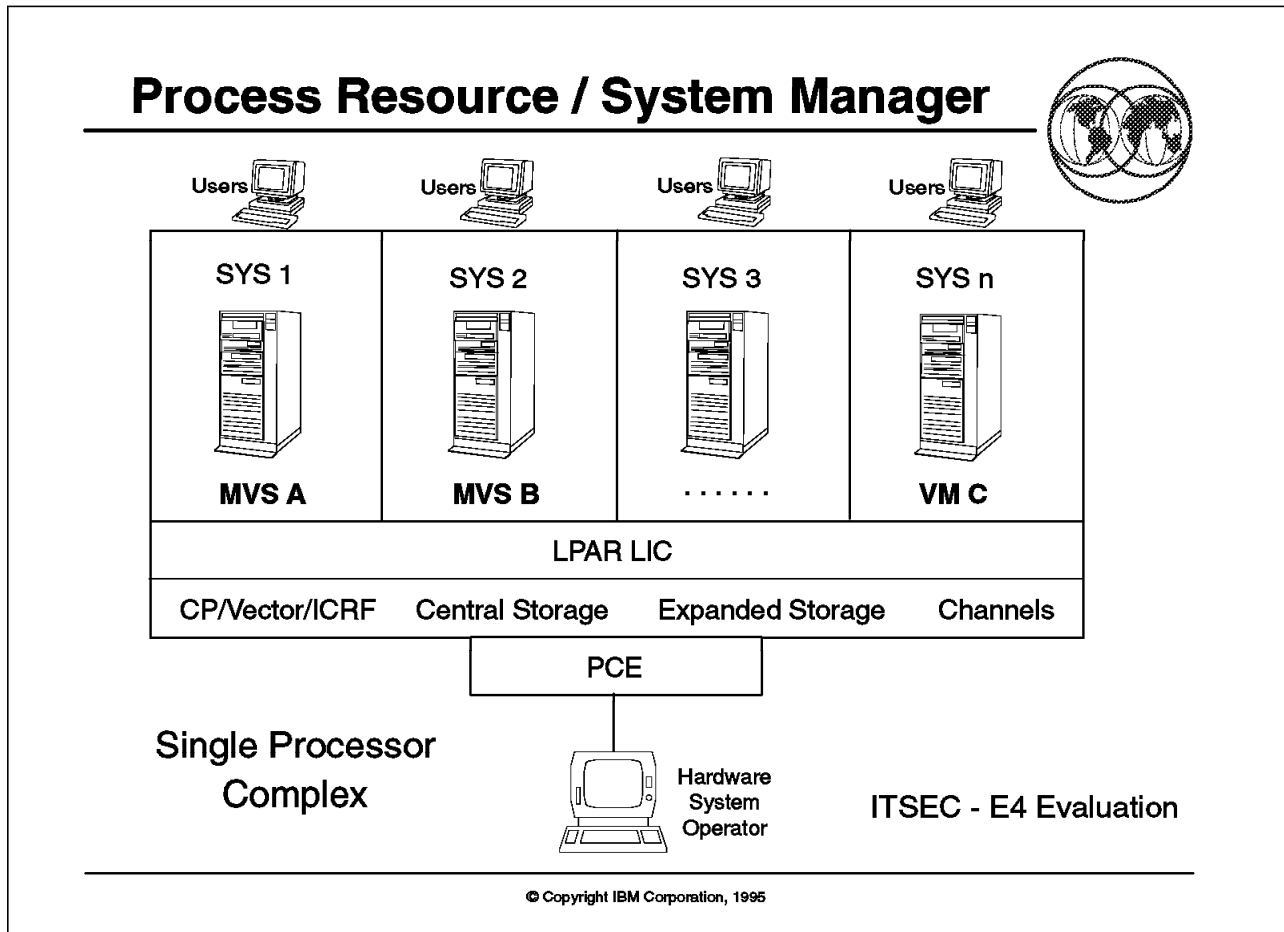


Figure 52. Process Resource/Systems Manager

Key Points

- Multiple operating systems exist on a single processor complex.
- Logical partitions (LPARs) can be isolated.
- Resources can be shared or secure dedicated.
- PR/SM completed ITSEC E4 evaluation.

Presentation Script

Process Resource/Systems Manager (PR/SM) is a hardware facility of the ES/9000 processor series that enables the resources of a single processor complex to be divided between distinct, predefined logical machines called *logical partitions* (LPARs). A LPAR is a collection of resources including storage (main and expanded), computation elements (vectors and central processors), and I/O that can run an operating system. Each logical partition can be isolated from all other logical partitions, and each is capable of running any S/370, 370-XA, ESA/370, or ESA/390 operating system. Computation elements can be shared by LPARs or can be dedicated to them.

The requirement for using PR/SM features can derive from the necessity to run multiple production systems on a single processor, for consolidation, migration test, development, maintenance, diverse workloads, backup, or recovery.

PR/SM has been evaluated against ITSEC at the E4 assurance level, which provides a very high degree of assurance of a secure consolidation platform. The evaluation was completed on the ES/9000 9021 and 9121 processor families.

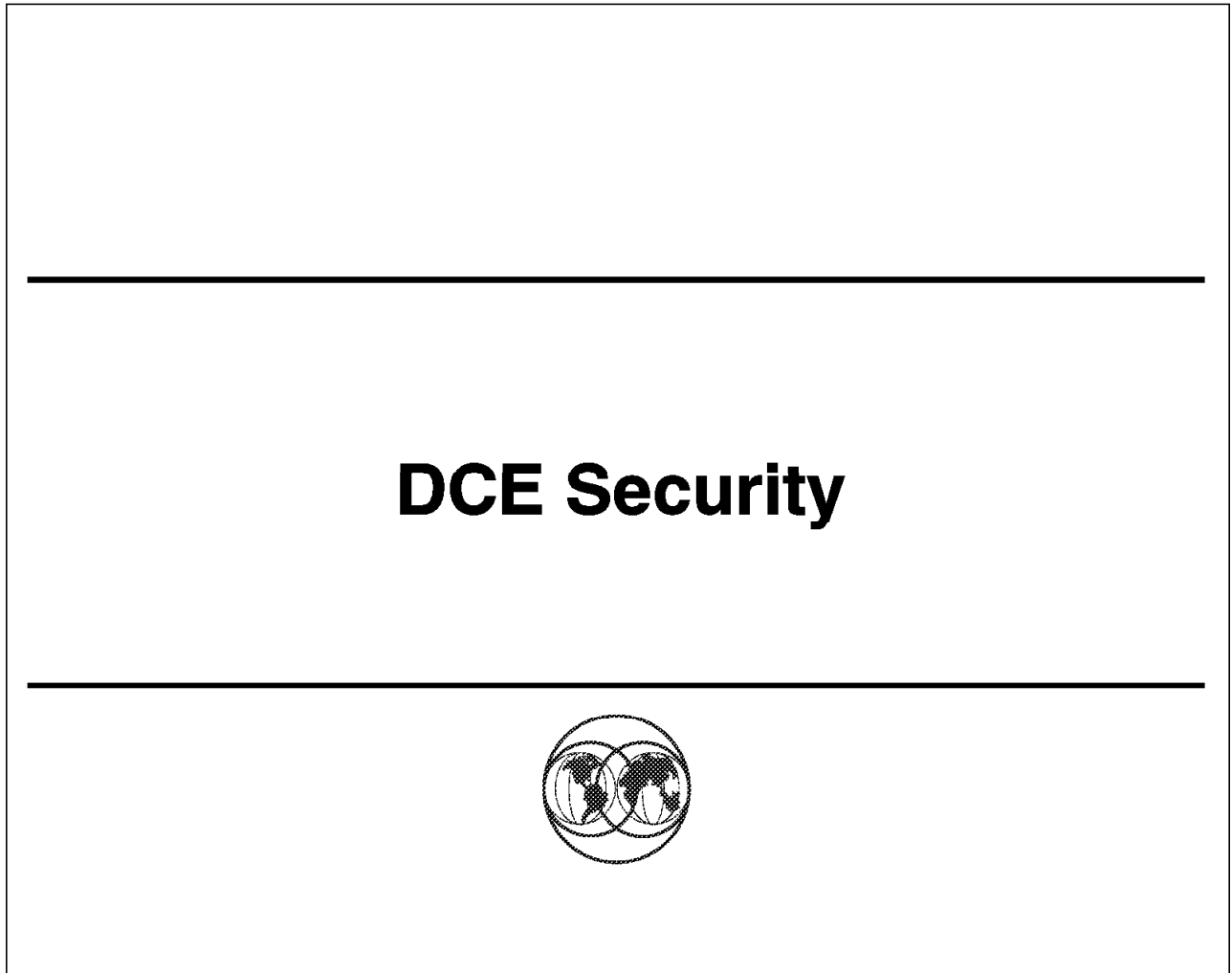


Figure 53. DCE Security

4.1 OSF DCE Structure

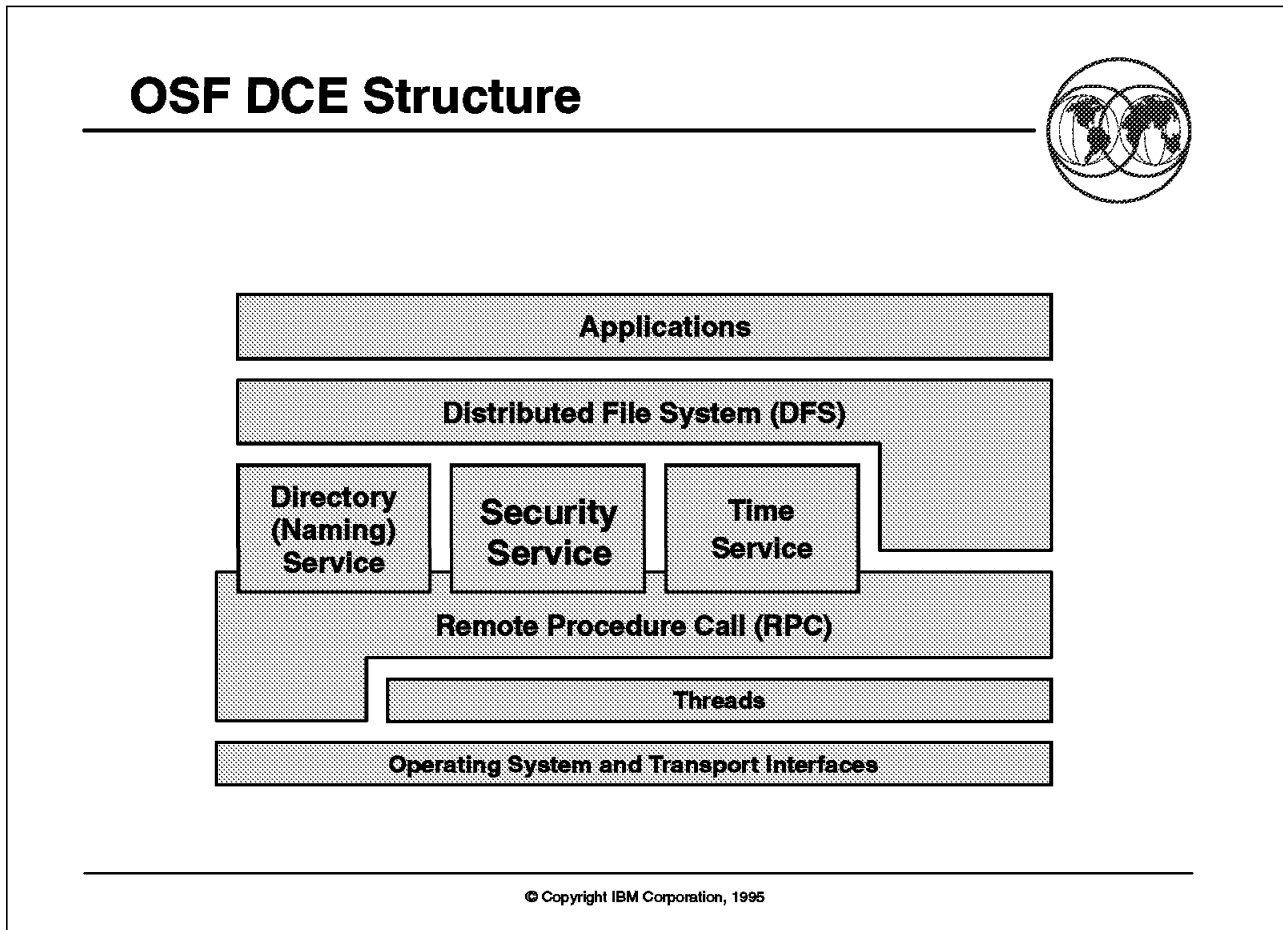


Figure 54. OSF DCE Structure

Key Points

- This foil depicts the OSF DCE structure and its components.
- DCE provides tools and services for distributed application support.
- DCE applications have secure access to enterprise resources.

Presentation Script

Many companies today find themselves with collections of computing hardware, software and networks that do not meet their business goals. They need a comprehensive and open set of infrastructure, applications development tools, system management applications, and end-use applications that could help them.

DCE is the foundation for open, enterprise distributed client/server computing. With DCE you can easily develop distributed applications in a network-independent manner, being able to use DCE's standards, integrated services across multiple hardware and software architectures. DCE applications have secure access to enterprise resources. DCE structure consists of several components, which were originally contributed by members of OSF in response to OSF Request for Technology. Later, OSF and its members enhanced and

integrated these components into a comprehensive, standard set of services that are available across multiple hardware and software architectures.

DCE's set of services is composed of several elements:

- *Remote procedure call (RPC)*

RPC is a facility for calling a procedure on a remote machine as though it were a local procedure call. RPC uses all of the other facilities (threads, security, time, and directory) to accomplish transparent access to servers throughout the network.

- *Directory service*

Directory service provides the naming mechanism and the functionality for registering and locating resources (such as servers, files, disks, printers, and so on) within a distributed environment. Applications can continue to successfully locate and use named resources, even if these resources change location.

- *Time service*

Time service provides loosely-coupled common time across a DCE *cell*. A cell is the fundamental unit of DCE administration. It spans multiple host computers over any network topologies. The organization of cells is determined by the DCE administrator. DCE provides facilities for inter-cell and multi-cell support, synchronizing the clocks in the systems that comprise the distributed system.

- *Thread service*

Threads are mainly used by server applications. They support multiple threads of execution within a single process or task. DCE's threading support is based on the POSIX 1003.4a (draft 4) standard. It consists of an API that gives C programmers the ability to create and manipulate threads.

- *Security service*

To prevent unauthorized access to the resources in a distributed environment, distributed services and applications must be able to securely identify users, guarantee the integrity and of communications, and control access to resources. As with the directory service, DCE provides replication of security servers for performance and availability.

The DCE security services will be described in greater detail later in this chapter.

- *Distributed File System (DFS)*

DFS provides a DCE based global distributed file system. Some DFS servers include a NFS gateway.

4.2 OSF DCE Security

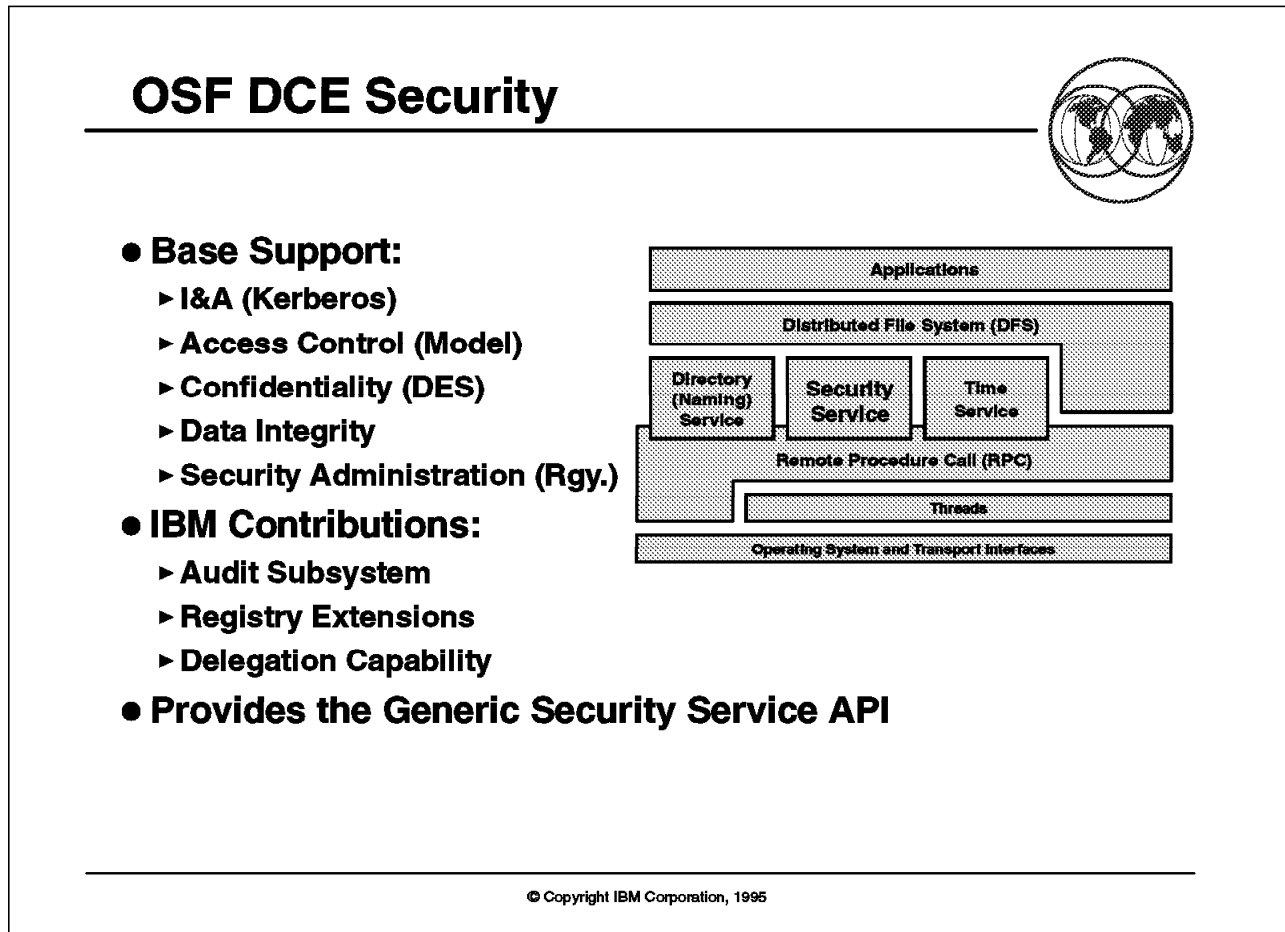


Figure 55. OSF DCE Security

Key Points

This foil lists the main security features available for OSF DCE Security and those features that have been contributed by IBM.

The Generic Security Services Application Programming Interface (GSS-API) supports a generic call interface for a subset of DCE security services.

Presentation Script

A distributed computing environment brings with it new security requirements, beyond those found in a non-distributed system, in which operating system can be trusted to protect resources from unauthorized access. A new security system is required to control access to resources in a distributed environment.

The DCE authentication mechanism provided by DCE security service is based upon MIT's Kerberos Version 5 shared-secret key mechanism.

The DCE authorization mechanism is provided via POSIX Access Control Lists (ACLs).

Most security services are provided transparently to application programs via Authenticated RPC. For non-RPC programs, OSF DCE Version 1.1 introduced support for DCE-extended Generic Security Services API (GSS-API). The Generic Security Service Application Programming Interface supports a generic call interface for a subset of security services. The generic interface allows applications to invoke the security services without detailed knowledge of the security mechanisms that actually provide the services.

4.3 DCE Security Services

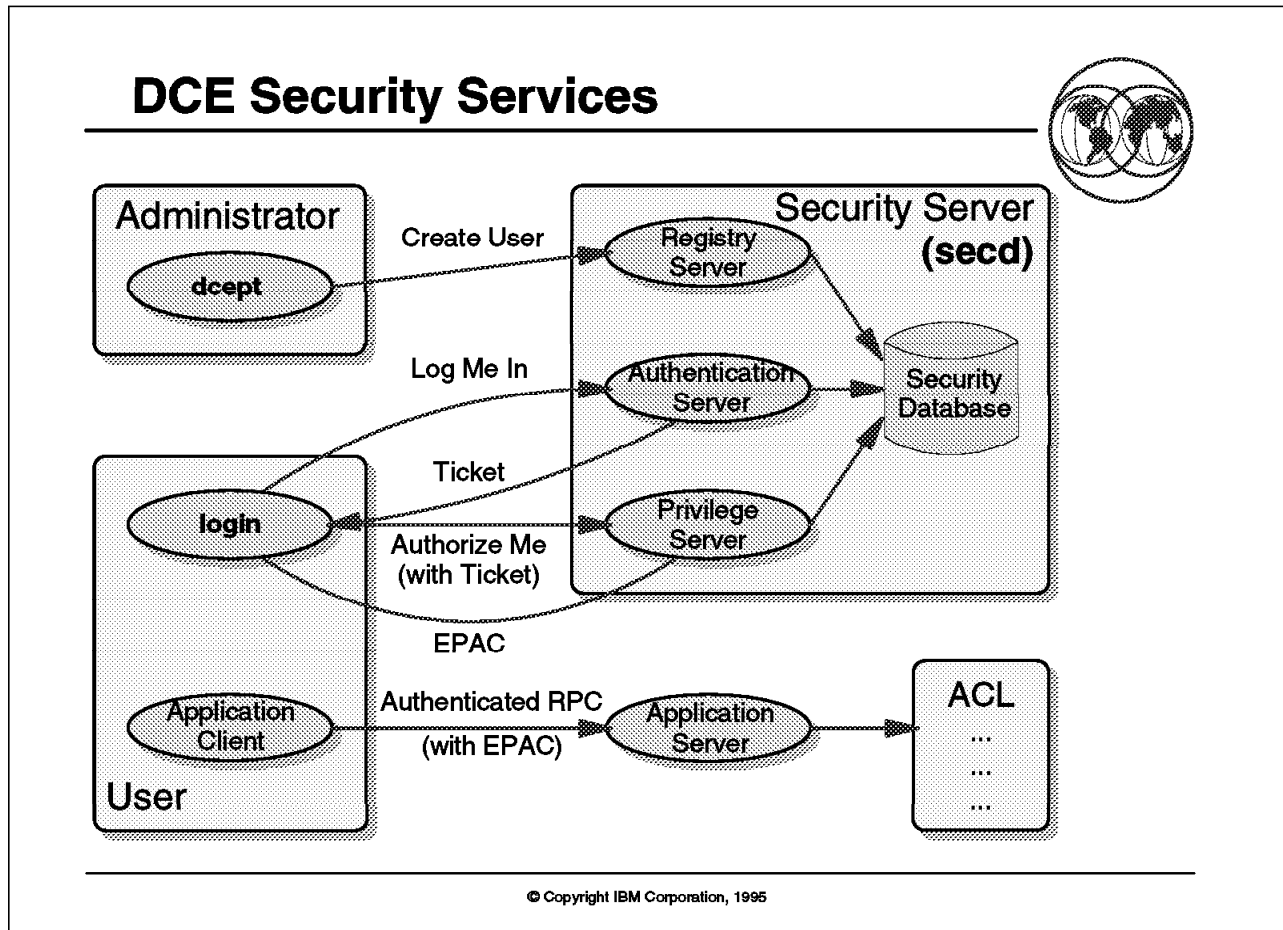


Figure 56. DCE Security Services

Key Points

This foil shows a simplified view of how the DCE security services and facilities interact to provide a secure distributed computing environment. These services are based on the third party authentication single signon issuing "tickets" to application servers.

Presentation Script

The DCE Security Service is composed of several services:

- The Authentication Service

The Authentication Service enables two processes on different machines to be certain of one another's identity. On a timesharing system, this function is provided in part by the operating system kernel. However, because a local host's operating system cannot necessarily be trusted in a distributed system, an authentication service is necessary in a distributed computing environment.

- The Privilege Service

Once a server has verified the identity of the user who is making a request, it still needs to determine whether the user should be authorized or granted

the requested access to a resource that the server controls. The Privilege Service forwards in a secure way the information that a server needs to know in order to determine what permissions it should grant to the user.

Both the DCE Authentication Service and the DCE Privilege Service are used in conjunction with DCE RPC and the Login Facility, so the typical application programmer does not interact with them directly, but instead uses Authenticated RPC.

- The Registry Service

The DCE Registry Service is a replicated service that manages the cell's Security database. The Security database contains entries for security entities, which are called principals. A principal can be a user or a server, for example. The database also contains information associated with each principal, such as encryption keys, which are used in authentication, authorization, and encryption of messages. The Registry Service enables administrators to access and modify the database of DCE users.

The Extended Registry Attribute interface allows the Registry schema to be modified so that user-defined attributes can be associated with registry objects.

- The Access Control List Facility (ACL)

DCE Access Control List (ACLs) is a list of users who are authorized to access a given resource. For example, a user can put a colleague on an ACL for a certain file, thus granting that colleague permission to read and write the file. DCE ACLs are associated with many DCE resources: files, entries in the Directory Service, and entries in the Security Service. DCE ACLs are based on the POSIX 1003.6/Draft 3 specification. An ACL API allows programmers to manipulate ACLs, and the *dcecp* command allows users to modify ACLs associated with resources they own.

- The Login Facility

The DCE Login Facility initializes a user's DCE security environment. It authenticates the user to the Security Service by means of the user's password. The Security Service returns security credentials, which are then used to authenticate the user to distributed services that are accessed during the user's session, such as the Distributed File Service or other applications.

- The Audit Service

The Audit Service detects and records the execution of DCE server operations that are relevant to the maintenance of a secure distributed computing environment. The Audit Service records the events in a log file. DCE application programmers build auditing into their DCE servers. The DCE Security Service and the DCE Distributed Time Service also use the Audit Service to track and record the use of their security-critical operations. Administrators can use the Audit Service to organize and tailor the recording of events into audit trail files.

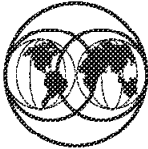
- The Key Management Facility

This facility consists of routines that an application programmer can call to manage the secret key of a nonhuman principal, such as an application server.

- The Principal ID Mapping Facility

This facility supports the mapping of principal names between a global representation and a local (cell-relative) representation.

4.4 Supported Platforms



	Windows 3.1x	OS/2	AIX	OS/400	MVS	VM
DCE Base Services	Avail.	Avail.	Avail.	Avail.	Avail.	Ann.
DCE Security Server		Avail.	Avail.		SoD	
DCE Directory Server		Avail.	Avail.			
Distributed File System			Avail.		SoD	
Encina Client		Avail.	Avail.			
Encina Server			Avail.			
CICS		Avail.	Avail.*	Avail.	Avail.	
Application Support/CICS					Avail.	
Application Support/IMS					Avail.	

* DCE-based

© Copyright IBM Corporation, 1995

Figure 57. Supported Platforms

Key Points

This foil shows the availability of DCE from IBM for the various platforms.

Presentation Script

IBM has chosen DCE as a key part of Open Blueprint (specifically, DCEs Remote Procedure Call, Directory, Security and Distributed File System are key Open Blueprint components). So, IBM's strategy for DCE is to make it pervasive; available everywhere, and used by all strategic software within the Open Blueprint framework.

The above foil shows complete coverage of DCE "base services" (that is Threads, RPC, Time, Directory Client and Security Client), with good progress in making other key services available when needed.

4.5 MVS Specific

4.5.1 DCE - RACF Interoperation

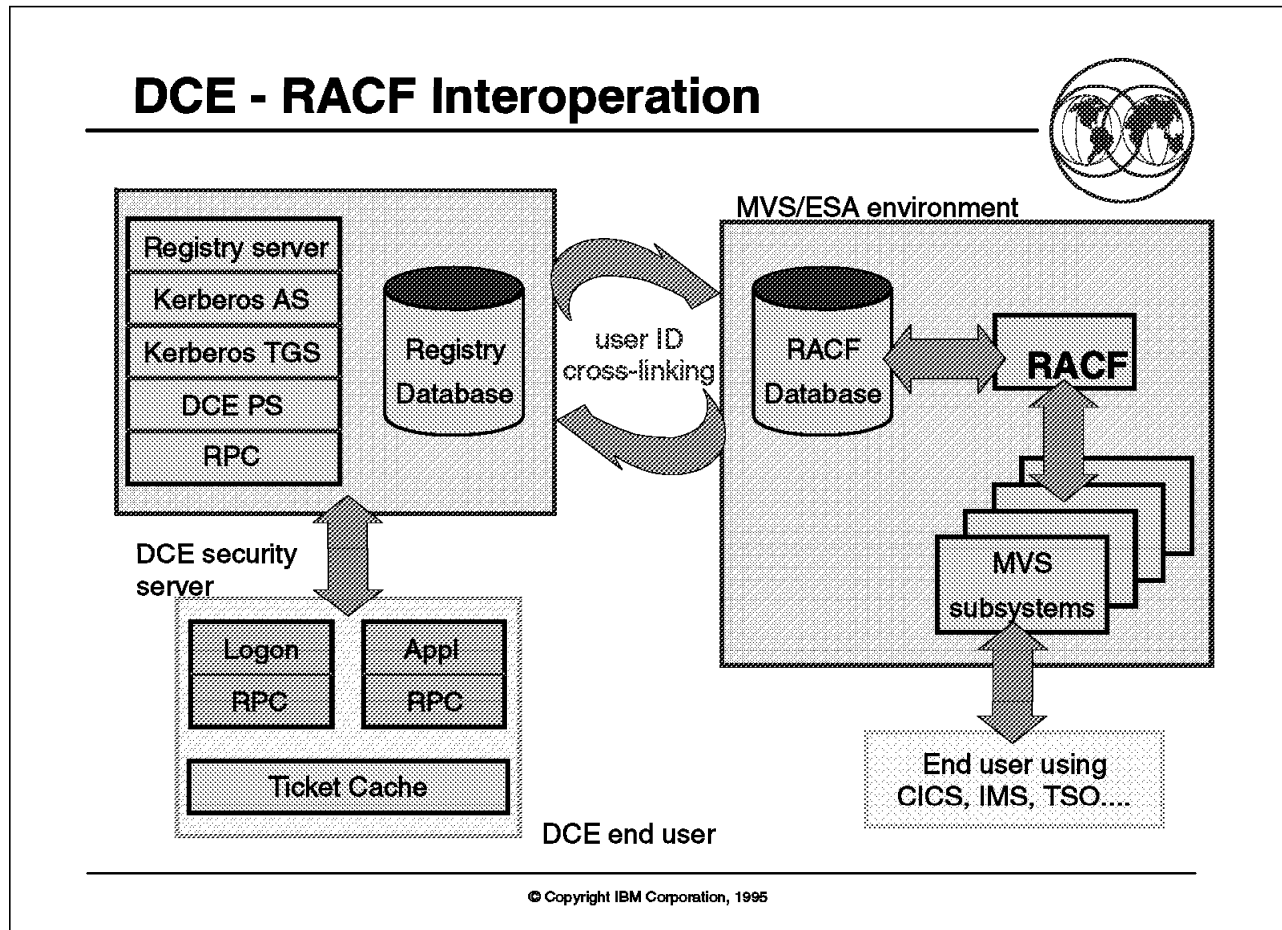


Figure 58. DCE - RACF Interoperation

Key Points

RACF will provide DCE-RACF interoperation that:

- Supports a single signon facility between DCE and MVS
- Supports synchronization of the DCE registry and RACF database
- Can combine administration of principals, groups and resources

Presentation Script

Together with the RACF V2.2 announcement, IBM announced its intention to enhance the RACF product for MVS to provide interoperation with OSF V1.1 security services.

RACF will provide support for OpenEdition DCE to enable single signon for RACF authenticated users. The OpenEdition DCE support enables access to both DCE and RACF protected resources. Additionally, RACF enhancements will enable a DCE identity to be associated with a RACF user identity.

The security service in DCE contains a registry (DCE registry) for storing the security attributes and the groupings of principals within a DCE cell. When DCE is implemented on an existing operating system platform, its security facilities must be integrated with the local security facilities on that platform. So, one key task is the integration of the DCE registry with the local security registry.

Integration of the local and DCE registry enables other aspects of DCE integration with local security services such as:

- Single signon to a local system in a network
- Transparent access to resources controlled by local access facilities
- Combined administration of DCE and local security information for principals, groups, and resources

4.5.2 DCE and OpenEdition MVS

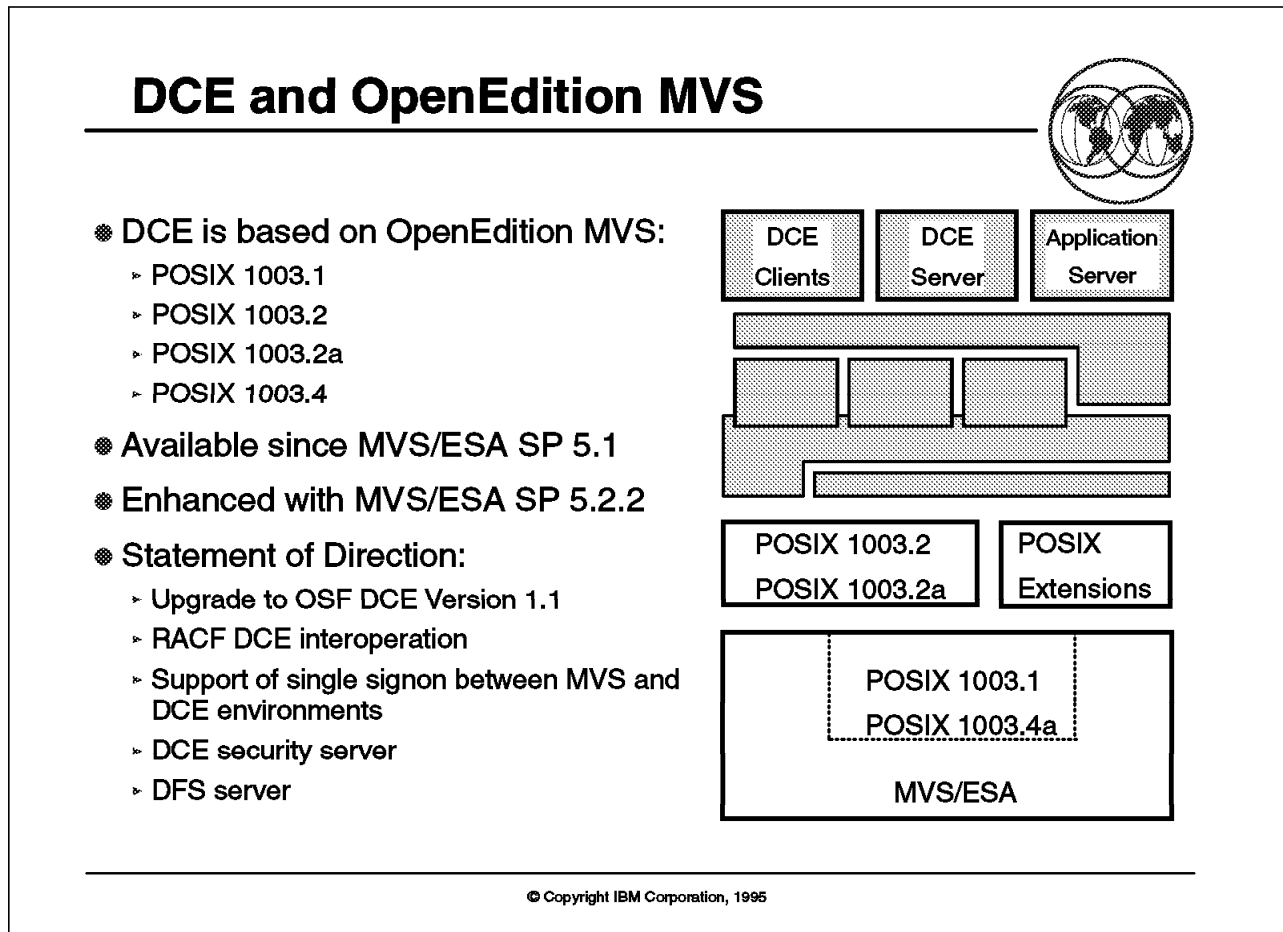


Figure 59. DCE and OpenEdition MVS

Key Points

DCE requires POSIX functions that are provided by MVS OpenEdition.

Presentation Script

DCE was built from technology gathered from the UNIX world. In the bottom boxes of the foil are shown the functions provided by MVS OpenEdition. POSIX 1003.1 provides the base operating system services (process, file system, and communications). POSIX 1003.2 and 1003.2a define over 180 commands and utilities, mainly used by administrators and application developers. POSIX 1003.4a is the standard on which DCE threads is based. There is no need to implement the threads support shipped with OSF/DCE on MVS, since this support is already integrated into MVS OpenEdition. MVS OpenEdition is a platform that implements international standard interfaces, allowing a easy porting of applications and products.

DCE is actually based on the usage of the C programming language, so an appropriate C compiler is required, such as IBM SAA AD/Cycle C/370. On MVS 5.2.2, the support for Language Environment for MVS and VM, and the MVS C/C++ Language support feature in MVS are available.

Application Security

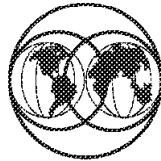


Figure 60. Application Security

5.1 CICS/ESA

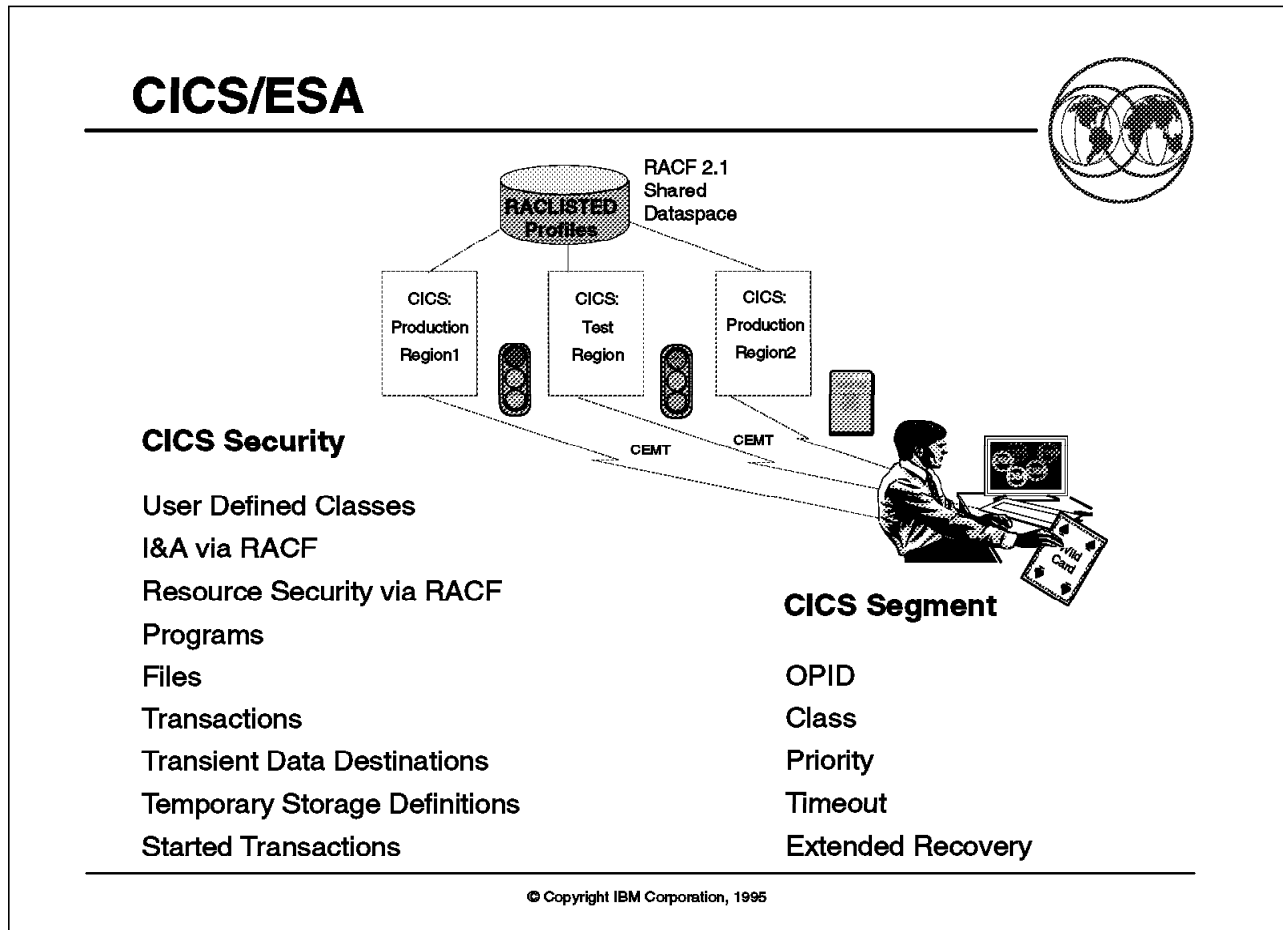


Figure 61. CICS/ESA

Key Points

CICS relies on an external security manager, such as RACF, for identification and authentication and to protect resources such as transactions, application programs, program specification blocks, files, journals, and application defined resources

Presentation Script

CICS: As an online transaction-processing system (often supporting many thousands of terminals), CICS clearly needs the protection of a security system to ensure that the resources to which it manages access are protected, and secure from unauthorized access.

To provide the necessary security for your CICS regions, CICS uses the MVS system authorization facility (SAF) to route authorization requests to an external security manager (ESM), such as RACF, at appropriate points within CICS transaction processing.

Identification and Authorization (I&A): To secure resources from unauthorized access, CICS needs some means of uniquely identifying individual users of the system. For this purpose, you must first define the users to RACF by creating an

entry in the RACF database, referred to as a user profile. To identify themselves to CICS, users sign on by specifying their RACF user identification (user ID), and the associated password (or PassTicket) in the CICS-supplied signon transaction, CESN. When users enter the CESN transaction, CICS verifies user IDs and passwords by a call to RACF. If the terminal user signon is valid, the CICS user domain keeps track of the signed-on user. Thereafter, CICS uses the information about the user when calling RACF to make authorization checks.

Transactions: The CICS facilities for transaction security ensures that CICS calls RACF each time a transaction is initiated to verify that the user IDs associated with that transaction are permitted access.

Security can also be specified for transactions that are not associated with terminals. These are:

- Started non-terminal transactions
- Transient data trigger-level transactions
- Program List Table (PLT) programs that run during CICS initialization

Resource Security via RACF: You can control access to CICS resources that a transaction uses. You do this by specifying YES on the resource security parameter, RESSEC, in the CICS TRANSACTION resource definition. These CICS resources can be:

- Application programs
- DL/I program specification blocks (PSBs)
- Files -- VSAM and BDAM
- Journals
- Temporary storage destinations
- Transient data destinations
- Transactions initiated by a CICS START command.
- Application defined resources

Application Defined Resources: In addition to using CICS security checking for CICS-controlled resources (or as an alternative to it), you can use the EXEC CICS QUERY SECURITY command to control security access within the CICS application. This method also allows you to define security profiles to RACF for resources other than CICS resource profiles, and enables a more detailed level of security checking than is available through the default resource classes.

CICS Segment: The information you can specify in the CICS segment is as follows:

OPIDENT: The one to three character operator identification code that you assign to each operator. CICS stores the code in the operator's terminal entry in the CICS terminal control table (TCTTE) when the operator signs on. This operator ID is displayed in certain CICS messages and can also be used in the EXEC CICS ROUTE command for routing BMS messages. (For more information about BMS, see the CICS/ESA Application Programming Guide). The operator ID forms part of the "Unit of Work" identifier that is used in recovery. It is also used when using the CEDA LOCK function.

OPCLASS: The operator classes are for use by CICS when routing basic mapping support (BMS) messages initiated within a CICS transaction. The operator classes are numeric values in the range 1-24.

You need to specify operator classes for users who use CICS transactions that issue EXEC CICS ROUTE commands with the (optional) OPCLASS parameter. You specify the corresponding value as an operator class in the CICS segment of the user profile for automatic routing to occur.

OPPRTY: The operator priority value--a decimal number that you want CICS to use when determining the task priority for CICS transactions that the operator invokes at a CICS terminal. The priority value can be in the range 0 through 255, where 255 is the highest priority.

CICS uses the sum of operator priority, terminal priority, and transaction priority to determine the dispatching priority of a transaction.

TIMEOUT: The time that must elapse since the user last used the terminal before CICS "times-out" the terminal.

For RACF Version 2.1, the time must be a decimal integer in the range 0 through 9959 (the rightmost two digits represent a number of minutes, and must be 00 through 59. Any digits to the left of these represent hours).

For RACF Version 1.9, the time must be a decimal integer in the range is 0 through 60.

XRFSSOFF: The CICS extended recovery facility (XRF) sign-off option. You specify this to indicate whether or not you want CICS to sign off the operator following an XRF takeover.

Specify FORCE if you want CICS to sign off the operator automatically in the event of an XRF takeover. Specify NOFORCE if you want CICS to leave an operator signed on in the event of an XRF takeover.

For information on CICS Security refer to:

- *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise*, SC28-8135
- *CICS/ESA CICS-RACF Security Guide Version 4 Release 1*, SC33-1185
- *ITSC Security in a CICS OS/2-CICS/ESA LU6.2 Environment*, GG24-3939

5.2 IMS/ESA and DB2

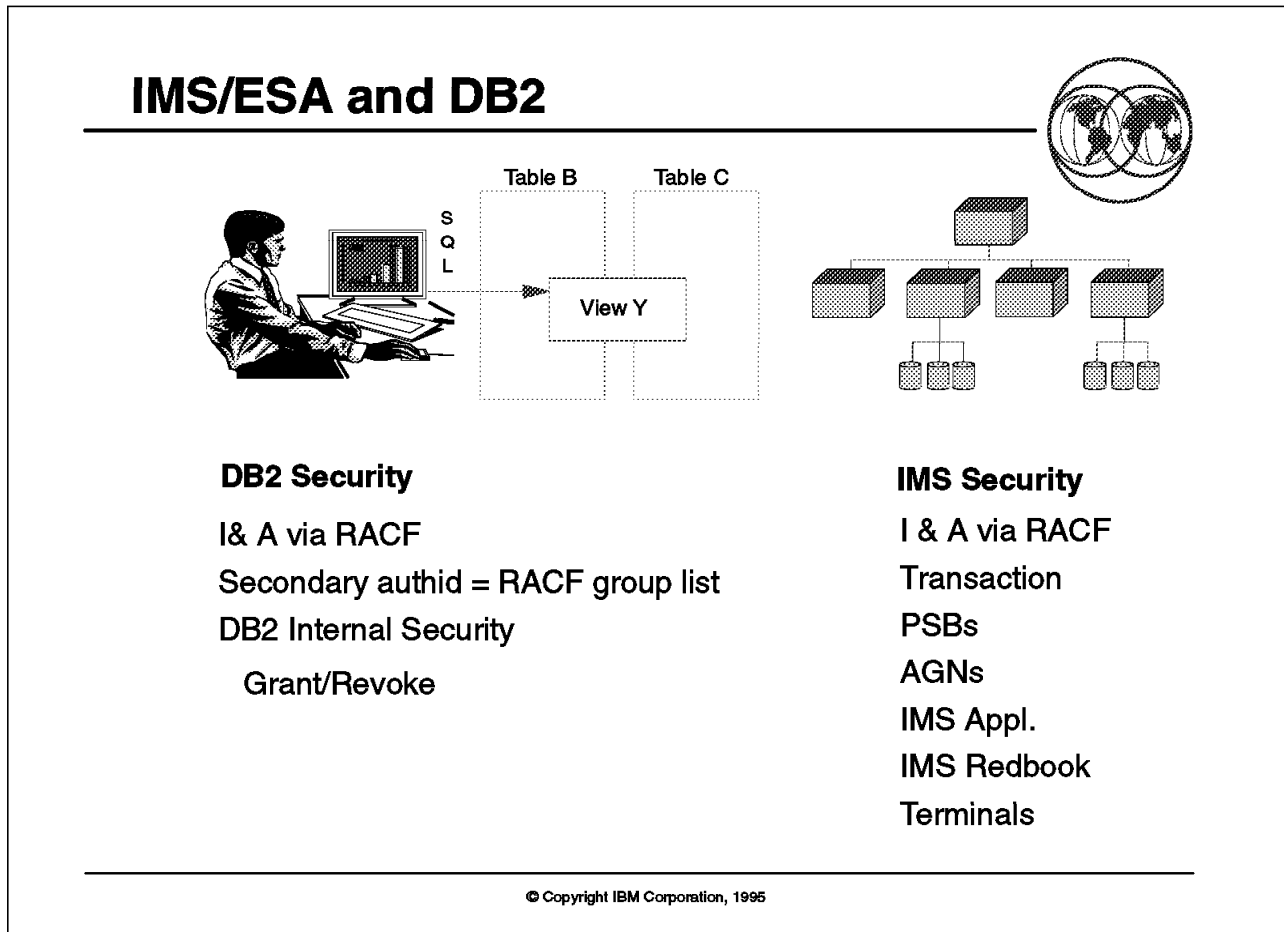


Figure 62. IMS/ESA and DB2

Key Points

User and group management are done by the system security support through RACF.

Control of access to the DBMS objects such as views, program specification blocks (PSBs), transactions, and application resources is done within DB2 and IMS.

Presentation Script

DB2: Controlling database access involves the control of access to the DBMS and its data. In IBM relational DBMSs, this control is implemented in two different layers: outside and inside the DBMS. User and group management are usually done outside the DBMS, whereas the control of access to the DBMS objects, and the permission to perform specific commands and functions is done inside the DBMS.

When we talk about database security, two important concepts come into play: privilege and authorization. The ability to create or access a resource is called privilege. Matching privileges with associated resources is called authorization.

The privileges and authorities combine to form a controlled access system for the DBMS objects.

Users can hold privileges that allow them to take certain actions. This is accomplished by associating a type to the user. Users can also be granted authorization within the DBMS to access specific objects and perform certain commands and functions.

Groups are composed of one or more users. If a user is a member of a group, that user automatically has all privileges granted to the group. Groups are very useful when it is necessary to grant the same set of privileges to many users.

DB2 for MVS: This section briefly reviews the security mechanisms implemented in DB2, describes how DB2 interacts with Resource Access Control Facility (RACF), and explains how to control remote access.

Authorization IDs: There are two levels of access control to DB2 resources. First, users must be authenticated before they can access a DB2 subsystem. Usually a security program outside DB2 control, such as RACF, authenticates users. Second, a user is validated; the user must also be authorized in the DB2 subsystem to access the resources. These authorizations are kept in the DB2 catalog and are based on identifiers (IDs).

The assignment of values, such as user IDs and RACF groups, to authorization IDs is made by either DB2 procedures or user exit routines when the user connects to DB2.

When a user issues a request to DB2, the request is checked against the authorization IDs assigned to that user. If any of the IDs have the required authorization, the request is executed; otherwise, it is rejected.

Privileges within DB2: To execute SQL requests in DB2, users must have specific privileges on the DB2 objects they are trying to access. These privileges are stored in the DB2 catalog. A user can obtain DB2 privileges in different ways, as explained below.

Explicit privileges are obtained as a result of a GRANT statement. Many explicit privileges are associated with each DB2 object. Through these privileges it is possible to obtain complete control of access to DB2 objects.

Implicit privileges are not a result of a GRANT statement. Implicit privileges are associated with the ownership of an object. When a user creates an object, the owner of the object implicitly gains privileges on that object. Some implicit privileges correspond to privileges that can be granted, some do not. Those that correspond can be granted to other users.

A user also can obtain privileges through administrative authorities. When users are granted administrative authorities, they receive a set of privileges associated with that authority. There are many different administrative authorities, each including a set of system privileges and object-related privileges. Administrative authorities include the following:

- System Administrator (SYSADM)

SYSADM is the highest authority in a DB2 subsystem. Among its privileges, it can access all data, create or drop any DB2 object, and change the SQLID to any valid value.

- System Control (SYSCTRL)
SYSCTRL has nearly complete control of the DB2 subsystem, but it cannot access user data, unless it is explicitly granted that privilege.
- System Operator (SYSOPR)
SYSOPR has privileges to issue most DB2 commands, terminate utilities, and carry out other activities associated with the operation of the subsystem.
- Database Administrator (DBADM)
DBADM holds privileges in a specific database. Is the highest authority at the database level.

Administrative authorities can be granted by GRANT statements and are stored in the DB2 catalog. The SYSADM and SYSOPR authorities are also obtained during the installation process of DB2. You can define one or two IDs to be the installation SYSADM and one or two IDs as the installation SYSOPR. These installation authorities are not stored in the DB2 catalog. They are crucial in situations where the catalog is not available and DB2 cannot check authorizations. In such situations, only an installation SYSADM authority can start the DB2 subsystem.

Privileges and administrative authorities granted with a GRANT command can be revoked using the REVOKE command. Implicit privileges of ownership cannot be revoked. You must drop and re-create the object with a new owner.

DB2 and RACF: The use of RACF to protect DB2 resources is recommended. RACF can be used to validate a user who wants to connect to DB2. In addition, RACF can control other security services associated with the DB2 environment:

- User and Group Management
The functions that RACF provides include creation of users and groups, password management, and user authentication. Used together with the DB2 user exits, some of these RACF functions can expand DB2 security. For example, if the exit sets the RACF groups associated with the user as secondary authorization IDs, in DB2 you can grant explicit privileges or administrative authorities to the RACF group ID. If you want to grant these privileges or authorities to a set of users, all you have to do is connect the users to the RACF group, or disconnect them if you want to revoke the privileges.
- Access control to DB2 subsystem
RACF can optionally control access to the DB2 subsystem. By defining RACF profiles, you can specify how to access a DB2 subsystem. Access requests from IMS, CICS, TSO and distributed DB2 environments may be controlled. You can limit access to the DB2 subsystem even more if you allow only specific users or groups to access these profiles.
- Data set protection
Data set protection is required to prevent unauthorized access to DB2 data sets outside the control of DB2. DB2 databases are stored in VSAM data sets. To provide full protection of data in DB2, you must ensure that no process other than DB2 has access to its data sets. RACF can be used for this function.
- Partner-LU validation

In a distributed database environment, partner-LU validation can be implemented through RACF to control the remote systems that can connect to the DB2 server.

IMS/ESA: Users performing tasks must have access to the IMS resources they require, but IMS resources must also be protected from unauthorized use. IMS security facilities provide the means to balance these needs.

You can use RACF for identification (user ID) and authentication (password or PassTicket).

The following IMS Transaction Manager(TM) and IMS DB resources may be protected with RACF:

- Transactions and commands
- IMS databases
- IMS applications
- IMS control region and IMS dependent regions (MPPs, BMPs and IFPs)
- Program specification blocks (PSBs)
- Application group names (AGNs)
- Physical terminals
- Logical terminals (LTERMs)

For information on IMS Security refer to:

- *National Market Support Center: IMS/VS RACF Implementation Guide, G320-5944*

5.3 Distributed Relational DB Architecture

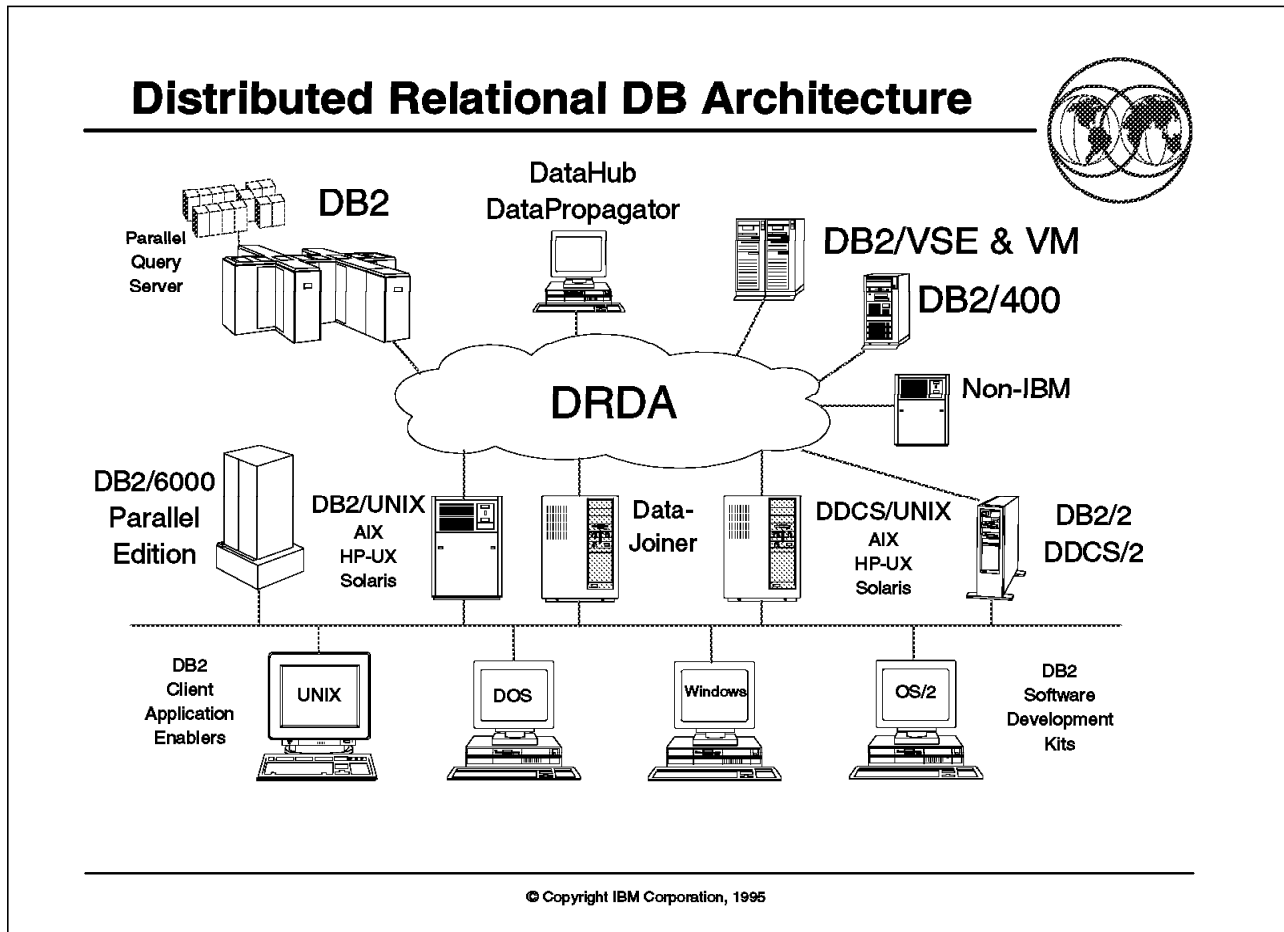


Figure 63. Distributed Relational DB Architecture

Key Points

DRDA is a client/server based architecture where a SQL application as a client accesses a remote relational database as a server.

DRDA security requires that a user ID is authenticated prior to access to the database. Authentication may be via userid/password as is available in VTAM, through DCE mechanisms, or through other security mechanisms such as NetSP.

Presentation Script

DRDA is an open architecture that describes a database protocol to exchange data between different remote database systems. Through DRDA, an application in one system can query and update data in another system, in a consistent manner, with functions to provide security and integrity of the databases. DRDA is the architectural base for the distributed relational database environment.

As DRDA is a published architecture, any software manufacturer that wants to use DRDA in its products can do so. Products that implement DRDA, regardless of who developed them, can participate in a distributed relational database management system.

In a distributed database environment, systems in different locations are connected, providing transparent access to the distributed data. These systems do not necessarily have the same hardware architecture, and probably the software including the DBMSs running on them is not the same. In a distributed environment, the task of connecting these systems while maintaining database integrity is complex.

As an example of this complexity, if you have different hardware architectures, you also have different data representation in each machine. In a connection between a programmable workstation (PWS) and a System /390, you have to provide conversion between ASCII and EBCDIC data. Also, the implementation of the relational database may vary in a few aspects in different platforms. Although most relational DBMSs use SQL for data access, each of them has its own dialect. In addition, each DBMS has its own catalog with a particular structure. These are only examples of the difficulties that arise when you connect databases in a distributed database environment.

An architecture is therefore needed to simplify the task of connecting these different environments by providing the necessary connectivity functions as well as a set of standards that allow the products and the functions to evolve in a consistent manner. An architecture provides a way of connecting different machines and different DBMSs, thus enabling the user to access data no matter how or where it is stored.

Structure: DRDA was designed to be integrated with existing network and system facilities. It is based on the following IBM architectures, which are the building blocks for DRDA:

- Character Data Representation Architecture (CDRA)
CDRA provides character data integrity when data is transmitted between systems with different encoding.
- Formatted Data Object Content Architecture (FD:OCA)
FD:OCA provides the description of the data with information about data types and representation.
- Distributed Data Management (DDM)
DDM describes the model of the database environment. It provides commands, parameters, data objects, and reply messages that work as an intermediate language that all systems understand.
- SNA logical unit type 6.2 (LU 6.2) protocol.
LU 6.2, also known as Advanced Program-to-Program Communication (APPC), is the communication interface between DRDA clients and servers. It provides robust communication functions such as authentication, error alerts, and session security.

Through this structure, DRDA provides location transparency to the application. Once connected to a specific remote database, users can perform operations as if they were accessing local data.

Products That Implement DRDA: Many IBM and non-IBM products implement DRDA today. IBM has relational database manager products that run on different platforms, each one with unique features and capabilities. With DRDA, it is possible to use these products together and take advantage of their unique capabilities.

The IBM relational database products that currently support DRDA are:

- IBM DATABASE 2 (DB2 for MVS)

DB2 is the IBM relational database product for the MVS environment. DB2 is designed to support large databases and a large number of users in a high availability environment.

- IBM DATABASE 2 VM (DB2 for VM)

DB2 for VM is the IBM relational database product for the VM environment. DB2 for VM is the follow-on product of the Structured Query Language/Data System (SQL/DS VM).

- IBM DATABASE 2 VSE (DB2 for VSE)

DB2 for VSE is the IBM relational database product for the VSE environment. DB2 for VSE is the follow-on product of the Structured Query Language/Data System (SQL/DS VSE).

- IBM DATABASE 2 OS/400 (DB2 for OS/400)

DB2 for OS/400 is the new relational database product for OS/400. It provides many new features, such as triggers and referential integrity.

- IBM DATABASE 2 AIX/6000 (DB2 for AIX/6000)

DB2 for AIX is the IBM relational database manager product for the RISC System/6000. The DB2 Client Support/6000 (CS/6000) product provides a client/server environment for both DB2 for AIX and DDCS for AIX products. Thus, applications executing on AIX, OS/2, or DOS/Windows clients can access a database residing on the DB2 for AIX server workstation.

DDCS for AIX is a separate product that provides DRDA support for the RISC System/6000.

- DATABASE 2 OS/2 (DB2 for OS/2)

DB2 for OS/2 is a relational database system designed for the OS/2 environment. DB2 for OS/2 databases can be accessed by OS/2 or DOS/Windows clients.

The DDCS for OS/2 product implements DRDA and works together with DB2 for OS/2 so that DB2 for OS/2 and its clients can access host databases.

- IBM DATABASE 2 for the Solaris Operating Environment

DB2 for the Solaris Operating Environment is a relational database system designed for Sun Microsystems' Solaris operating system environment. The DDCS for the Solaris Operating Environment product implements DRDA so that DB2 for the Solaris Operating Environment and its clients can access host databases.

- IBM DATABASE 2 for HP-UX (DB2 for HP-UX)

DB/2 for HP-UX is a relational database system designed for Hewlett-Packard's HP-UX operating system environment. The DDCS for the HP-UX product implements DRDA so that DB2 for HP-UX and its clients can access host databases.

For more information on DRDA, see *Distributed Relational Database Architecture Reference*, SC26-4651.

5.4 DB2/x Data Security

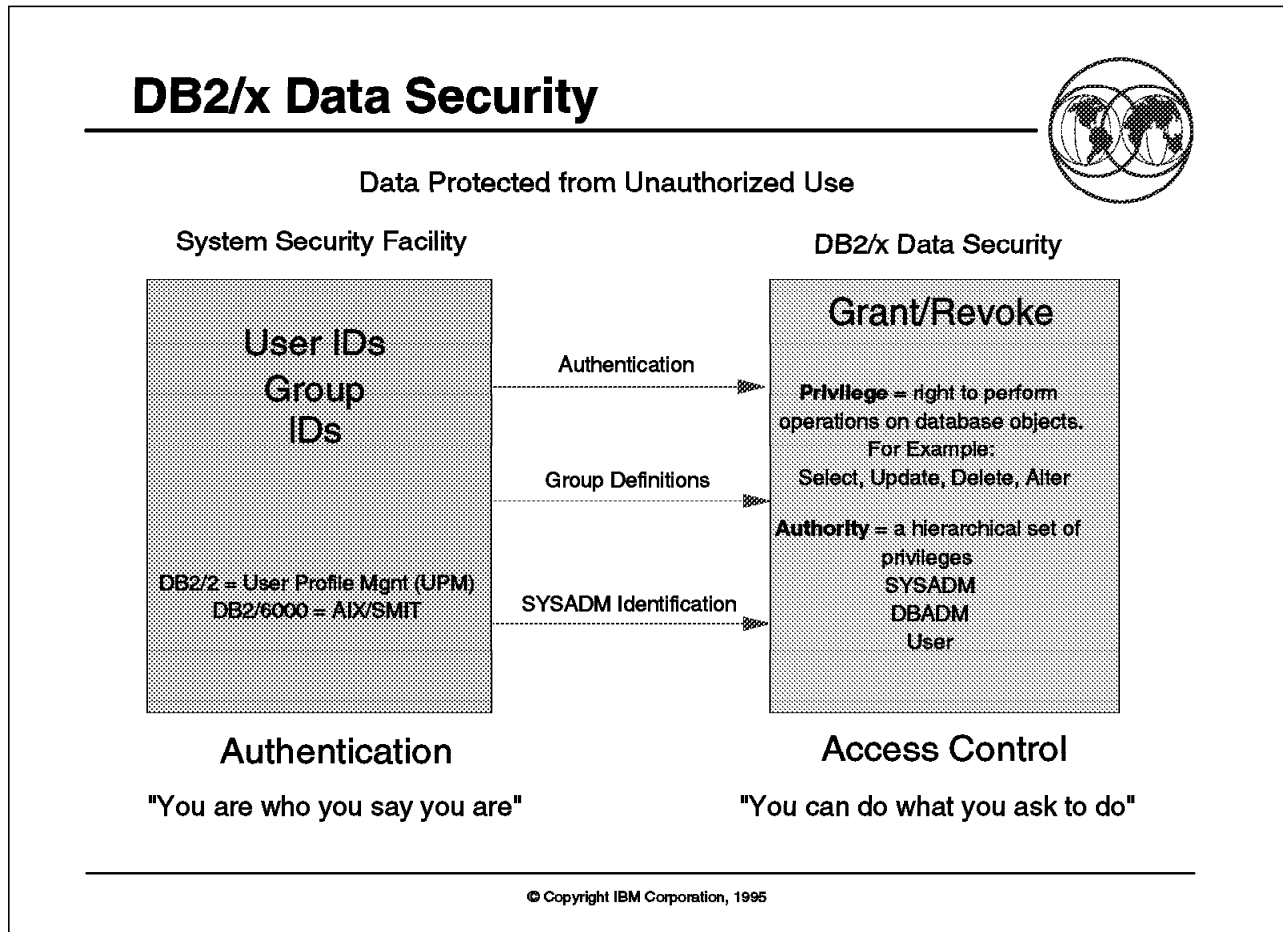


Figure 64. DB2/x Data Security

Key Points

DB2/x security is based on the user and group identification, which determines user authorities and privileges when controlling access to objects.

Presentation Script

DB2 for AIX: This section explains the security mechanisms implemented in DB2 for AIX and the security aspects of remote connections to DRDA servers.

Authorization: DB2 for AIX uses AIX security to provide authentication of users. Users are identified to DB2 for AIX by two types of IDs maintained by the AIX operating system:

- User name (UID)

Identifies a user to the operating system and to DB2 for AIX. A user name always has a UID associated with it.

- Group name (GID)

A groups consists of one or more users.

Privileges in DB2 for AIX can be granted to either the UID or GID. UIDs that are members of a group have all of the privileges granted to that GID. DB2 for AIX also has a PUBLIC ID. Privileges granted to PUBLIC are valid for all users accessing the database.

Authentication: The authentication of a user is performed outside DB2 for AIX by the AIX operating system. However, in a distributed database environment, you can specify in which workstation the authentication process is to be performed by parameters in the catalog database application programming interface (API).

Controlling Access to Database Objects: After a user has been authenticated, to access DB2 for AIX data, the user must also be checked inside DB2 for AIX for the privileges needed to satisfy the request. There are many ways to gain privileges in DB2 for AIX. Through administrative authorities, the user can receive a set of privileges.

There are two administrative authorities:

- SYSADM authority
- DBADM authority

There are three other ways to gain privileges in DB2 for AIX:

- Implicit authorizations, which are obtained when the user creates an object
- Explicit authorizations, which allow specific functions on specific objects
- Indirect authorization associated with programs

DB2 for OS/2: The following section details how access is controlled inside and outside of DB2 for OS/2.

Managing Users and Groups: UPM is the first layer of validation that DB2 for OS/2 uses. To establish a connection, a user must be logged on to a UPM user ID; each request to access DB2 for OS/2 is associated with that user ID.

With UPM it is possible to manage users and groups. DB2 for OS/2 has a special group called PUBLIC. Granting a privilege to the PUBLIC group means granting the privilege to all users.

A user inside UPM always has a type associated with it, which may be one of the following:

- User: has no privileges other than logging on, accessing his or her own information inside UPM, logging off, and whatever other privileges are granted to the PUBLIC group.
- Local administrator: can perform all tasks of a UPM user and has database SYSADM authority within DB2 for OS/2 on the local workstation.
- Administrator: is an administrator not only within DB2 for OS/2 but also within UPM who can perform user and group management tasks.

UPM defines the following types of logons:

- Local: used to access data on the local workstation. The local UPM always performs user ID and password authentication. When accessing a host database, it is not necessary to issue a local logon.

- Node: used to access data at a remote server workstation or to access a host database system.

The user IDs on the database client and the database server workstations do not have to be the same, but using the same string for both user IDs reduces the complexity of the access scheme. If the user ID and password are the same on both the database client and server workstations and the user is logged on locally, the user is automatically logged on (node logon) when connecting to a remote database server. If the user IDs or passwords are different, the user is given a message indicating that the logon was unsuccessful and then prompted to log on for the remote connection.

Controlling Access to Database Objects: Access within DB2 for OS/2 is managed by database services. For the version of DB2 for OS/2 used during this project, database services provide two administrative authorities:

- SYSADM authority
- DBADM authority

DB2 for OS/2 controls authorization in three ways:

- Explicit authorization through privileges controlled with the GRANT and REVOKE statements
- Implicit authorization controlled by creating and dropping objects
- Indirect privileges associated with programs

5.5 Data Administration - DataHub

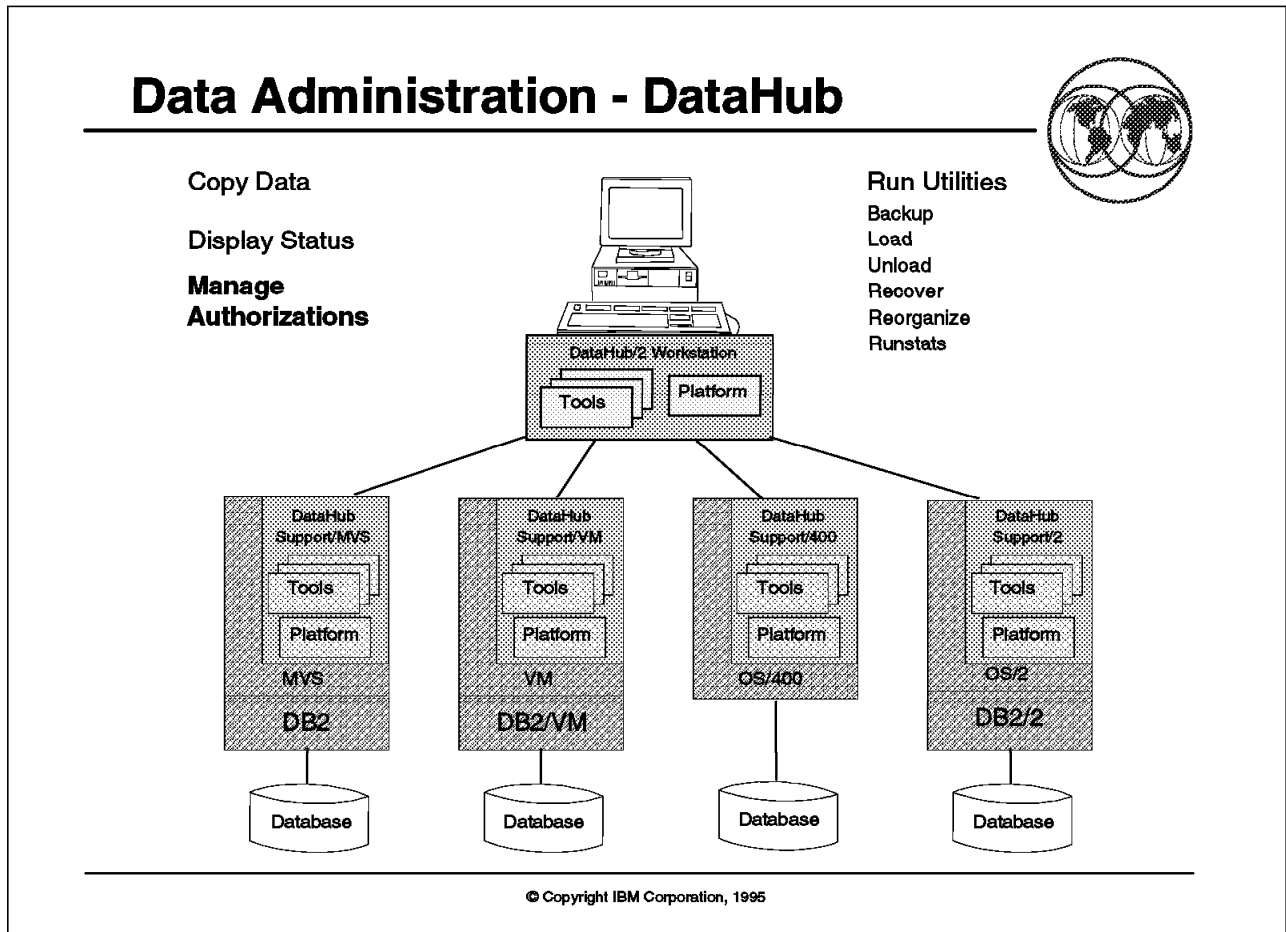


Figure 65. Data Administration - DataHub

Key Points

:1i.security administration

DataHub provides functions that help the database administrator manage authorizations in a DRDA environment:

- Add and delete authorizations
- Copy object and user authorizations
- Perform conversions of authorization types on copy targets

Presentation Script

DataHub is a family of products designed to simplify the management of distributed database environments. With DataHub you can perform system management tasks on any supported relational database using DRDA from a single workstation on the network.

DataHub helps database administrators to create and manage the DRDA environment in the following ways:

- Manage databases from a single point of control

- Display database objects
- Copy data between databases
- Manage authorizations on relational data

DataHub provides many functions that help the database administrator manage the authorizations in a DRDA environment:

- Add and delete authorizations

From the DataHub control workstation, you can add and delete authorizations at any relational database registered to DataHub.

- Copy object and user authorizations

Authorizations for an object or user can be copied from one relational database to another. DataHub evaluates and reports any implications of differences between databases. This function also provides the ability to copy object or user authorizations in a single database.

- Perform conversions of authorization types

During the copy, DataHub uses translation tables to convert a type of authorization at the source to a type of authorization at the target when the type of authorization at the source does not exactly correspond to the type of authorization at the target.

- Processing options

DataHub provides a set of options such as continue or stop after an error, commit frequency at the target environment, and implication reports. Implication reports provide information to the user, such as objects and authorizations affected by cascading delete requests, authorization translations performed, and implications when PUBLIC or groups are involved.

For more information, consult the following publications:

- *DataHub General Information*, GC26-4874
- *DataHub User's Guide*, SC26-3045
- *DataHub Installation and Administration Guide*, SC26-3043

5.6 Structured Query Language (SQL)

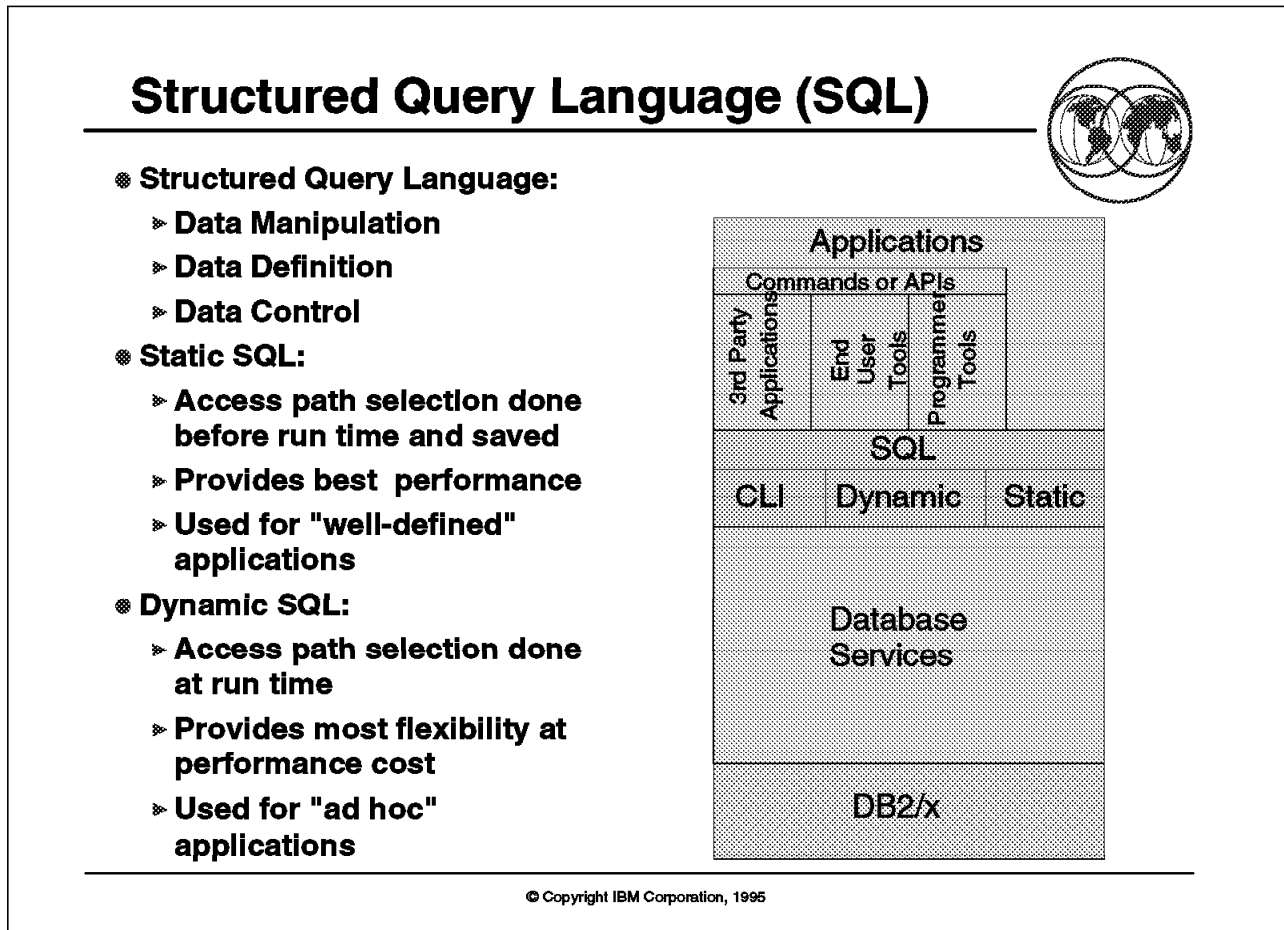


Figure 66. Structured Query Language (SQL)

Key Points

Structured Query Language allows users to define, retrieve, manipulate, and protect information in a relational database.

The IBM SQL security authorization interfaces are GRANT and REVOKE.

Presentation Script

SQL is a standardized language for defining, manipulating and controlling data in a relational database. In accordance with the relational model of data, the database is perceived as a set of tables, relationships are represented by values in tables, and data is retrieved by specifying a result table that can be derived from one or more base tables.

An SQL statement is executed by DB2. All executable SQL statements must be prepared before they can be executed. Preparation is also known as "binding." Preparing a statement determines a sequence of internal operations for its execution. In the process, DB2 tries to select an optimal sequence.

Optimization is especially important when an INSERT, UPDATE, DELETE, or SELECT statement is being prepared. When it optimizes such statements, DB2

can use, among other information, statistics recorded in the catalog for the base tables and a knowledge of the indexes for those tables. The sequence of operations to retrieve the requisite rows from those tables is called the statement's access path.

Two different SQL statements that produce the same result can have very different access paths. DB2 allows you to examine the access paths by applying EXPLAIN to the statements.

SQL statements can be static or dynamic. The method of preparing an SQL statement and the persistence of its operational form distinguish static from dynamic SQL.

- Static SQL

Static SQL comprises the executable statements embedded in source programs. Those statements are prepared when their DBRM is bound, either as a package or a member of an application plan. Static SQL statements need never be rebound unless changes in the environment invalidate them (for example, the dropping of a base table). Static SQL statements could be rebound to advantage when, for instance, new indexes are added for a table that they reference.

- Dynamic SQL

Dynamic SQL comprises the statements whose source form is a character string. The program passes the string to DB2, using the static SQL statement PREPARE or EXECUTE IMMEDIATE. The statement passed is then prepared, and (for EXECUTE IMMEDIATE) is executed immediately afterwards. The operational form of the statement is destroyed on or before the end of the application.

The IBM SQL specification for access to relational data is based on standard ISO and ANSI SQL. SQL allows users to define, retrieve, manipulate and protect information in a relational database. The IBM SQL security authorization interfaces are GRANT and REVOKE. These interfaces are supported by DB2 on all the platforms DB2 runs on.

For more information on the IBM SQL specification, see *IBM SQL Reference*, SC26-3255.

5.7 MQSeries

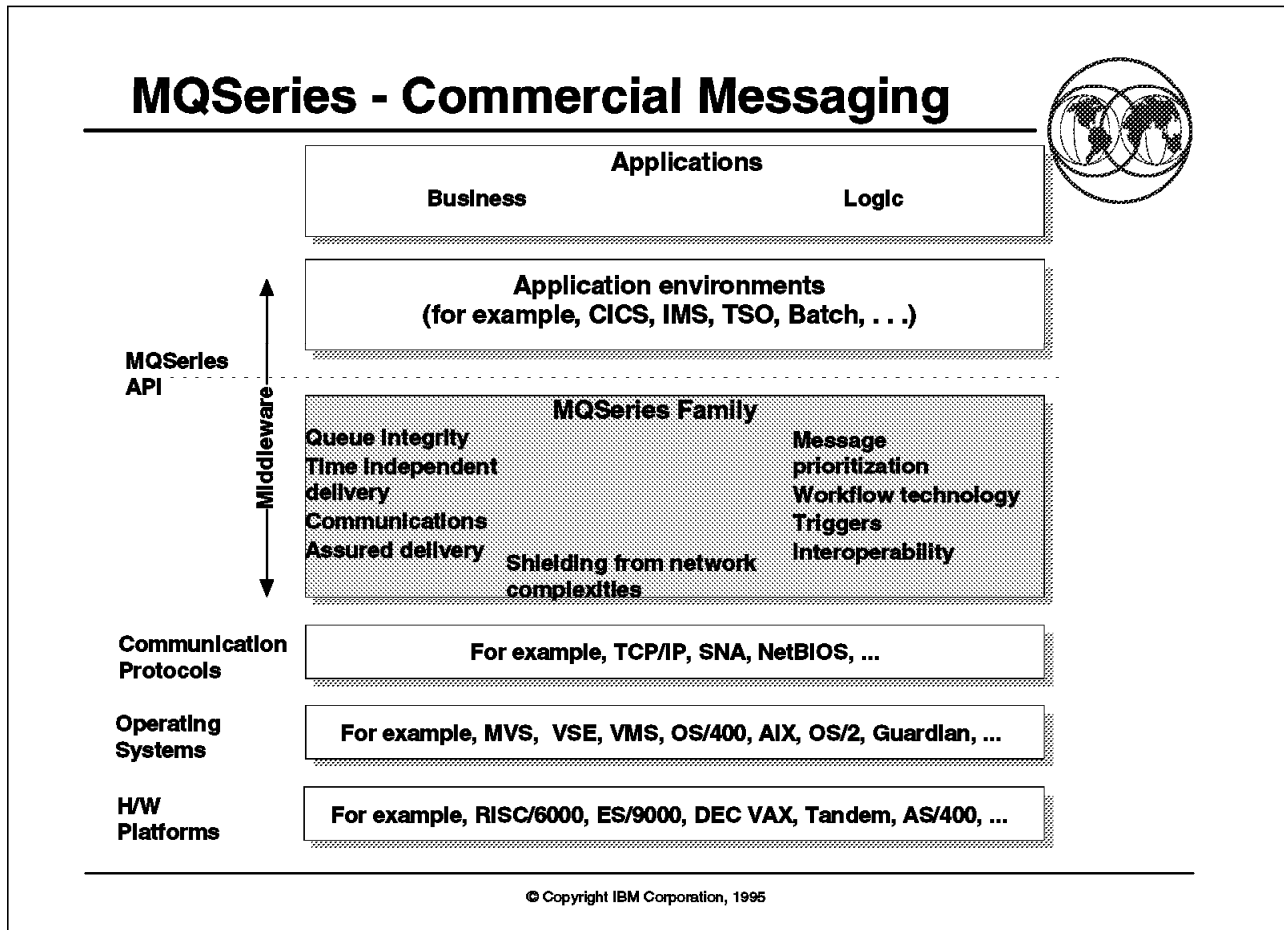


Figure 67. MQSeries

Key Points

MQSeries provides reliable, asynchronous message based communication between applications using a protocol independent format.

MQSeries has been developed with an extensive security interface which calls an external security product, for example, RACF.

Presentation Script

MQSeries is a set of products providing reliable, asynchronous message based communication *between applications*. The MQSeries product set covers a wide base of all IBM platforms, and many non-IBM platforms. Further, MQSeries exchanges messages between systems using a protocol independent format, making the choice of protocol fairly arbitrary.

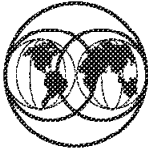
The products are, architecturally speaking, resource managers and, as such, do not attempt to provide any internal security service. Instead, it is preferable to use the security services provided by the native operating systems. Because MQSeries is available on such a diversity of platforms and protocols, the provision of uniform security support is greatly hindered. To ease this difficulty, MQSeries provides a generic set of exit points where security services can be

“installed,” both for authorization and authentication processing. For some platforms, services are provided, either by the operating system or MQSeries, and for other platforms, it is left to the end user to provide the installable services.

For authorization, there is a set of calls provided by an installable authorization service. It is assumed that a previously authenticated name is passed to MQSeries which then uses that name in authorization calls. This security service is available for MQSeries Version 2 products. The MVS platform, which already has the SAF interface for security, is an exception in that MQSeries for MVS uses the SAF interface instead of an MQSeries installable service.

Authentication of other MQSeries queue managers may be required when MQSeries implementations exchange messages. The communications components of MQSeries handle any required authentication by providing exit points where an external authentication service can be called. There is no authentication code included within MQSeries. All MQSeries Version 2 products support these security exit points. There are corresponding exit points provided to allow for authentication of user IDs associated with individual messages.

ACF/VTAM



- Available on MVS, VM and VSE operating systems

- Controls and verifies terminal, logons, connections and applications with RACF

- LU6.2 Bind Security with RACF

- SNA Session Level Encryption (SSLE) support

- Session Management Exit (SME)

© Copyright IBM Corporation, 1995

Figure 68. ACF/VTAM

Key Points

ACF/VTAM is IBM's strategic SNA program product for MVS, VM and VSE operating systems.

ACF/VTAM offers SNA, RACF and encryption security services.

Presentation Script

ACF/VTAM directs the transmission of data between application programs and terminals in a telecommunication network.

Using VTAM facilities, an installation can control the use of sensitive resources, such as specific terminals and application programs. These controls can be performed at various points in the telecommunication processing. Depending on the desired type of control, an installation can exercise security controls through the network control program (NCP), VTAM, an authorization exit routine (SME), or the application programs.

SME is called for a wide range of functions, covering session authorization, connection, and accounting.

VTAM works with RACF to control and protect resources by:

- Verifying terminal identifications
- Verifying logons
- Controlling the connections between application programs and terminals
- Controlling which application programs can use VTAM
- Restricting an application program's use of VTAM facilities

Peer-to-peer application communications using LU6.2 have several options for identifying the partner:

- Session-level LU-LU verification can verify the identity of an LU to its session partner during activation of the session.
- User ID verification can allow an LU to inform its partner that the user ID and password for a requested conversation have been already verified. Or the LU can send to the partner both the user ID and the password and let it perform the verification process itself.
- Partner LU verification is a 3-flow exchange between the two LUs, with each LU using an LU-LU password and the DES algorithm. This exchange is called LU-LU verification.

In addition, VTAM on MVS has an optional SNA Session Level Encryption (SSLE) support to assure the security of data as it passes through the network. This option, when used with either ICRF with ICSF/MVS, Programmed Cryptographic Facility or the IBM Transaction Security System, allows users to establish, control and terminate access to stations and application programs with cryptographic sessions. This support is transparent to the application subsystems.

5.9 NetView Access Services (NV/AS)

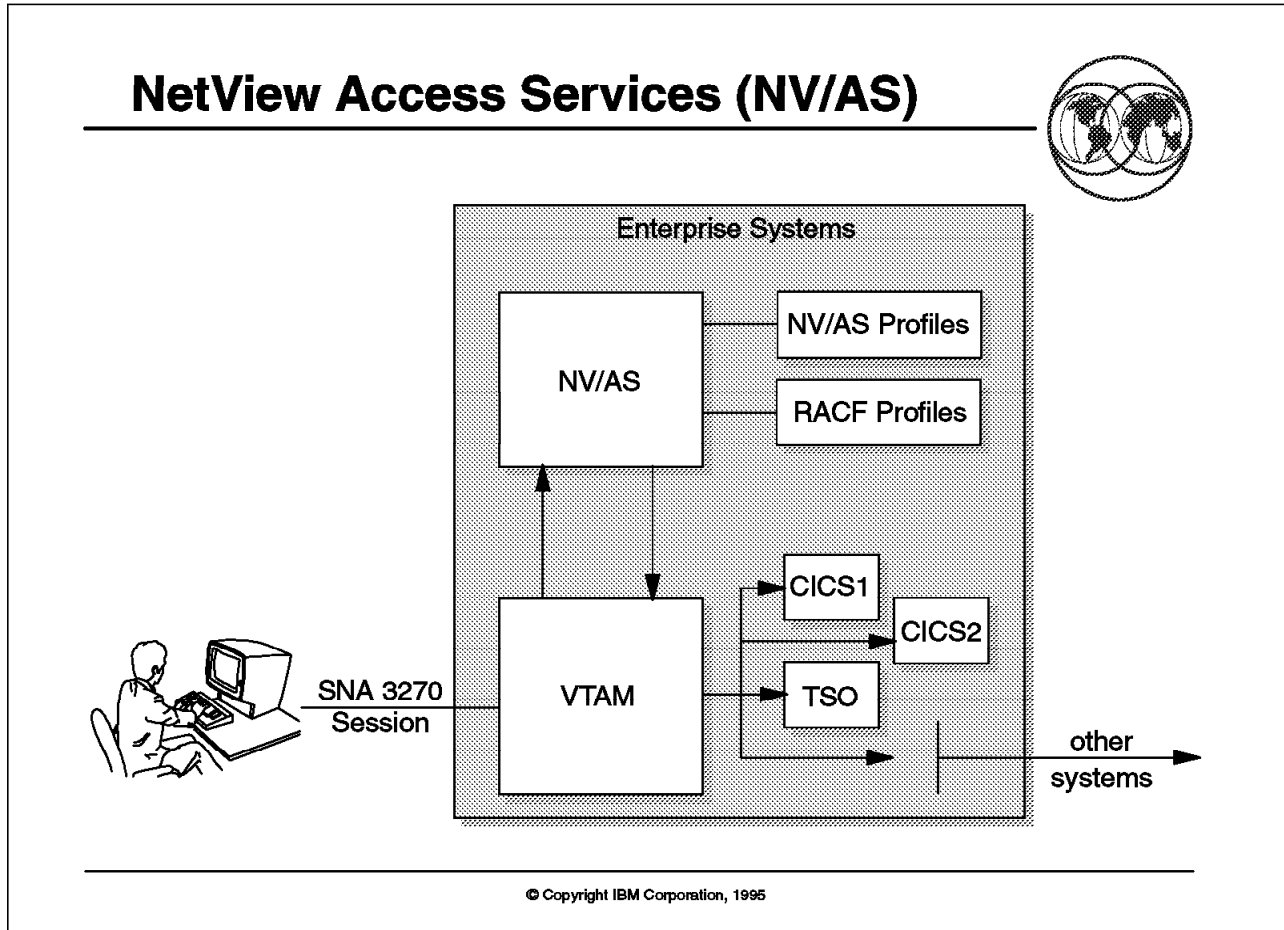


Figure 69. NetView Access Services (NV/AS)

Key Points

Netview Access Services provides front-end authorized application selection and automatic “single signon” services.

Presentation Script

NetView Access Services (NV/AS) is available for MVS and VM systems.

NetView Access Services can provide concurrent access to different applications on one or more host systems from a single 3270 terminal. It can be used to secure access to both networks and applications, by acting as a “welcome” application and front-end security system for network access, and it can also be used to perform automatic logon to those applications that the user is authorized to access.

The security features of NV/AS include the ability to control user-profile access, to choose the level of logon procedures that are automated, and to select ways inactive users can be timed out from an application, or from NV/AS itself. These controls are performed through an external security manager, such as RACF, or through NV/AS internal tables and profiles.

5.10 NetSP Secured Logon Coordinator

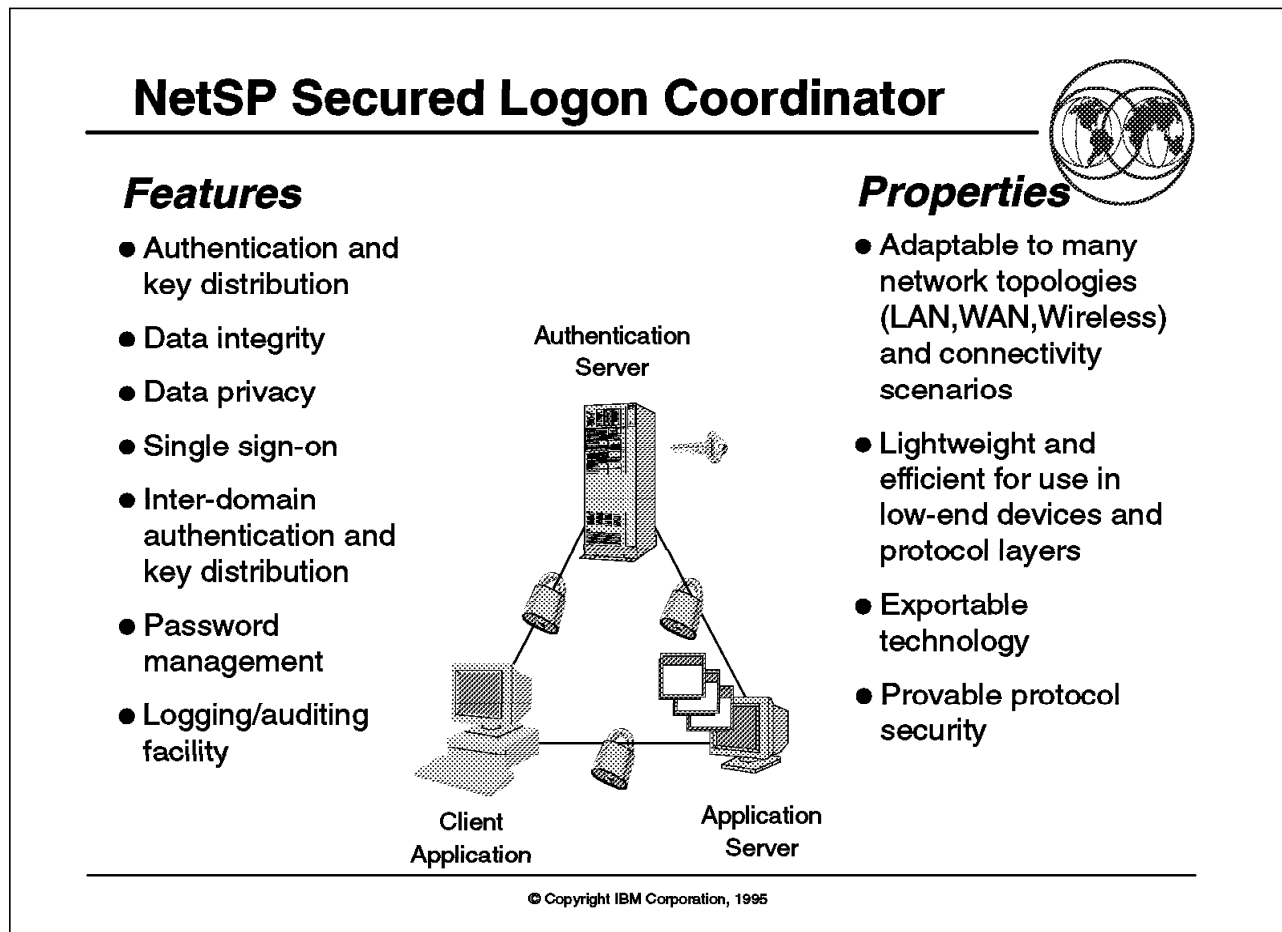


Figure 70. NetSP Secured Logon Coordinator

Key Points

The NetSP Secured Logon Coordinator (SLC) product provides secure single signon to host and LAN applications based on third-party authentication protocols.

NetSP SLC has been designed in concert with RACF to enable a one-time PassTicket to be used for mainframe logon instead of passwords that would flow in clear text.

Presentation Script

Network Security Product Secured Logon Coordinator features include:

- Secured Sign-On using RACF PassTicket

NetSP supports a one-time-use encoded password substitute (PassTicket) for sign-on to RACF-protected applications. This facility ensures that no passwords are sent over a network in "clear text."

- Single Sign-On to Multiple Applications

NetSP makes it easy to access multiple network resources with a single sign-on command. With one NetSP password, you can access resources

including OS/2 LAN Server, NetWare server, RACF applications and client server applications using the GSS API.

This is a major benefit for users who have to manually maintain userids and passwords on multiple host and LAN platforms.

- Third-Party Authentication

NetSP offers authentication of the identities of users and applications using a trusted third-party server.

- Callable Security Services

NetSP supports the industry standard Internet GSS API (RFC 1508 and RFC 1509) that can be used in any of your application programs.

- Data Masking

To mask data sent between session partners, NetSP uses the Commercial Data Masking Facility (CDMF) technology, a 40-bit encryption method that is exportable.

- Data Integrity

NetSP supports data checking through the GSS API to expose unauthorized changes or substitutions to data transmissions.

- Audit Facility

NetSP's audit capabilities not only record authentication requests, but also enable you to analyze unauthorized attempts to access the network.

- Password Aging

NetSP can be used to enforce password restrictions and regular password changes.

- Multiple User Login Support

NetSP allows secure individual logins for multiple users on a single workstation.

NetSP solves the problem of distributed security by combining robust authentication technologies and industry standards. NetSP has the following advantages:

- Minimizes security exposures

The NetSP Security Server eliminates the exposure of transmitting passwords in clear text across the network. Plus, its audit facility tracks failed authentications, so that you can track unauthorized attempts at access.

- Simplifies security processes

With NetSP's single sign-on facility, users can access multiple applications using a single NetSP password. Fewer passwords reduce demand on support personnel. Users have easy access to applications using NetSP's simple graphical interface.

- Ensures consistency across the network

NetSP provides consistent security for applications in a heterogeneous network. You can secure OS/2, AIX/6000, DOS, Hewlett-Packard UX, Sun Solaris, or Windows systems across many protocols with one NetSP interface.

- Enhances productivity today

Because NetSP supports the Generic Security Services Application Programming Interface (GSS API), an industry-wide security standard, you can use simple verbs instead of creating new security routines for every application. As you make security upgrades in your network, the GSS API lets you migrate your applications without changing them.

- Protects your investment tomorrow

NetSP supports more platforms and vendors than any comparable product on the market today. NetSP's platform flexibility protects your hardware and software development investment. The GSS API standard also protects your software development investment.

For more information on the Network Security Program, see *Network Security Program Product Guide*, SC31-6500.

Cryptographic Security

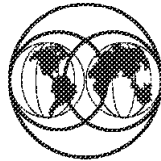


Figure 71. Cryptographic Security

6.1 Why Cryptography?

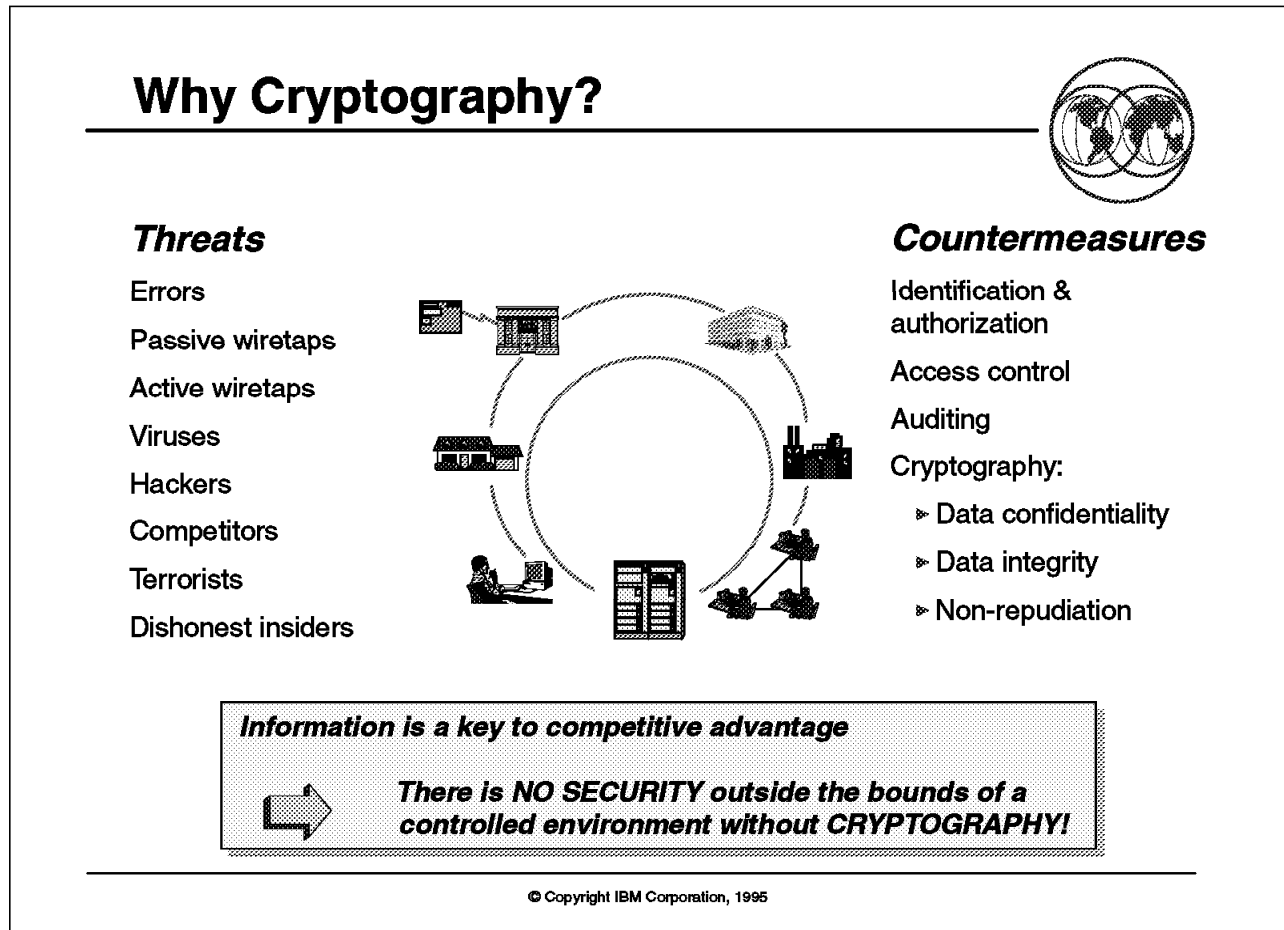


Figure 72. Why Cryptography?

Key Points

- Protecting information is key to maintaining a competitive advantage.
- Threats can jeopardize the protection of sensitive information.
- Cryptography is necessary to guarantee security outside the bounds of a single processor.

Presentation Script

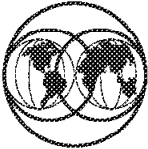
The word *cryptography* literally means secret writing. Throughout history, information has been an asset that provided the owner a *competitive advantage*. Failure to adequately protect information has had significant consequences for individuals, companies and countries. *Threats* exist due to errors, passive wiretaps, active wiretaps, viruses, hackers, competitors, terrorists and dishonest insiders. Today, an enterprise risks losing their competitive advantage and market share through industrial espionage or losses through law suits from not exercising due care in protecting sensitive information about others.

Not only is confidentiality important, but integrity (or the assurance of validity) of information is critical to business success across the world. Commercial enterprises send contracts, private documents, money orders, and other legal

documents across communications networks, all of which must arrive with the same content with which they were dispatched. Before the electronic age, paper, signatures, and seals were used to guarantee the integrity of a document. With electronic communication of information, another mechanism is required.

Cryptography is the only known practical method of protecting information transmitted electronically through communications networks. It can also be an economical way to protect stored information. As computing systems become increasingly exposed through increased computer literacy and reliance on distributed computing, the pervasiveness of cryptography will increase as industry seeks ways to protect their information assets.

Cryptographic Algorithms



- **Data Encryption Algorithm (DEA):**
 - ▶ Symmetric algorithm, keys are secret
 - ▶ Frequently referred to as DES (Data Encryption Standard)
 - ▶ Published algorithm
 - ▶ Export restricted

- **Commercial Data Masking Facility (CDMF):**
 - ▶ Symmetric algorithm
 - ▶ Frequently referred to as limited DES
 - ▶ Generally exportable

- **Rivest Shamir Adleman (RSA) Algorithm:**
 - ▶ Asymmetric algorithm ('Public Key Algorithm')
 - ▶ Key pair: one public, one secret

© Copyright IBM Corporation, 1995

Figure 73. Cryptographic Algorithms

Key Points

There are two fundamental categories of cryptographic algorithms:

- Symmetric or secret key

IBM supports the Data Encryption Algorithm for symmetric encryption. The export of DES is restricted outside the United States and Canada or the banking industry.

Therefore, IBM also provides Commercial Data Masking Facility (CDMF) as an exportable limited DES implementation.

- Asymmetric or public key

IBM supports the Rivest Shamir Adleman (RSA) Public Key Algorithm for asymmetric encryption.

Presentation Script

Cryptographic algorithms are categorized as either symmetric key (secret key) or asymmetric key (public key) algorithms with different usage attributes, security capabilities and performance characteristics.

In a *symmetric* key algorithm, both the sender and the recipient know the single secret key and must maintain the integrity and confidentiality of the key value. One requirement to use symmetric key algorithms is the initial key must be exchanged between the parties in a secure manner preserving both integrity and confidentiality. This is often solved by using a bonded courier or by using a device such as a smart card (a device containing a small crypto processor and memory within a chip enclosed in a tamper-resistant credit card). Examples of symmetric key algorithms are the Data Encryption Algorithm (DEA) and the exportable Commercial Data Masking Facility (CDMF).

An *asymmetric* algorithm has a unique pair of keys consisting of one public key which can be known by everyone and one private key that is kept in the secure environment of the owner. The confidentiality and integrity of the private key must be maintained by the system so that the owner of the key is assured that these requirements are met. Before using a public key, a user must be assured of the integrity of the key value and that the public key is truly associated with the claimed owner. The cryptographic system typically aids the user in meeting these requirements. A digital signature can be created using the private key such that this digital signature can be verified by everybody who knows the appropriate unique public key, but it cannot be recreated without access to the private key. Digital signatures are of value where legal documents such as orders, invoices, contracts, debentures, and so forth are electronically transmitted. Some asymmetric algorithms can also be used to distribute a symmetric key. Examples of asymmetric key algorithms are the Rivest Shamir Adleman (RSA) algorithm and the Digital Signature Standard (DSS).

The digital signature provides:

- Authentication of origin - proof of the identity of the sender.
- Authentication of content - proof that the signed message has not been altered.

Symmetric algorithms are typically faster than asymmetric algorithms. For example, comparable implementations of the DEA are usually over 100 times faster than implementations of RSA.

Data Encryption Standard (DES)

The Data Encryption Standard (DES), frequently referred to as the Data Encryption Algorithm (DEA), is a symmetric key algorithm with an input and output blocksize of 64 bits and a key of 64 bits. The key contains 56 independent bits that determine the specific cryptographic transformation and 8 bits that may be used for parity checking. The DES is defined in USA Federal Information Processing Standard (FIPS) 46-2; the DEA is defined in ANSI standard X3.92. The DES was designed by cryptographers at IBM with assistance from NSA. The DES is the best known and most used commercial cryptographic algorithm. It is used to protect stored files, messages, Personal Information Numbers (PINs), Electronic Funds Transfer (EFT) transactions, and cryptographic keys.

The DES was recertified in 1992 by the U.S. National Institute of Standards and Technology (NIST).

Commercial Data Masking Facility (CDMF)

The Commercial Data Masking Facility (CDMF) algorithm is a new scrambling technique for data confidentiality. The CDMF algorithm is intended as a substitute for the Data Encryption Algorithm (DEA) in cryptographic products exported to customers who have heretofore been unable to receive products with DEA-based data confidentiality services due to government regulations. A CDMF key is 64 bits, of which 56 determine the data scrambling algorithm and 8 which may be used for key parity. However, a CDMF key has an effective strength of 40 DEA-key bits. CDMF is currently implemented in the Transaction Security System and other products, with requirements to support confidentiality in additional future product environments.

Public Key Algorithm (PKA)

The most common asymmetric algorithm is the RSA algorithm, named after its inventors: Rivest, Shamir, and Adleman. The RSA algorithm is based on the mathematical problem of factoring a large composite number that is the result of multiplying two large prime numbers together.

RSA is currently implemented in the Transaction Security System products, with requirements for future support in other products.

6.3 Keys Within Cryptography

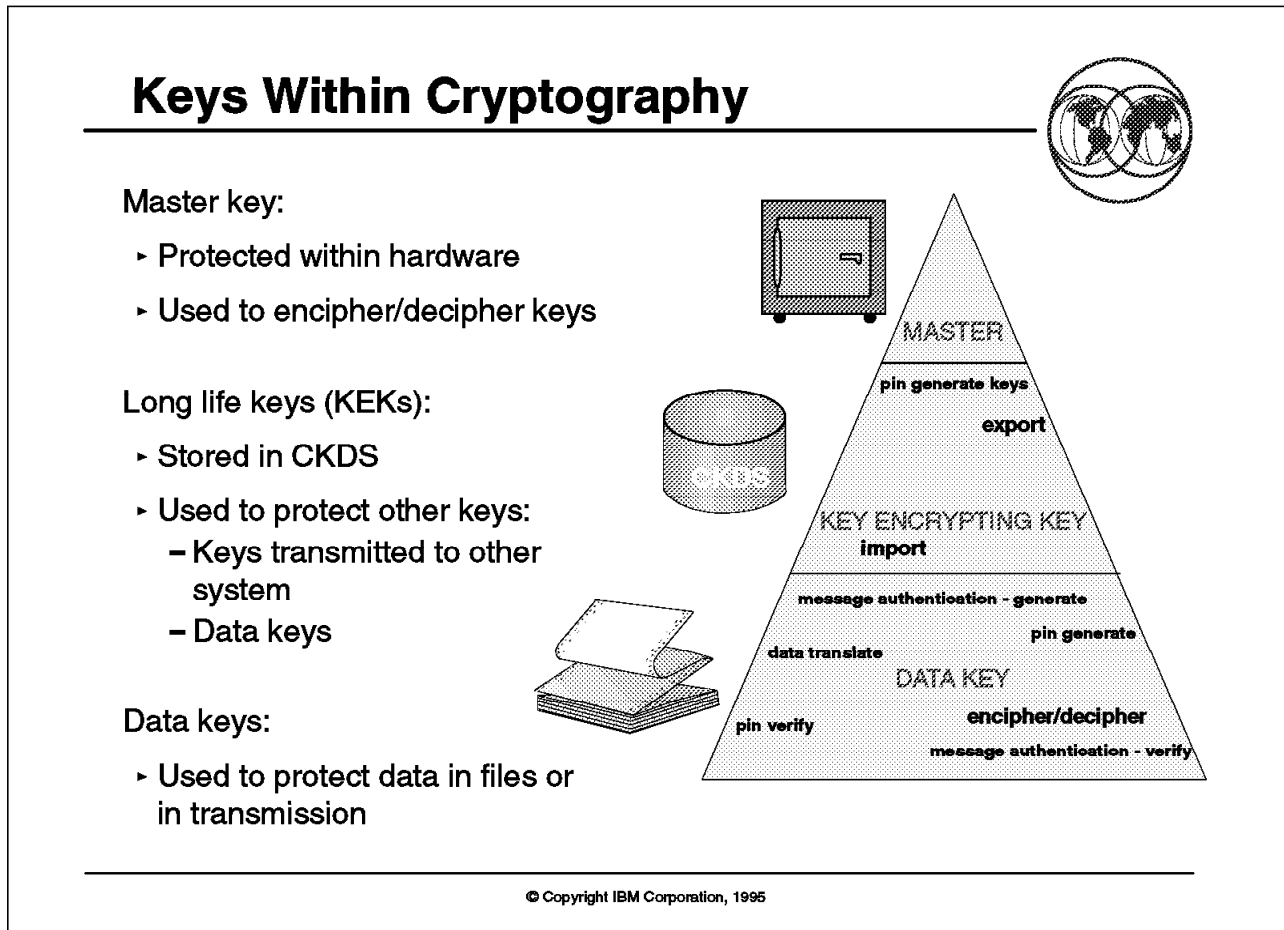


Figure 74. Keys Within Cryptography

Key Points

- Keys are the anchor point for cryptographic algorithms.
- Cryptography is used for secure data and key exchange between two parties.
- The key hierarchy defines three levels of cryptographic keys.
- Effective key management is essential to successful cryptography.

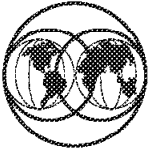
Presentation Script

Effective key management is essential to successful cryptography. Since the algorithm is usually public knowledge, the security of the data depends on the security of the key used to protect the data. Protected data may be obtained by an adversary, but without access to the cryptographic key, the data remains secure.

Since the secret key provides access to the enciphered data, it should be shared by only those needing the data and used only for its intended function. These requirements translate into having many key types that are organized hierarchically. The three key levels and the types defined in each are as follows:

- At the highest level is the master key. It is a 128-bit key kept in the clear in the cryptographic facility. It is used only to encrypt other keys on the system.
- The next level of keys is the key encrypting key (KEK). Two types of KEKs are available, an importer key and an exporter key. These keys are 128-byte unidirectional keys that are used to distribute keys among systems, or encrypt keys stored with archived encrypted data. An exporter key protects keys of any type that are sent from a system. An importer key protects keys of any type that are sent from another system to this system or keys that are archived so they can be imported at a later time. The exported key at the sender has the same clear value as the importer key at the receiver. The key encrypting keys (KEKs) are stored in the Cryptographic Key Data Set (CKDS).
RSA keys may also be used to protect the exchange of other keys.
- The lowest level of keys used to protect information is the following:
 - **Data encryption key** - a 64- or 40-bit key used to encipher and decipher data for data privacy purposes.
 - **Data translation key** - a 64- or 40-bit key used to protect data that is transmitted to an intermediate system when the sender and receiver do not share a common key.
 - **MAC generation key** - a 64-bit key used to generate a MAC that is transmitted along with a message for data integrity purposes.
 - **MAC verification key** - a 64-bit key used to verify a MAC that was transmitted along with a message for data integrity.
 - **PIN generation key** - a 128- or 64-byte key used to generate clear PINs or clear PIN offsets.
 - **PIN verification key** - a 128- or 64-byte key used to verify a trial PIN.
 - **PIN encryption key** - a 128-byte unidirectional key used for PIN translation. The outbound PIN encrypting key at the sending system has the same clear value as the inbound PIN encrypting key at the receiving system.
 - **Signature key** - a 512- to 1024-bit key used to generate and verify digital signatures.

Cryptographic Strategy



- **Fundamental to all Security Services**
- **Based on Data Encryption Standard**
- **Extended for RSA Public Key Algorithm**
- **Enhanced with CDMF for Export**
- **Implemented in IBM Common Cryptographic Architecture (CCA)**
- **IBM is working closely with acknowledged consortiums world wide in developing and defining Application Interfaces and Architectures, for example X/Open GCS-API**
- **Implement them as they evolve across strategic platforms**

© Copyright IBM Corporation, 1995

Figure 75. Cryptographic Strategy

Key Points

- Cryptography is key to all other security services.
- IBM intends to implement cryptography across strategic platforms.
- IBM intends to support standard key algorithms such as DES and RSA PKA.
- IBM intends to support standard key programming interfaces as they evolve.

Presentation Script

The IBM Cryptographic Strategy is to provide cryptographic products driven by the requirements of the market, which are standards-compliant, open-systems solutions, capable of exploiting the advantages of both symmetric (DES, CDMF) and asymmetric (RSA) cryptography. To that end, IBM is proactive in the standards arena, utilizing the skills and knowledge of its cryptographers to meet customer needs. IBM is active in the X/Open working group designing the Generic Cryptographic Services Application Programming Interface (GCS-API).

IBM also developed the Common Cryptographic Architecture described in the next foil.

6.5 Common Cryptographic Architecture (CCA)

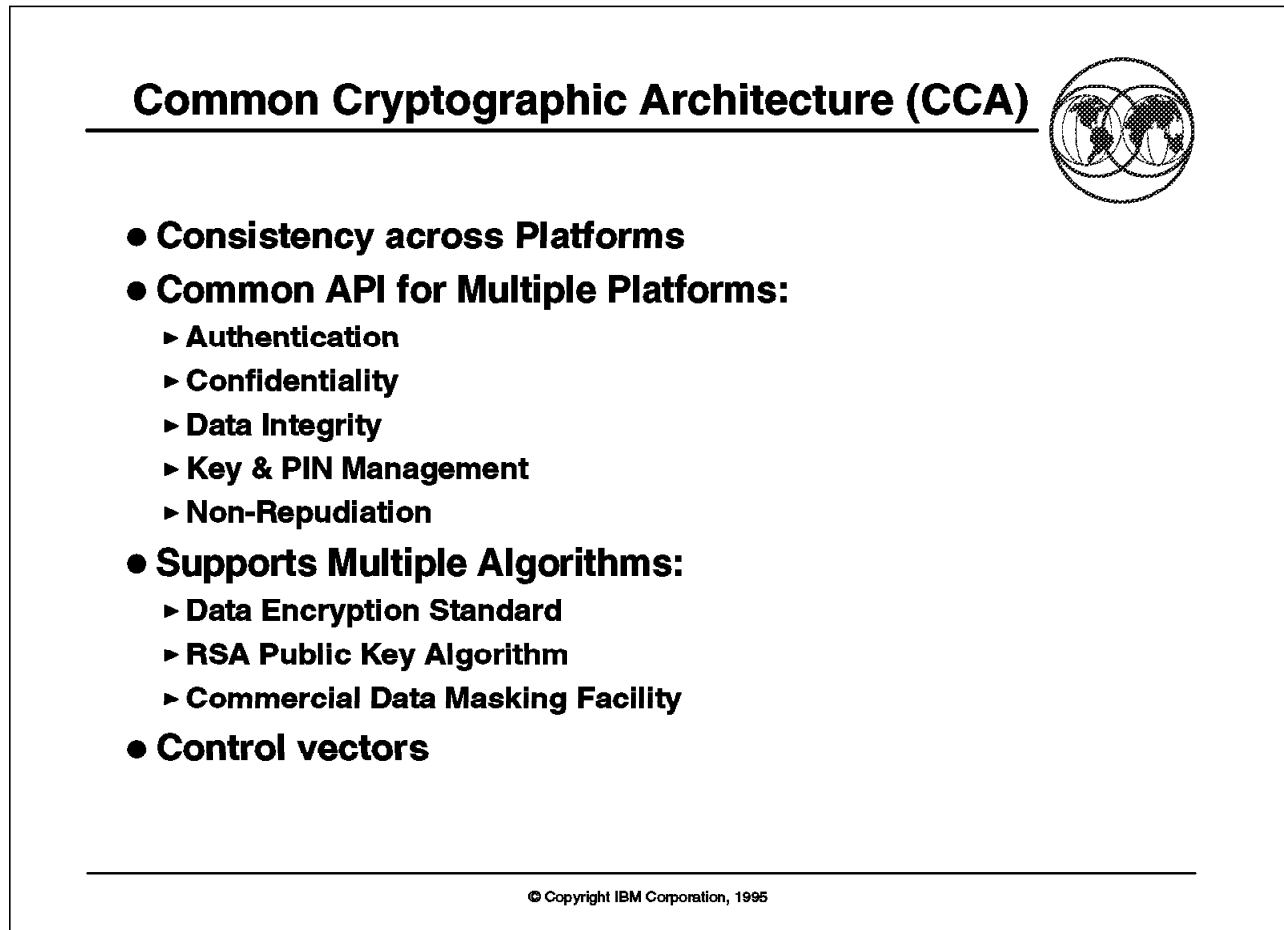


Figure 76. Common Cryptographic Architecture (CCA)

Key Points

- CCA provides consistent functions across platforms.
- CCA provides a common programming interface.
- CCA addresses several services of the Security Architecture:
 - Authentication
 - Confidentiality
 - Data Integrity
 - Key & PIN Management
 - Non-Repudiation
- CCA supports multiple algorithms.
- CCA introduces control vectors for key separation.

Presentation Script

The IBM Common Cryptographic Architecture defines a set of cryptographic functions, external interfaces, and a set of key management rules.

The Common Cryptographic Architecture was developed to:

- Ensure consistent implementation of cryptographic services across IBM platforms
- Facilitate enterprise-wide security solutions
- Provide interoperability guidance to other vendors of cryptographic products
- Allow for compatibility with previous implementations of cryptographic services
- Prevent interface attacks across the cryptographic API

Highlights of the Common Cryptographic Architecture include:

- Defines a unified application programming interface for the following services:
 - Cryptographic key management
 - Data encryption
 - Message authentication and verification
 - Modification detection
 - Personal identification number (PIN) management
 - PIN generation and verification
 - Signature generation and verification
- Provides added security capability for the Identification and Authentication, Data Integrity, Confidentiality, Non-Repudiation and Security Management facilities as described in the IBM Security Architecture:
 - Identification and Authentication - PIN Generation and Verification as an authentication mechanism to assure an individual is who he or she claims to be.
 - Confidentiality - Data encryption and decryption services for the protection of sensitive and valuable data.
 - Data Integrity - Message Authentication Code generation and verification and Modification Detection Code generation as a means to assure data is not modified
 - Key & PIN Management - Encryption key management and PIN management services to generate, install, distribute, maintain, and destroy encryption keys and PINs.
 - Non-Repudiation - RSA Public Key Algorithm for digital signature generation and verification.
- *Control vectors* - a method for controlling cryptographic key usage. Each cryptographic key has an associated control vector that defines the permitted uses of the key within the cryptographic system. At key generation, the control vector is cryptographically coupled to the key via a special encryption process. Each encrypted key and control vector is stored and distributed between cryptographic systems as a single token. Decryption of a key for use within cryptographic hardware requires respecification of the control vector. As part of the decryption process, the cryptographic hardware also verifies that the requested use of the key is authorized by the control vector.
- Supports the following International and U.S. standards:
 - ANSI X3.92 - 1981 Data Encryption Algorithm (DEA)

- ANSI X3.106 - 1983 Modes of DEA Operation
- Electronic Code Book Mode (ECB)
- Cipher Block Chaining Mode (CBC)
- FIPS 46-1 - 1988 Data Encryption Standard (DES)
- ISO 8730 Banking Requirements for Message Authentication (Wholesale)
- ISO 8731 Banking Approved Algorithms for Message Authentication - Part 1: DES-1 Algorithm
- ANSI X9.9 - 1986 Financial Institution Message Authentication (Wholesale)
- ANSI X9.23 - 1988 Encryption of Wholesale Financial Messages
- ISO 9564 Personal Identification Number Management and Security Part 1 - PIN Protection Principles and Technique
- ANSI X9.8 - 1982 Personal Identification Number (PIN) Management and Security
- ANSI X9.17 Wholesale Banking Key Management

For more information on the Common Cryptographic Architecture see:

- *Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference, SC40-1675*
- *Common Cryptographic Architecture: Cryptographic Application Programming Interface Reference - Public Key Algorithm, SC40-1676*

6.6 IBM CCA Offerings

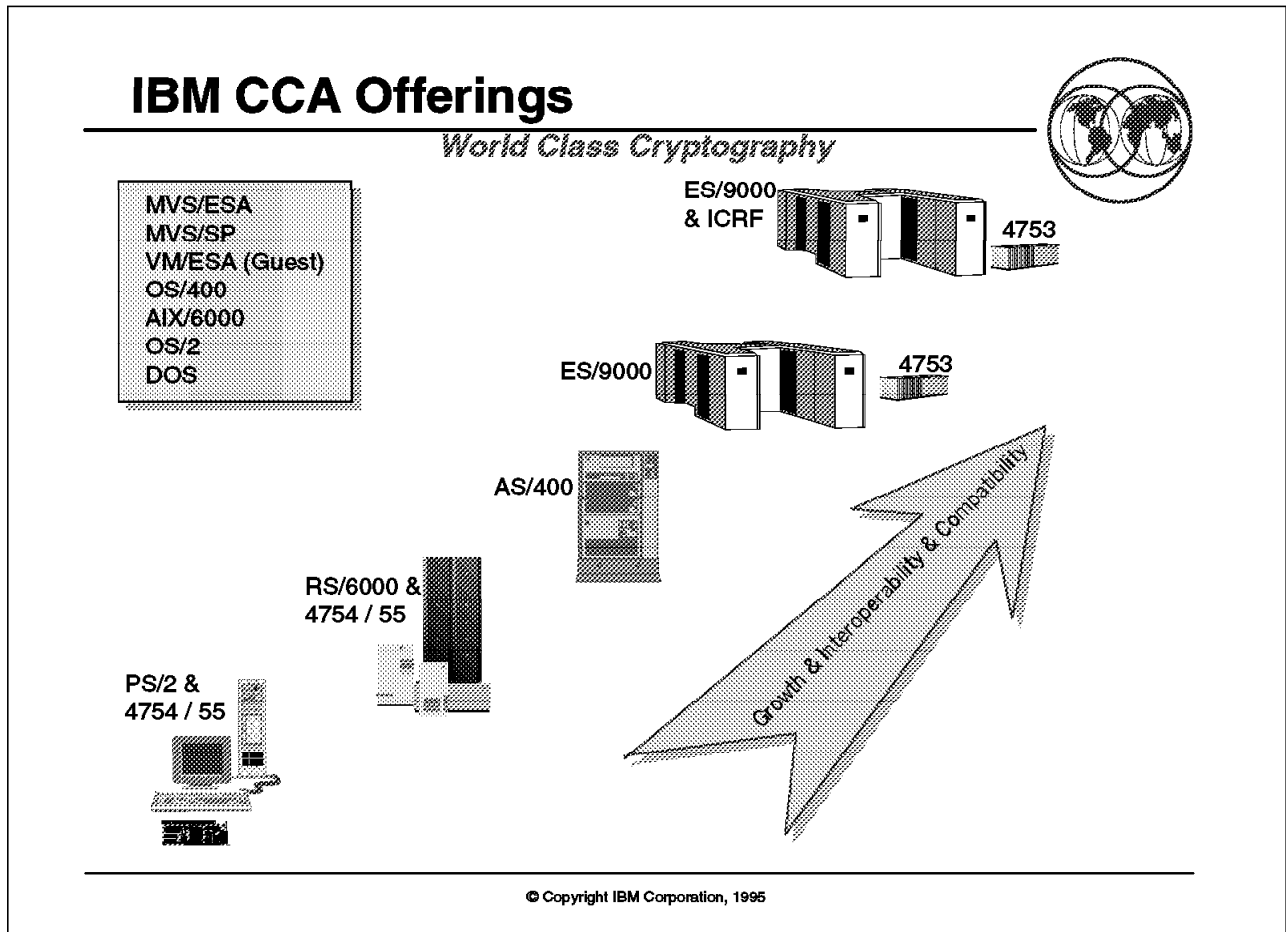


Figure 77. IBM CCA Offerings

Key Points

IBM offers consistent, compatible, cryptographic solutions across all strategic platforms.

Presentation Script

The CCA offerings provide scalability, growth, interoperability and compatibility across the platforms.

The IBM Transaction Security System and the IBM Integrated CRYPTOgraphic Facility (IBM ICRF) with its supporting Integrated Cryptographic Services Facility/MVS (ICSF/MVS) are the IBM offerings that conform to the IBM CCA Application Programming Interface (API).

Across the platforms:

- PS/2 - Transaction Security System
- RISC/6000 - Transaction Security System
- AS/400 - 2620 and 2628 Cryptographic Processors (Transaction Security System)

- ES/9000 - Transaction Security System or ICRF

6.6.1 Transaction Security System

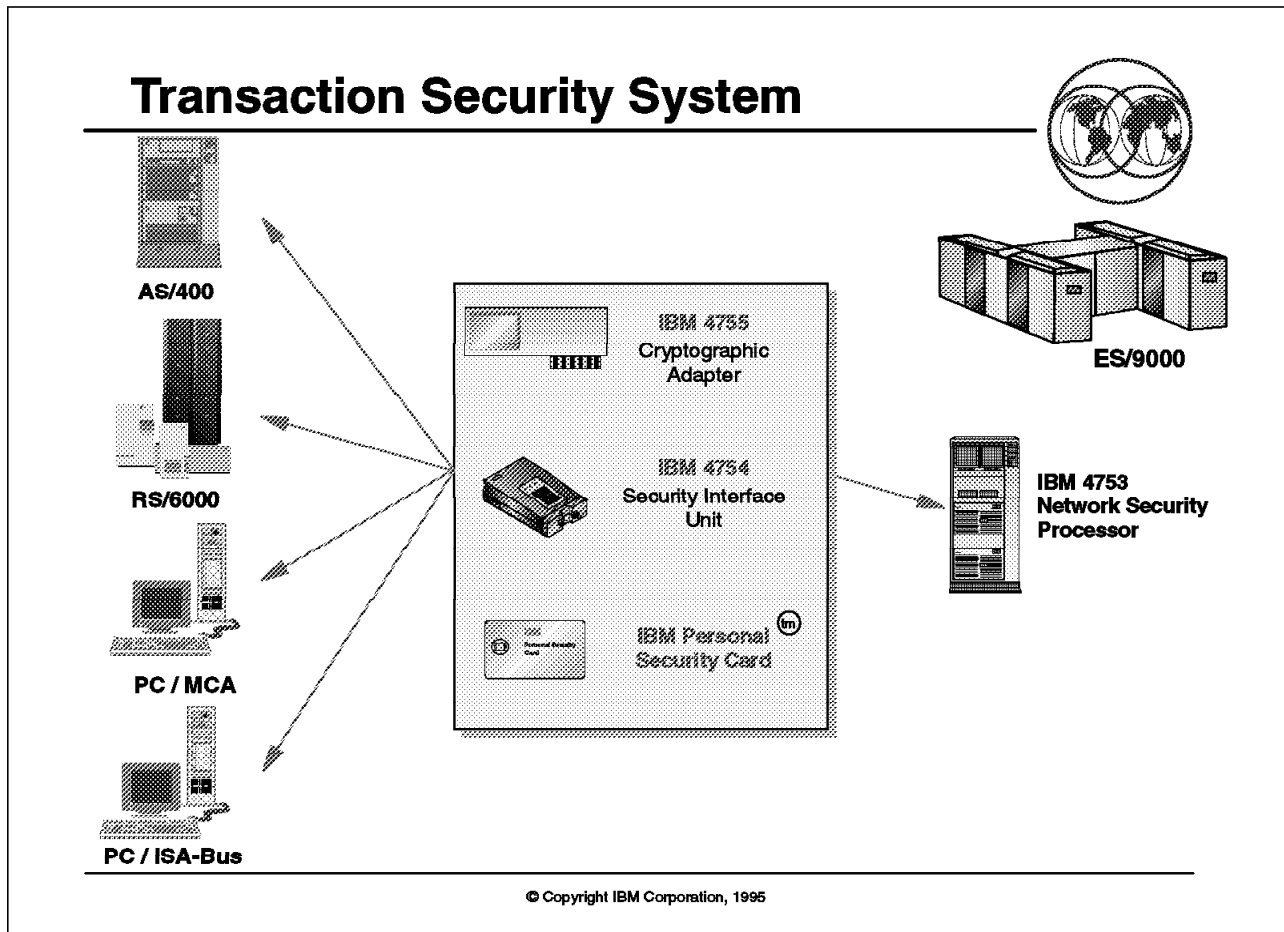


Figure 78. Transaction Security System

Key Points

The Transaction Security System provides a product family consisting of:

- The IBM 4755 Cryptographic Adapter is available for the personal computer (ISA-Bus, MCA-Bus) and RISC/6000 (MCA).
- The IBM Personal Security Card is a credit-card sized "smart card" that contains computer, memory and communication circuits in a single chip. DES or CDMF is implemented on the Personal Security Card.
- The IBM 4754 Security Interface Unit provides a Personal Security Card reader and a 12 key keypad as an input/output device.
- The IBM 2620 and 2628 Cryptographic Processors are AS/400 I/O processors that use the cryptographic adapter.
- The 4753 Network Security Processor is a channel-connected cryptographic-processing I/O unit that uses the cryptographic adapter. Multiple processors can be connected to a host system that uses the MVS operating system.

Presentation Script

The IBM Transaction Security System products provide comprehensive support for DES-based and RSA public-key-based cryptographic processing. The hardware products feature tamper-resistant mechanical and electrical designs that are combined with a sophisticated set of access controls. Together, these products create a secure subsystem.

The Transaction Security System products are supported in major computing environments where application and system programs access the hardware services through a programming interface that is common across the environments. The cryptographic services are consistent with the IBM Common Cryptographic Architecture. The software support consists of access methods and utility programs that help set up the system and perform basic cryptographic key-management functions.

Workstation Products

The following hardware products can be used in many personal computers and Reduced Instruction-Set Computer System/6000 (RISC System/6000) workstations:

- IBM 4755 Cryptographic Adapter
- IBM Personal Security Card
- IBM 4754 Security Interface Unit
- Signature Verification feature.

The following software products can be used, depending on the operating environment:

- IBM Workstation Security Services Program
- IBM Advanced Interactive Executive Security Services Program/6000

IBM 4755 Cryptographic Adapter

Several models of the cryptographic adapter are available that support a broad range of DES, CDMF, and RSA public-key cryptographic processes. These cryptographic processes are performed within a highly secure module that is mounted on the adapter. The adapter can be used in the disk operating system (DOS), Operating System/2 (OS/2), and AIX/6000 environments. Different models of the adapter support the ISA and Microchannel bus architectures.

The adapter performs many different cryptographic processes designed to enable application programs to support various cryptographic standards. In addition, the adapter supports the performance of custom-designed cryptographic processes to support unique cryptographic applications.

IBM Personal Security Card

This credit-card sized "smart card," the Personal Security card, contains a computer, memory, and communication circuits in a single chip mounted behind the interface contacts on the surface of the card. The computer performs DES-based cryptographic processing, provides secure portable data storage for over 4000 bytes of access-controlled data, and provides access controls that authorize unique functions for up to four users. This credit-card sized "smart card" is used with the security interface unit and other readers that support its communications protocols. The Personal Security Card conforms to basic international smart card standards.

IBM 4754 Security Interface Unit

This input/output (I/O) device provides a means to exchange information with the Personal Security card including secure entry of a PIN to authorize card access controls, provides a secure DES cryptographic processing environment, and a secured time-stamp clock source. The security interface unit includes the following in a tamper resistant package:

- DES-based cryptographic processor
- Numeric keypad
- Controlled access clock-calendar
- Interface circuitry for the signature verification pen

The security interface unit can be used in the DOS, OS/2, AIX, and AS/400 environments:

- On a personal computer, the unit connects to the IBM 4755 Cryptographic Adapter or an RS-232 serial port.
- On a RISC System/6000 workstation, the unit must connect to the adapter.
- On an AS/400 system, the unit can connect to the cryptographic processor.

Signature Verification Feature

The Signature Verification Feature consists of a pen attached to the 4754 security interface unit, and a co-processor card attached to the 4755 cryptographic adapter. When a person signs their name, this Signature Verification feature compares the movements of the signature verification pen with reference data that is stored on their Personal Security card. The feature tests the way in which the pen is moved, instead of the appearance of the signature, to decide whether the signature belongs to the card holder.

IBM Workstation Security Services Program

This software provides an access method and utilities for the personal computer. The workstation security services program enables the use of the cryptographic adapter, the security interface unit, the Personal Security card, and the signature verification pen. The software is designed for use in the DOS and OS/2 environments. The workstation security services program can be ordered with all models of the cryptographic adapter, except Models L05 and 5, and with the security interface unit.

IBM AIX Security Services Program/6000

This software provides an access method and utilities for the RISC System/6000 computers in the AIX environment. The AIX Security Services Program/6000 enables the use of the cryptographic adapter, the security interface unit, the Personal Security card, and the signature verification pen. The software is provided with the cryptographic adapter Models L05 and 5 and supports the installation of one or two cryptographic adapters and, optionally, one security interface unit. The hardware and software support DES-only functions.

Host Products

The Transaction Security System products provide hardware and software for an MVS host environment and for an AS/400 host environment.

MVS Host Environment

In an MVS host environment, the IBM 4753 Network Security Processor and the IBM Network Security Processor Multiple Virtual Storage (MVS) Support Program are the Transaction Security System components.

IBM 4753 Network Security Processor

This channel-connected, cryptographic-processing I/O unit uses the cryptographic adapter to provide a comprehensive set of DES-based, CDMF-based, and RSA public-key-based cryptographic processes. Multiple processors can be connected to a host system that uses the MVS operating system. If feature code 9750 is specified, the CDMF algorithm is substituted for the DES algorithm for data confidentiality operations.

The IBM Network Security Processor Control Program is provided with the network security processor. This software directs the operation of the processor during testing, offline operation, and online operation.

IBM Network Security Processor MVS Support Program

This licensed program provides an access method for the network security processor to use with the MVS operating systems. The access method can be used in the following environments:

- Customer Information Control System (CICS) transaction programs
- Time Sharing Option (TSO) regions
- MVS regions
- Batch regions

The access method supports the Advanced Communication Function for the ACF/VTAM Virtual Communications Access Method (ACF/VTAM) Systems Network Architecture (SNA) session-level encryption cryptographic requirements. One or more network security processors can be connected to a single access method; one access method can be used for each (logical) MVS host.

The access method interfaces do the following:

- Support the Common Cryptographic Architecture (CCA) that is also used by the high-performance Integrated Cryptographic Facility (ICRF) on the largest System/390 processors
- Support extensions to CCA, primarily in key management, financial PIN management, and customer-defined processes and algorithms
- Permit the use of older programs such as the IBM Cryptographic Unit Support Program (CUSP) software, which is used with the IBM 3848 Cryptographic Unit, or the IBM Programmed Cryptographic Facility (PCF) software.

AS/400 Host Environment

In an AS/400 host environment, the IBM 2620 and 2628 Cryptographic Processor hardware features support the Transaction Security System function.

IBM 2620 and 2628 Cryptographic Processor

Each of these AS/400 I/O processors uses the cryptographic adapter to provide a comprehensive set of cryptographic services. The processor and its supporting

software, the Common Cryptographic Architecture Services/400, support the DES-based cryptographic services, PKA-based cryptographic services, ANSI X9.17 key management services, and the attachment of a 4754 security interface unit. The 2628 cryptographic processor provides data enciphering and deciphering through CDMF.

IBM Common Cryptographic Architecture Services/400

This PRPQ software supports the 2620 and 2628 Cryptographic Processors. The software enables the use of the cryptographic processor, the security interface unit, and the Personal Security card at an AS/400 host. The software runs under Operating System/400 (OS/400) Version 2 Release 3 Modification 0 or greater, and includes a security API that extends the Transaction Security System security API to an AS/400 environment. Public-key cryptographic services and ANSI X9.17 key management services require OS/400 Version 3 Release 1 Modification 0.

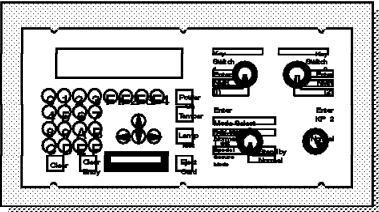
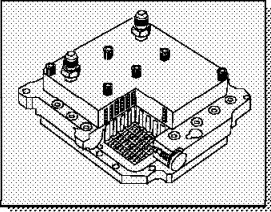
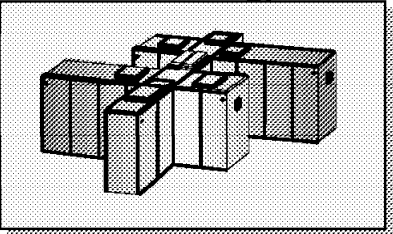
For more information on the Transaction Security System refer to:

- *IBM Transaction Security System Concepts and Guidelines - Workstation*, GG24-3590
- *IBM Transaction Security System 4753/MVS Installation and Session Level Encryption Guidelines*, GG24-3591

6.6.2 Integrated Cryptographic Feature (ICRF)

Integrated Cryptographic Feature (ICRF)

- **High performance (>2000 trx/sec)**
- **Continuous operation (can update MK while running)**
- **Fully integrated coprocessor**
- **One ICRF per side**
- **Consists of:**
 - ▶ **Thermal Conduction Module (TCM):**
 - Hardware Master Key stored here
 - Duplicate DES engines
 - Physically protected
 - Removal detection
 - ▶ **Key Storage Unit (KSU):**
 - Key entry unit
 - Secure Storage
 - ▶ **Secure Cable:**
 - Path by which keys flow from KSU to TCM
 - Secure Connection



© Copyright IBM Corporation, 1995

Figure 79. Integrated Cryptographic Feature (ICRF)

Key Points

- The ICRF hardware was designed to address high volume cryptographic transaction rates and bulk security requirements on MVS/ESA.
- The Integrated Cryptographic Service Facility/MVS (ICSF/MVS) provides the interface to high level language callable service routines supported by the hardware, such as key management.

Presentation Script

The IBM Integrated Cryptographic Feature (ICRF) and Integrated Cryptographic Service Facility/MVS (ICSF/MVS) were designed to address high volume cryptographic transaction rates and bulk security requirements on MVS/ESA .

ICRF and ICSF/MVS enable rapid encryption and decryption of large amounts of data, and provide for the generation and management of cryptographic keys. International cryptographic standards relating to PIN processing, message authentication, and data encryption are supported.

The Integrated Cryptographic Service Facility/MVS (ICSF/MVS) provides the interface to the hardware via an application program interface consisting of high level language callable service routines. The application programming

interface conforms to the IBM Common Cryptographic Architecture and allows for inter-operability with other CCA-based products, such as the IBM Transaction Security System. Interoperability is also possible with products from IBM and other vendors that are not IBM Common Cryptographic Architecture compatible.

Key management functions, such as key generation, key import, and key export, are provided so that key exchange can be performed electronically. The master keys can be changed dynamically to allow *continuous operation* across master key changes. Master key integrity is ensured by ICSF/MVS, and the changes are non-disruptive to applications. Using PR/SM, a different master key may be used to support each of the PR/SM partitions accessing the ICRF.

As of August 28, 1995, the Integrated Cryptographic Service Facility/MVS Version 1 Release 2 supports the ANSI X9.17 standard on all 9021-711 based machines. ANSI X9.17 is a key management standard for financial institutions. Seven new callable services have been added to support application implementation of this standard. Enhancements to the existing MAC services will also be available as an SPE. OFFSET and NOTARIZATION functions for the ANSI X9.17 key management standards are supported through APAR OW13633 and PTF UW90181.

ICRF is an optional hardware feature of the ES/9000-9021 water-cooled processor family that provides cryptography function and strong security features. ICRF includes:

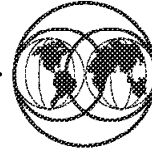
- Thermal Conduction Module (TCM)
- Key Storage Unit (KSU)
- Secure cable connecting the TCM and KSU

The KSU provides dual-control key entry via integrated key pad or IBM Personal Security Card. The listed ICRF components include tamper-detection and response features and establish the ICRF secure boundary.

For customers who wish to use VM/ESA and its guest capability to test or run MVS/ESA applications, VM/ESA allows guest MVS systems to use the IBM Common Cryptographic Architecture family of host cryptographic products. These include the Integrated Cryptographic Feature (ICRF) and its supporting software: Integrated Cryptographic Support Facility/MVS (ICSF/MVS); and the IBM 4753 and its supporting software: IBM Network Security Processor MVS Support Program.

6.6.3 Distributed Key Management System (DKMS)

Distributed Key Management System (DKMS) - Key Points



- **Main objectives:**

- ▶ Provide a general key management system to customers of Transaction Security System and ICRF product
- ▶ Provide keys for a broad range of devices including Automated Teller Machines (ATMs) and Point-Of-Sale (POS) terminals

- **Highlights are:**

- ▶ Key management function in central location
- ▶ Distribution of keys to remote locations
- ▶ *Secure* key management & distribution
- ▶ Easy operation & administration
- ▶ Separation between test and production keys & applications
- ▶ Tailorable
- ▶ Scalable

© Copyright IBM Corporation, 1995

Figure 80. Distributed Key Management System (DKMS) - Key Points

Key Points

Distributed Key Management System provides a general key management facility to customers using the Transaction Security System and ICRF.

Presentation Script

The objectives of the IBM Distributed Key Management System are to:

- Provide customers using the Transaction Security System products and the Integrated Cryptographic Facility (ICRF) a general key management system, which takes advantage of the built-in security functions of these two cryptographic products and automates the key management process. This system will ensure that all operations are performed with the highest possible level of security and will:
 - Enforce the separation of key usage
 - Exchange and replace keys on demand
 - Maintain backup copies of all critical keys
- Provide keys for a broad range of devices including Automated Teller Machines (ATMs) and Point-Of-Sale (POS) terminals.

- Share keys between the host environment and other DES-based non-control vector systems, or systems that implement different control vector principles (for example, key variants).
- Keep growth and change as simple as possible. This includes adding more devices, adding new device types and changing key characteristics.
- Allow each customer to tailor DKMS, because organizations installing DKMS must be able to retain their existing security strategies.
- Provide for the definition and separation of test and production keys.
- Separate the development of cryptographic systems and application development. This separation will increase the productivity of the application programmers who should have no need to know anything about cryptography.
- Provide easy key management support for the cryptographically secured interchange of transactions between financial institutions.
- Maximize system throughput via load balancing as required.

See the *IBM Distributed Key Management System, Installation and Implementation Guide*, GG24-4406 for further details.

Distributed Key Management System (DKMS) - Architectural Overview

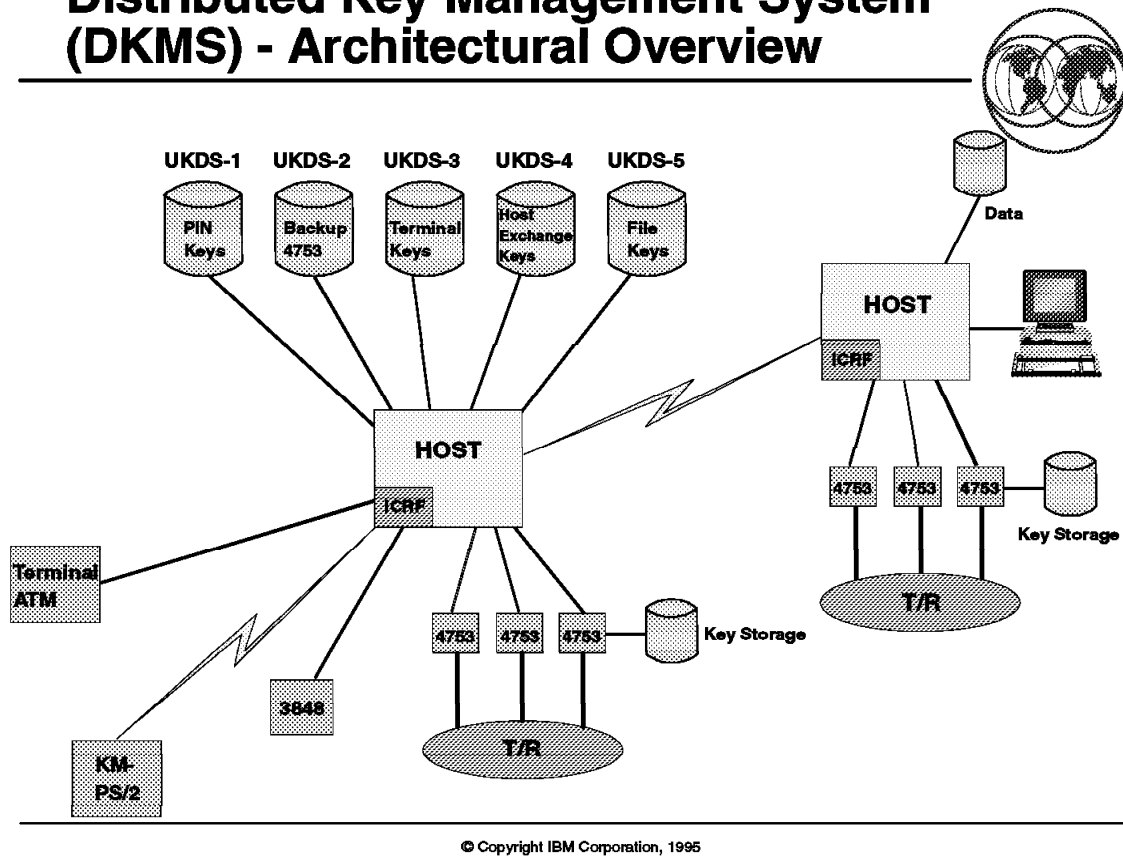


Figure 81. Distributed Key Management System (DKMS) - Architectural Overview

Key Points

Distributed Key Management System provides:

- Key management function in central location
- Distribution of keys to remote locations
- Secure key management & distribution
- Easy operation and administration
- Separation between test and production keys
- Separation between development of cryptographic systems & applications
- Tailorability to retain existing security strategies
- Scalability to allow growth and change

Presentation Script

DKMS Functional Overview: The Distributed Key Management System (DKMS) is IBM's strategic solution for cryptographic key management. It manages cryptographic keys from a central location with an easy to use, menu driven interface. There are two offerings available: a stand-alone version and an online version.

DKMS provides key management for a variety of terminal types including:

- Most Automated Teller Machines (ATMs)
- IBM 4737 noncash terminal
- IBM 4718 PIN Pads
- IBM 4778 PIN Pads
- Workstations containing cryptographic HW or SW

DKMS provides the following functions:

- Generate new versions of keys with new activation dates
- Generate and print terminal keys
- Generate and print exchange keys (XKK) for other institutions
- Verify the status of keys
- Recover keys into IBM 4753 Network Security Processor key storage
- Monitor active state of attached IBM 4753 Network Security Processors
- Enter received key parts

Access to DKMS function is through menus. DKMS allows each installation to customize the menus to its specific needs. At the lowest level of the menu, the specified function is performed by calling a program in the Key Management PS/2. The installation can define menu access tables for groups of people or individuals. Each specified table includes only the functions that are allowed for that particular group or individual.

DKMS Versions: The DKMS stand-alone version is based on a PS/2 with OS/2 Application Manager (AM) and the IBM 4755 Cryptographic adapter. It offers the same functionality as the DKMS online version except for those functions directly related to the host. The initial logon to DKMS optionally requires an IBM Personal Security card (PSc).

See the *IBM Distributed Key Management System, Installation and Implementation Guide*, GG24-4406 for further details.

Internet Security

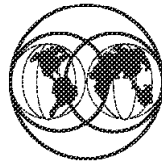



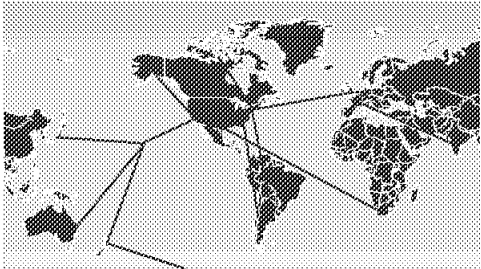
Figure 82. Internet Security

7.1 What is the Internet?

What is the Internet ?



- **The Internet is the world's largest computer network:**
 - ▶ More than 4.8 million computers
 - ▶ More than 30 million users
- **Based on the TCP/IP protocol suite, which runs on most computer architectures**
- **Links universities, government agencies, companies, and other organizations**
- **Large international presence:**
 - ▶ More than 170 countries
- **1994+ Killer Applications for Business:**
 - ▶ World Wide Web applications
 - ▶ Commercial Applications
 - ▶ Electronic Commerce



© Copyright IBM Corporation, 1995

Figure 83. What is the Internet?

Key Points

The Internet is the largest computer network linking TCP/IP based universities, government agencies, companies and computer "hosts." Security is a major concern when connecting to the Internet.

Presentation Script

The Internet is:

- A Network of Networks - concatenation of over 40K networks all connected together.
- Second largest network in the world, after the global phone system. The phone system can be a good analogy since they both have no single entity in charge and it still works, grows, and evolves as demanded. You can also analogize about the infrastructure and technology evolutions.
- Connection of the network access points which tie all the nets together.
- There are 4.8 million computers on the Internet as of Spring 1995. At that time, the NSFnet did the estimates. Since then, the NSFnet formal backbone has been discontinued, the subsidization has gone away, and the Acceptable Use Policy (AUP) has diminished in importance.

- The Internet has 4.8 million computers registered. To calculate the number of users, they take an average of 10 users/per address (based on a range of 1/address and IBM/250,000/address.) So this turns out to be about 10 users/Internet address, or 30-50 million users. Remember, all computers on the Internet are called "hosts," a difficult concept for some to grasp, but true nonetheless.
- TCP/IP is the only protocol that runs on the internet and has changed and improved over the years through a Request for Comment process, which allows anybody to propose new or improved protocols and processes. This grass roots effort is what makes the architecture so fluid and adaptable to changing requirements.
- In 1992 a group of Internet Service Providers decided that their customers wanted to do business over the Internet, a practice that was precluded by the Acceptable Use Policy dictated by the National Science Foundation. So a group of these ISPs formed a partnership in a non-profit organization named CIX (Commerical Internet Exchange) that all linked together and bypassed the NSFnet. Thus the demise of importance of the NSFnet. Today, peer agreements are being set up for all the Internet Service Providers to interconnect. Legalities and interconnection fees are just beginning to be defined.
- Over 170 countries are part of the Internet, but remember over 1/2 have EMAIL only. Of course this is changing, but may be important for certain customers.
- In 1994, a new protocol was created at CERN, Switzerland, the World Wide Web. This incorporated several new protocols that allowed for a consistent format of information. These information servers could all connect to one another in a web-like formation. The World Wide Web can also accommodate multimedia, which, along with the hyperlink technology, guaranteed its success.

7.2 What is a Firewall?

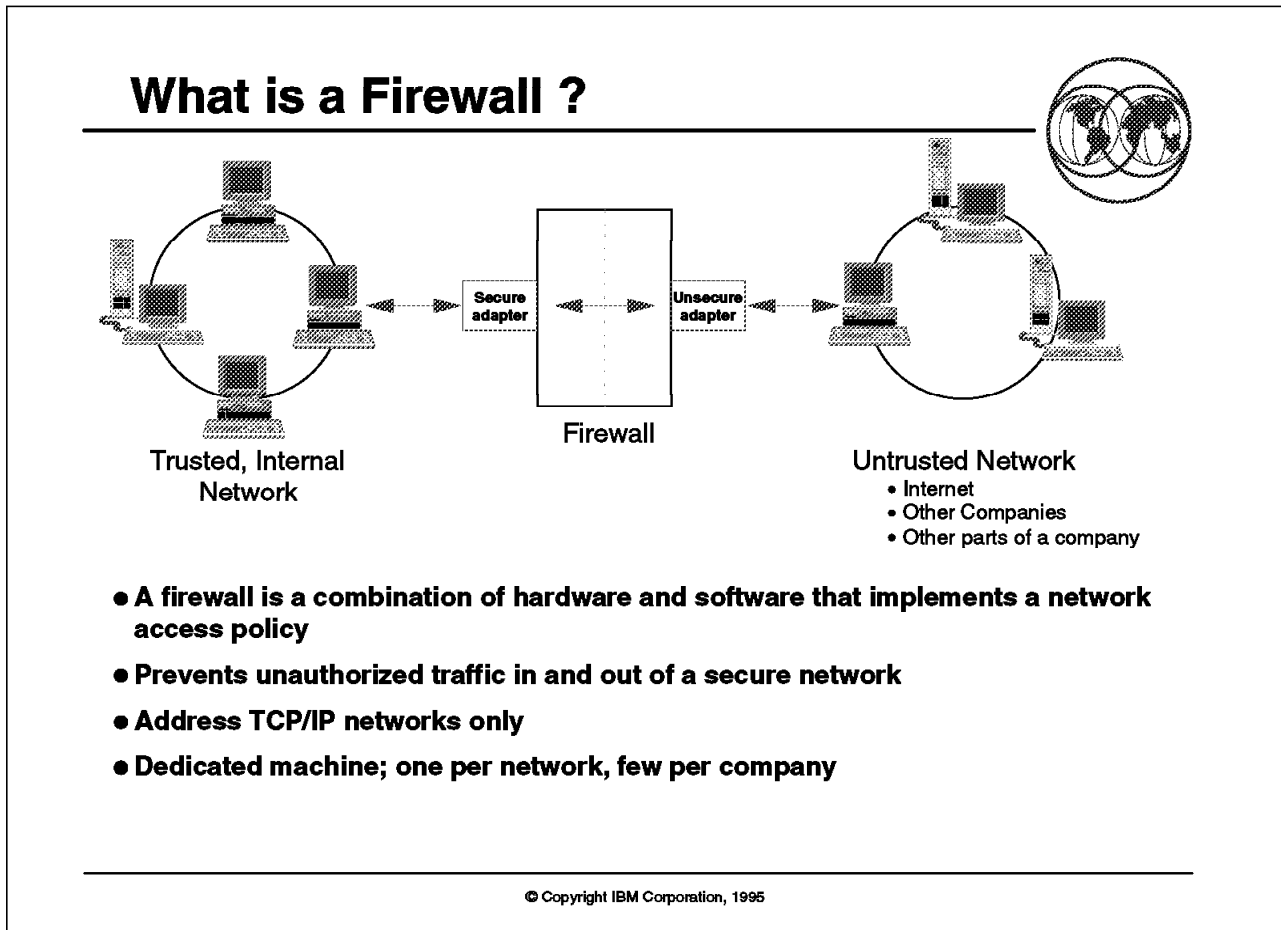


Figure 84. What is a Firewall?

Key Points

A firewall acts as a gateway between an untrusted outside network and a trusted internal network.

A firewall is a combination of hardware and software that implements a network access policy. It is recommended that the firewall be a dedicated machine.

Presentation Script

Firewalls are systems that establish a controlled connection point between different networks. They are a combination of hardware and software that implements a security policy for network access.

A firewall is *not* a single plug and play system that magically eliminates security risks. A firewall needs careful adaption to the environment it is used in, to ensure it works the way it is intended to. The quality of a firewall depends primarily on the way it is configured. When setting up a firewall, all possible connections to and from it, as well as the system itself, must be carefully analyzed for potential security problems. That means the whole system needs to be considered.

Firewalls can help you to establish controlled network access points. They do not allow you to control the data that flows through it. An e-mail message, ftp, http file transfer or even a telnet session can transfer unwanted data. There is no way to automatically and correctly analyze the transferred data.

A firewall should be a dedicated machine. Adding additional applications on a firewall machine is very dangerous, because complexity increases the number of possible weak spots.

7.2.1 Firewall Security Options

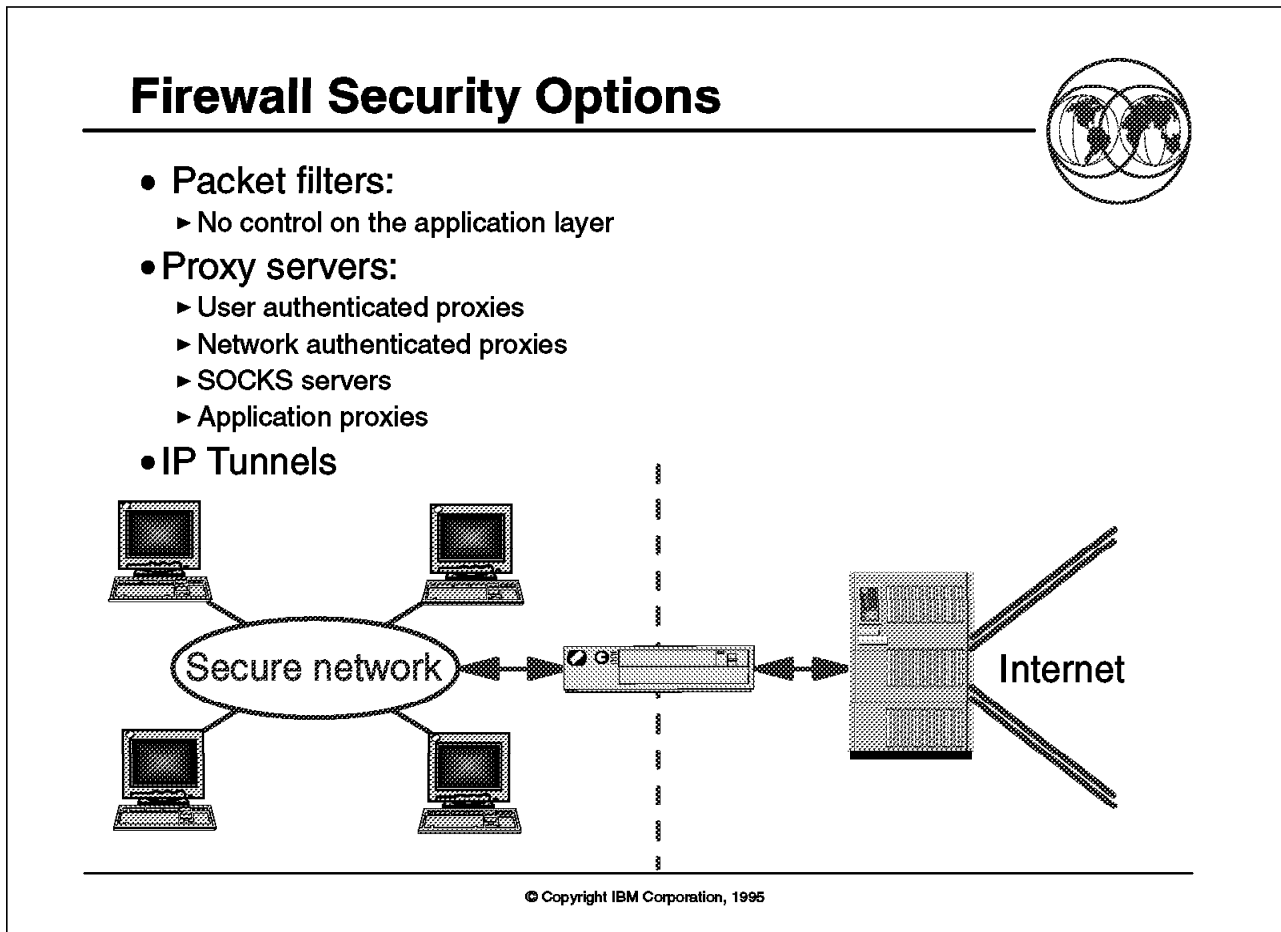


Figure 85. Firewall Security Options

Key Points

Firewall security features fall into three basic categories:

- Packet filters, which are based on routers that can limit access based on origin address, destination address, or TCP/IP protocol
- Proxy servers act as intermediaries for the applications such as:
 - User authenticated proxies
 - Network authenticated proxies
 - SOCKS server
 - Application proxies for mail
- Secure IP Tunnels, which use encryption to protect communication between two secure trusted firewalls

Presentation Script

There are many technologies that can be used to implement firewalls, such as:

Packet filter

- A standard method to generally isolate networks is the packet filter. It is a router or a system, which has a modified IP kernel that has access control lists which specify which host/network is allowed to talk to which

host/network and what protocols and ports are allowed. All other methods usually fall into the proxy family.

Proxy services

- User authentication

Proxy services are, for example, modified telnet or ftp daemons on the gateway that you log onto, which will then connect you to the final destination via some additional commands.

- Network

There are also proxies on the market that do not need user authentication but use additional command line parameters from standard clients to get to the external network.

- SOCKS

A generic form of proxy for TCP connections that is getting more and more popular is SOCKS. To use SOCKS, one runs a SOCKS daemon on the gateway and so called socksified clients on the inside. The clients know how to use SOCKS to access external systems.

- Application

Another form of proxy access is the handling of mail through some mail agent (like sendmail) on the gateway.

Secure IP Tunnels

- Tunnels provide a means of sending data securely over the Internet (or any unsecure network) between two firewalls through the use of a virtual “tunnel” formed by encapsulating/encrypting IP packets sent between the two firewall endpoints.

7.2.2 Internet Connection Secured Network Gateway

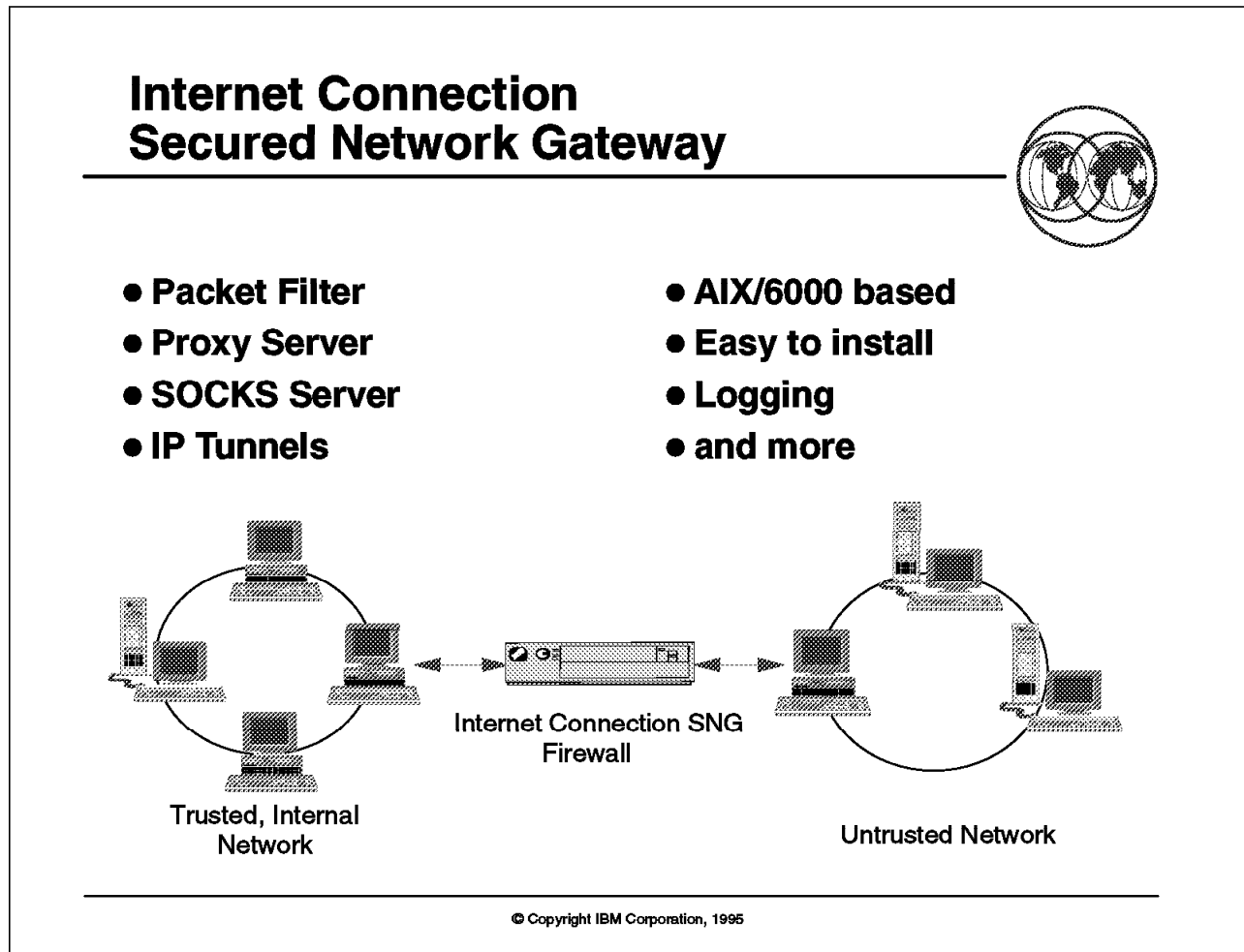


Figure 86. Internet Connection Secured Network Gateway

Key Points

The Internet Connection Secured Network Gateway (SNG) product provides firewall security features that protect your trusted internal network from untrusted outside networks.

Presentation Script

The security features of Internet Connection SNG are:

- Packet Filtering

Simple, programmable filters route allowed traffic, trap unauthorized traffic, and support TCP, User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). Using criteria like origin address, destination address, or TCP/IP protocol, these filters offer a way to easily limit user access into or out of a secure network. The Internet Connection firewall filters also differentiate between secure and nonsecure networks, inbound and outbound traffic, and local and routed traffic.

- Proxy Server

The proxy server, or application gateway, secures traffic for a particular TCP/IP application. The proxy server asks the user for the name of the remote host. After authenticating the user, the proxy server makes contact with the remote host as a proxy for the actual user. The firewall forms a controlled barrier between inside and outside your network.

- SOCKS Server

The SOCKS server intercepts and redirects all TCP/IP requests that cross between your network and the Internet. It handles data to and from TCP applications like Telnet, FTP, finger, Gopher, and Mosaic. The SOCKS server intercepts a request, validates the user ID, and checks for authorization to come into or go out of the secure network. The SOCKS server either denies the request or pipes it through the firewall, providing seamless access to the Internet for the end user.

- Secure IP Tunnels

Tunnels provide a means of sending data securely over the Internet (or any unsecure network) between two firewalls through the use of a virtual "tunnel" formed by encapsulating/encrypting IP packets sent between the two firewall endpoints.

- AIX/6000 based

Internet Connection SNG runs on AIX V3.2.5 and upwards. AIX has been designed to meet the TCSEC C2 rating.

- Easy to install

The straightforward, menu-driven panels of the firewall make installation and configuration easy, whether you are an experienced or new UNIX user.

- Logging

Continuous log and audit facilities can be customized to meet your requirements.

Additional features include:

- Mail Handler SENDMAIL Program

Provides mail routing from outside the firewall to a secure mail server within your network, and from your network out through the firewall mail handler. Users outside your secure network see only the firewall host and not the structure of the internal network or the name of the secure mail server.

- Domain name service

Prevents users outside the secure network from seeing addresses of secure hosts, while assisting secure hosts in resolving addresses of hosts in the non-secure network.

- Secure Remote Administration

Provides the ability to administer or configure the SNG from a remote location by using IP Tunnels technology to ensure the security of such administration.

- Intrusion Alarms

Provides a means to detect failed authentication patterns or trends that could represent security attacks.

- Concise Logging

Provides more granular output specifications for logging and compresses the format of the log records to achieve more efficient use of DASD necessary for logging.

- Idle Proxy

Provides a mechanism for detecting idle connections that are using the proxy gateway function and warns the user before ultimately breaking the connection.

- NetSP Authentication

Provides for the use of the NetSP Secured Logon Coordinator (SLC) authentication function to be used as one of the choices for authentication when using proxy services (telnet/ftp).

- IP Filter Enhancements

Provides enhanced IP filtering capabilities, for example:

- Granular icmp filtering
- Selective logging of filtered packets

- NLS/DBCS Enablement


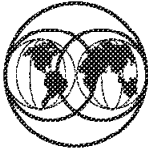
Provides double byte character support to facilitate National Language Support through future translation of messages/ interfaces to other languages.

For more information about the Internet Connection Secured Network Gateway, see *Internet Connection Secured Network Gateway for AIX: Installation, Configuration, and Administration Guide*, SC31-8113.

7.3 World Wide Web (WWW)

World Wide Web (WWW)

- **Started by CERN**
- **Documents can be linked to other documents by completely different authors**
- **To access the WWW (W3) , you run a WWW-Browser**
- **Documents on the W3 are written in "markup language" called HTML**
- **W3 is an industry consortium that seeks to promote standards and encourage interoperability**
- **Hypertext Transfer Protocol (HTTP) can be used to transfer documents over the network**
- **The W3-Browser can also access files by using FTP, NNTP, gopher and so forth**



© Copyright IBM Corporation, 1995

Figure 87. World Wide Web (WWW)

Key Points

The World Wide Web is an industry consortium that seeks to promote Internet standards and encourage interoperability:

- Consistent information format called HyperText Markup Language (HTML) allows information servers to browse data
- File transfer options include HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), Network News Transfer Protocol (NNTP), and Gopher

Presentation Script

- The WWW was started by CERN Switzerland. It incorporated several new protocols that allowed for a consistent format of information. These information servers could all connect to one another in a web-like formation.
- There are three ways to access the WWW:
 - Use a browser on your own machine. This is the best option.
 - Use a browser that can be telneted to. This is a usable option but not as good as the previous option.

- Access the web by e-mail. This is the least attractive option, but for some it's the only way.
- Documents on the WWW are written in a simple “markup language” called HTML, which stands for Hypertext Markup Language.
- HyperText Transfer Protocol (HTTP)

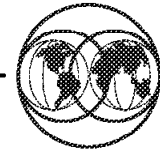
HTTP is an application level protocol for hyper media information systems. It is a generic, stateless, object oriented protocol which can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods (commands). HTTP has been in use by the World Wide Web global information initiative since 1990.
- File Transfer Protocol (FTP)

The file transfer protocol currently most used for accessing fairly stable public information over a wide area is “Anonymous FTP.” This means the use of the internet File Transfer Protocol without authentication. As the WWW project currently operates for the sake of public information, anonymous FTP is quite appropriate, and WWW can pick up any information provided by anonymous FTP. FTP is defined in RFC 959, which includes material from many previous RFCs. Directories are browsed as hypertext. The browser will notice references to files, which are in fact accessible as locally mounted (or on DECnet on VMS systems), and use direct access instead.
- Network News Transfer Protocol (NNTP)

The Network News Transfer Protocol (NNTP) is defined in RFC 977 by Kantor and Lampsley. This allows transient news information in the USENET news format to be exchanged over the internet. The format of news articles is defined in RFC 850, Standard for Interchange of USENET Messages by Mark Horton. This in turn refers to the standard RFC 822 which defines the format of internet mail messages. News articles make good examples of hypertext, as articles contain references to other articles and news groups. News groups appear like directories, but more informative.
- Gopher

The Gopher distributed information system uses a lightweight protocol very similar to HTTP. Therefore, it is now included in every WWW client, so that the Gopher world can be browsed as part of the Web. Gopher menus are easily mapped onto hypertext links. It may be that future versions of the Gopher and HTTP protocols will converge.

WWW Security



- **Secure HyperText Transfer Protocol (S-HTTP):**
 - ▶ Authentication
 - ▶ Encryption
- **Netscape Communications Secure Socket Layer (SSL)**
- **DCE Web:**
 - ▶ Ported to AIX
- **Secure Web server and browser:**
 - ▶ For AIX and OS/2
 - ▶ Using S-HTTP and SSL



© Copyright IBM Corporation, 1995

Figure 88. WWW Security

Key Points

There are several proposals for standard World Wide Web security:

- Secure HyperText Transfer Protocol (S-HTTP)
- Secure Socket Layer (SSL)
- DCE Web Project
- Secure Web Servers such as OS/2 and AIX

Presentation Script

- Secure HyperText Transfer Protocol (S-HTTP)

Developed by E. Rescorla and A. Schiffman of Enterprise Integration Technologies for CommerceNet.

S-HTTP (Secure HTTP) is an extension of HTTP, providing independently applicable security services for transaction confidentiality, authenticity/integrity and non-reputability of origin.

- Netscape Communication Secure Socket Layer (SSL)

Developed by Kipp E.B. Hickman of Netscape Communications Corp.

Secure Socket Layer is a security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate in a

way that cannot be eavesdropped. Servers are always authenticated and clients are optionally authenticated.

The SSL protocol provides “channel security” which has three basic properties:

- The channel is private. Encryption is used for all messages after a simple handshake is used to define a secret key.
- The channel is authenticated. The server endpoint of the conversation is always authenticated, while the client endpoint is optionally authenticated.
- The channel is reliable. The message transport includes a message integrity check (using a MAC).

- DCE Web

The DCE Web project is working to bring a new level of capability to the World Wide Web by providing a layer of advanced distributed computing services between Web applications and the network. The basic idea is to extend the power of the Web without necessarily having to reengineer Web clients and servers or the protocols that they use to communicate. The DCE Web provides powerful security, naming, and other services to existing Web applications.

The DCE Web has been ported to AIX at the University of Stuttgart, where a public DCE Web server is now (1 August 1995) up and running.

For more information about DCE WEB, see the DCE WEB home page in the Internet. (<http://www.osf.org/www/dceweb/index.html>)

- Secure Web Servers and Browsers

Anchoring IBM’s portfolio of security products and services is the announcement of IBM Internet Connection Family secure Web servers and browsers. Servers for the OS/2 and AIX platforms offer customers interoperable SSL and S-HTTP encryption capabilities as well as remote administration from a WWW client. Included are public as well as private keys, key certificates, data encryption, digital signatures, and message authentication.

IBM’s OS/2 WebExplorer browser software likewise integrates SSL and S-HTTP security solutions.

7.4 Internet Keyed Payment Protocol (iKP)

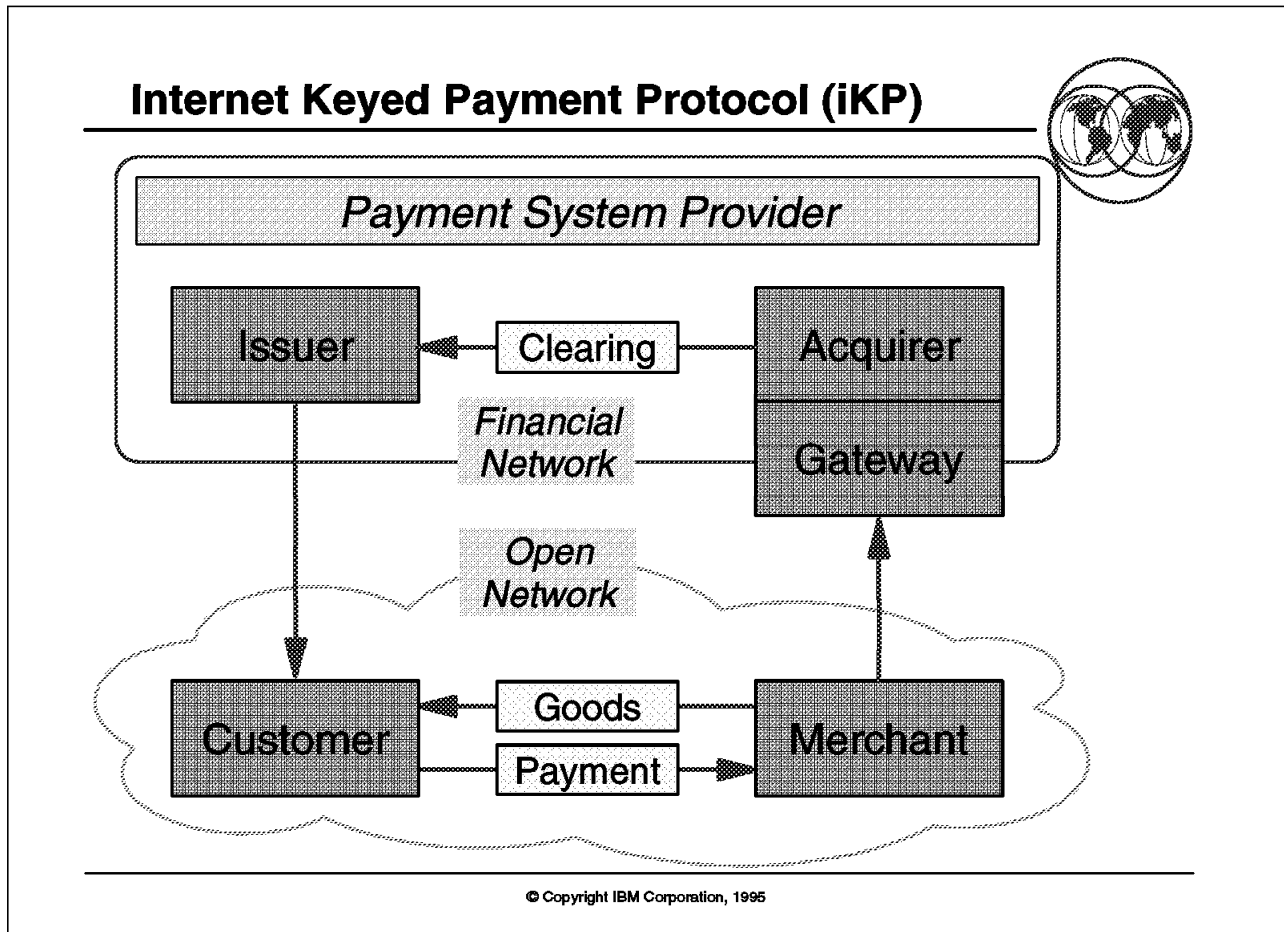


Figure 89. Internet Keyed Payment Protocol (iKP)

Key Points

The Internet Keyed Payment Protocol (iKP) is an IBM proposal to allow customers, merchants, banks and credit card issuers to securely communicate credit card transactions on the Internet based on encryption protocols.

Presentation Script

iKP is a multiparty security protocol developed by IBM Research. iKP enables buyers and sellers to engage third parties, such as banks and credit card companies, in a single secure payment transaction. iKP will enable buyers to securely send their encrypted credit card number to a seller, who then forwards it to the credit card company for decryption and transaction approval. The credit card company then notifies the seller of credit approval without the seller ever seeing the unscrambled buyer's credit card number.

iKP is an open proposal that has received favorable responses from both the financial and technical communities, and is being proposed as an open Internet Secure Payments standard.

The particular advantage of iKP over existing proposals are:

- The iKP family allows for a gradual deployment. iKP is based on what already exists today - credit cards, PINs, and the existing payment system networks - and presents a feasible shortterm solution. Introduction of public key certification of merchants will usher in 2KP and, as soon as the certification infrastructure for customers is in place, 3KP can be phased in to achieve full multi-party payment security.
- iKP is an evolving design, rather than a fixed, closed protocol. It is intended as a starting point for a standard for secure payments over the Internet. IBM encourages comments on its qualities and suggestions for improvement.
- The use of encryption in iKP is limited to well-defined payment data - credit card numbers and PINs - and the interface to cryptographic primitives can be designed in a way that makes them inaccessible to the end user.

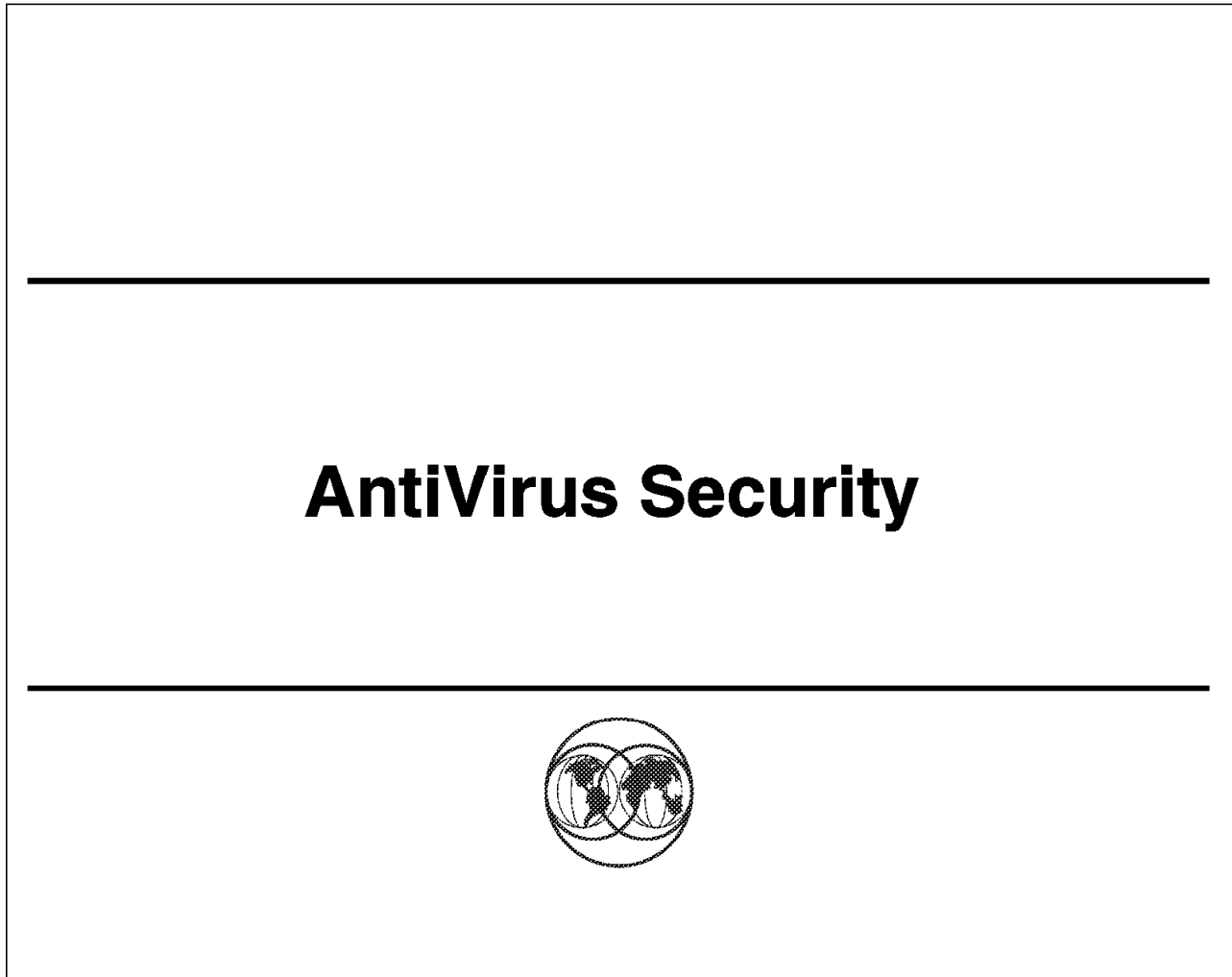


Figure 90. AntiVirus Security

8.1 Computer Viruses

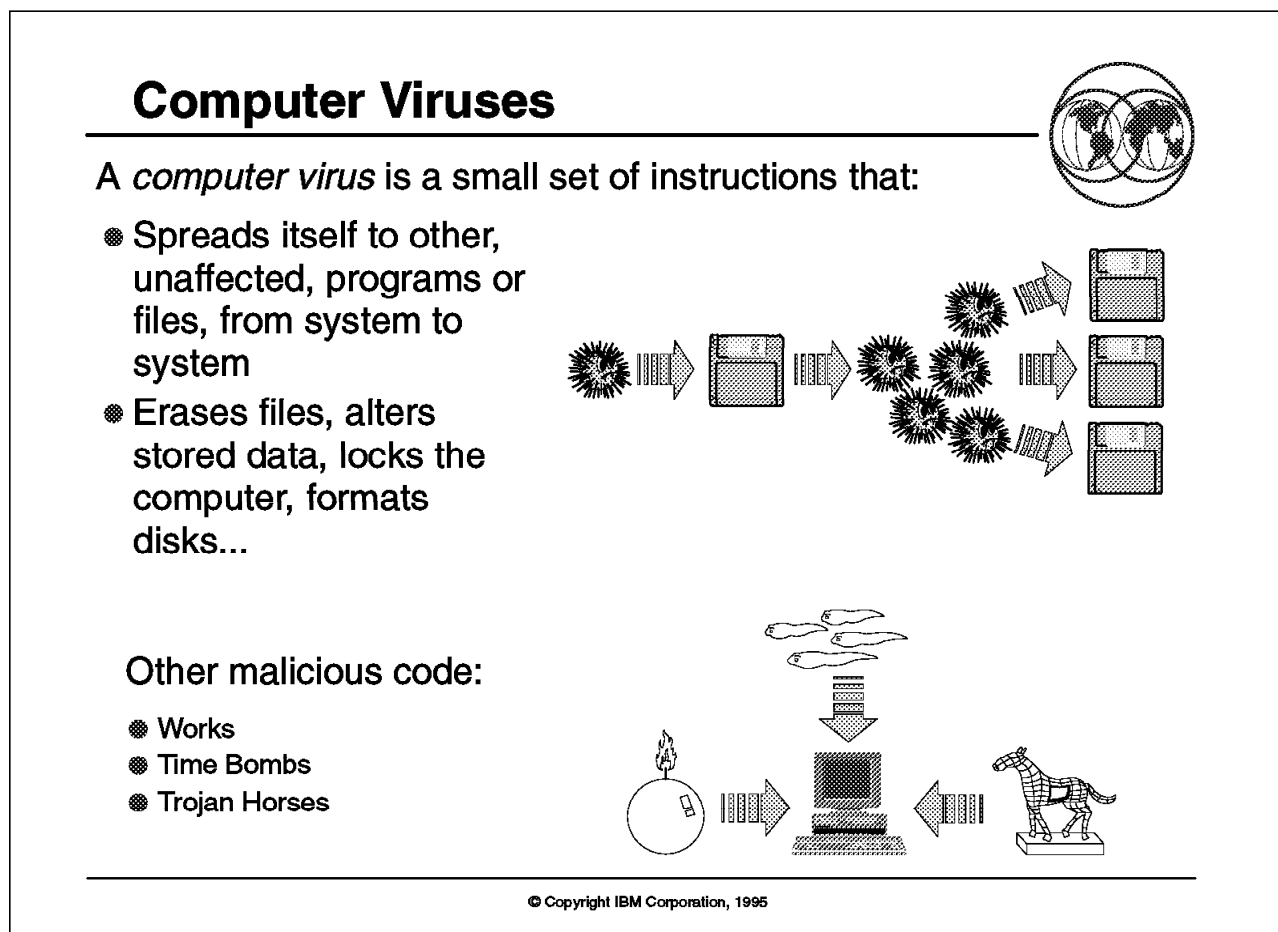


Figure 91. Computer Viruses

Key Points

Computer viruses are a major security threat that are capable of spreading and causing malicious damage.

Presentation Script

A computer virus is one type of threat to the security and integrity of computer systems. Like other threats it can cause the loss or alteration of programs or data. Unlike many other threats, a computer virus can spread from program to program, and from system to system, without direct intentional intervention.

How a computer virus works: Typically a computer virus performs two functions. First it copies itself into previously uninfected programs or files. Second (perhaps after a specific number of executions, or on a specific date), it executes whatever other instructions the author included in it. So it can simply display a warning message, but it can also erase files, format disks, lock the computer, alter stored data, or take up scarce resources, such as disk space, CPU time, or network connections.

The targets of virus infections can include:

- Ordinary program files (EXE and COM files in PC-DOS, for instance)
- The initial-program-load (“boot”) areas on diskettes and fixed disks
- Device drivers
- Shell scripts
- Interpreted data

Furthermore, any system that provides any sort of service on a network can be the target for a network worm.

How viruses infect a computing system: The initial introduction of a virus into a computing system can occur through a variety of channels, including:

- A data diskette accidentally booted from because it was left in the drive
- Software introduced on the system by an outsider who can access the system
- Software used at home by an employee whose home computer is, unknown to the employee, itself infected
- Software purchased from a commercial company whose production facilities are infected
- Software downloaded from public bulletin boards for business use or use by the employee
- Software intentionally infected by a malicious employee
- Network transmissions via Internet, BBS, or other electronic sources

Many microcomputer viruses are known for IBM PC-compatible and other major microcomputers systems, but not all of them are actually spreading. No viruses for mainframe or minicomputer systems are known to be actively spreading, but this may well change in the future.

Other malicious code: There are several threats similar to computer viruses with colorful names such as worms, bacteria, rabbits, Trojan horses, Time Bombs, and so on. These are still unwanted and unauthorized code, and as such they appear to be like a virus, but they normally not capable of replicating themselves.

8.2 AntiVirus Security

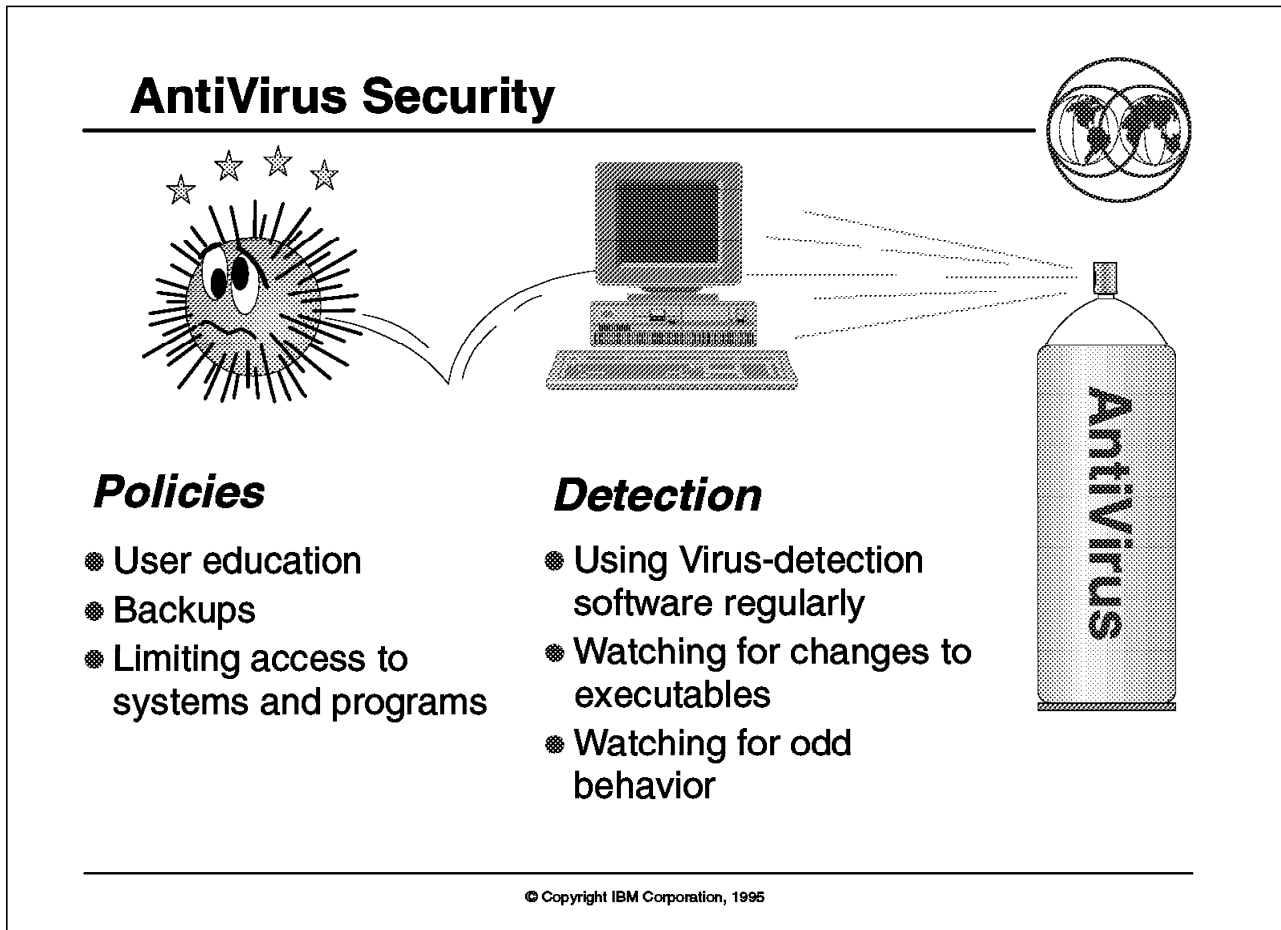


Figure 92. AntiVirus Security

Key Points

The key to effective computer virus controls are:

- Good security policies
- Good virus detection

Presentation Script

Good security policies depend on the knowledge and cooperation of the users. Users should be aware of the dangers that exist, and know what to do if they suspect they have found a security problem. These are general rules which are not just valid for security against viruses.

Security Policies: Even without the threat of viruses, backups are an important part of system management. Often the only way to recover altered or lost files is by restoring them from backups. However, great care must be taken not to reintroduce a virus into the system with an infected backup. So backup should also be verified and certified "clean."

Since viruses spread to new users and systems only when information is shared or communicated, you can prevent viruses from spreading by isolating users and

systems and permitting users to utilize only the software and hardware really needed.

The two most important resources available for detection of viruses are watchful users and watchful programs. Virus checking programs should be run frequently on production systems, and on multitasking systems they should be continuously running in the background.

Users should always be aware of visible things that are known to happen on virus-infected systems, and should report suspicious behavior in the computer systems.

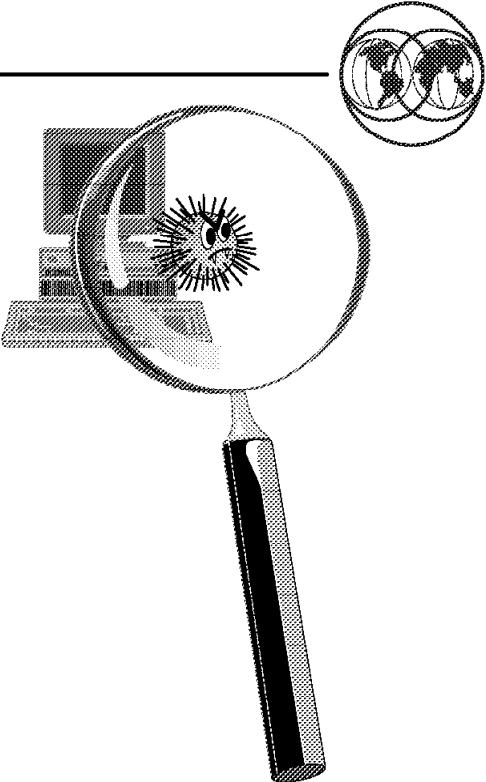
Symptoms of Known Viruses: This section lists specific oddities that are known to occur in workstations infected with viruses:

- Unexpected changes in timestamp or length of files, particularly executables, or to volume labels
- Programs taking longer to start
- Programs attempting to write to write-protected media for no apparent reason
- Unexplained decreases in the amount of available memory
- Executable files vanishing
- Workstations unexpectedly rebooting
- Unusual thing appearing on displays, including “scrolling” of odd parts of the screen, odd messages, and so on
- Unusual load on local networks or other communication links

8.3 IBM AntiVirus Product

IBM AntiVirus Product

- Support for all PC based environments (DOS, OS/2, Windows) and NetWare Servers
- Advanced Heuristic analysis
- Automatic Check and Detection
- Automatic Repair of most infections
- DOS Shield to avoid spreading
- Quarterly Updates



© Copyright IBM Corporation, 1995

Figure 93. IBM AntiVirus Product

Key Points

The IBM AntiVirus Product is an advanced state-of-the-art tool for detecting, disinfecting, and repairing virus damage.

Presentation Script

The IBM AntiVirus Product provides protection against the growing problem of PC viruses, and is designed to carefully analyze every part of a system that is vulnerable to infection:

- System memory
- Disk files (floppy, hard, removable and compressed)
- “hidden” disk areas (including boot records)
- NetWare servers
- The IBM AntiVirus program itself

The IBM AntiVirus Product provides support for current and future versions of Intel-based desktop operating systems (including DOS, OS/2, Windows), as well

as Novell NetWare servers. It detects more than 6,000 known viruses and includes new and previously unknown viruses.

To ensure reliability, the IBM AntiVirus product uses multiple strategies to accurately detect, verify and remove viruses:

- Change detection - to compare current file attributes against a built-in database
- Signature scanning - to detect known virus signatures in disk files and memory
- Fuzzy scanning - to detect virus variants
- Heuristic analysis - to detect potential new viruses
- Safe disinfection of known and unknown viruses
- DOS Shield - to quarantine the affected application and allow it to continue running without risk of spreading the infection

To keep your protection up-to-date, IBM regularly makes the latest IBM AntiVirus updates available to users individually, or by subscription, on disk or by electronic download. Furthermore, the IBM AntiVirus product is believed to have the lowest rate of false alarms in the industry.

Chapter 9. Security Management

Security Management

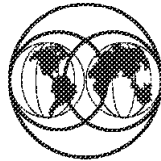


Figure 94. Security Management

9.1 Security Management - The Challenge

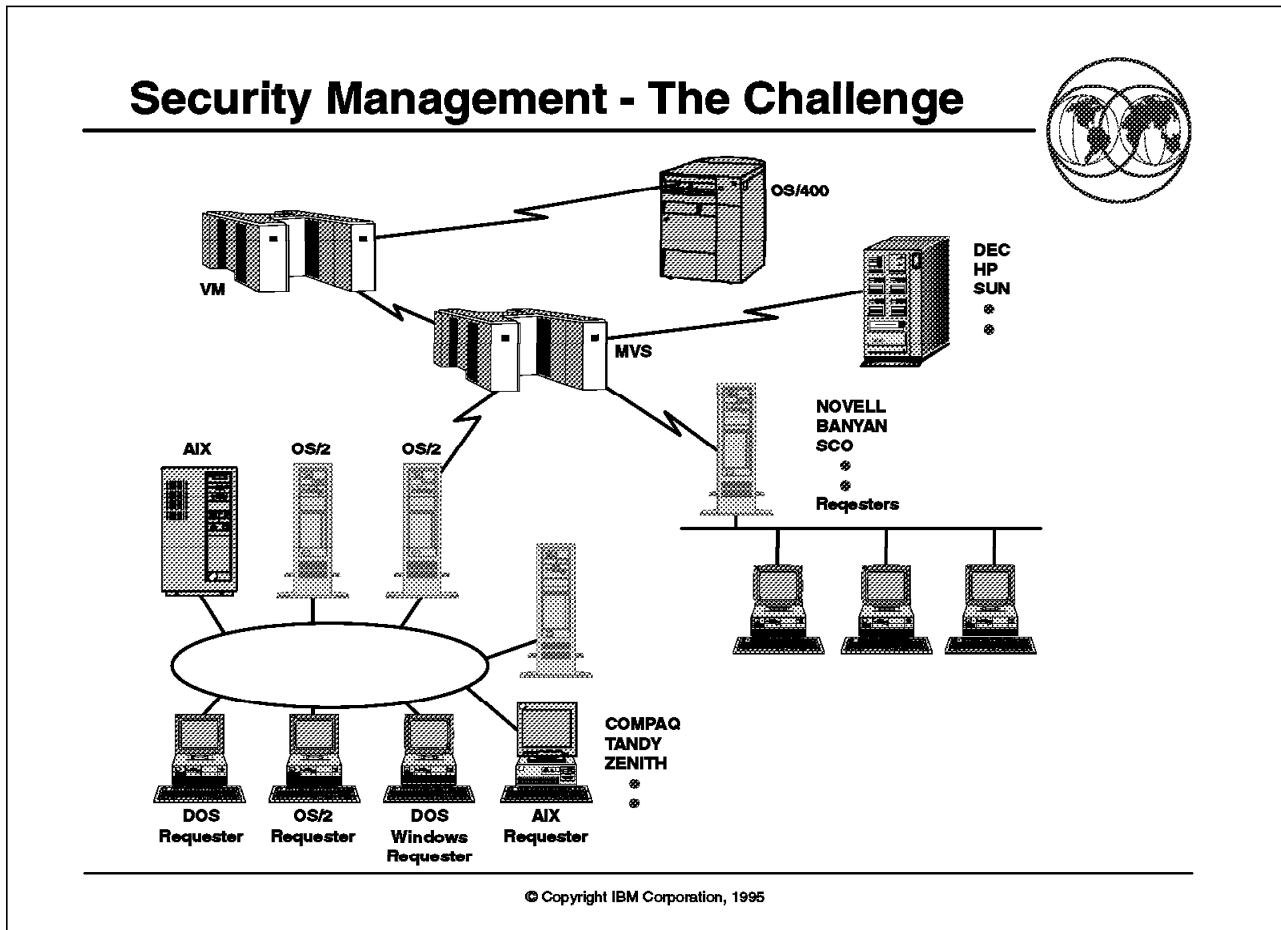


Figure 95. Security Management - The Challenge

Key Points

Customers face the challenge of security administration in today's I/T world whose characteristics are:

- Client/server distributed computing environment
- Heterogeneous hardware and software platforms
- Multiple security products and solutions
- High cost of security administration
- Difficult to achieve the desired security and auditability

Presentation Script

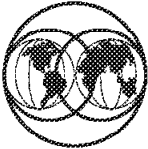
Security management involves the establishment and enforcement of security policy, the management of security services, mechanisms, and objects, and the auditability of the security environment. Today, in many cases, administrators must perform administrative tasks through multiple interfaces via multiple systems and subsystems. They are looking for a way to perform these tasks through a single interface without having to log on to multiple systems and subsystems. In addition, they want to be able to structure their security management around their business management organization. That is, some

businesses need a centralized management solution, others need a distributed solution, and others need some combination of the two.

To protect against the generic set of security threats in the open environment, the ISO OSI Security Architecture Standard has specified a set of generic security services, a set of security mechanisms to implement those services, and an outline of security management functions to enforce the system security policies. Security management is a key component of overall system management, being one of the set of common management functions specified in the ISO OSI Management Standard. The other common management functions are configuration management, performance management, fault management, and accounting management.

Security management is a critical element of the IBM Security Architecture. It relates to all security services, mechanisms, and objects. In addition, the trend toward a client/server distributed system environment requires that a solution for security management be cross system in nature.

Security Management Strategy



- **Defined as Part of the:**
 - ▶ IBM SystemView Business Discipline
 - ▶ IBM Open Blueprint

- **Security Management Definitions are Proceeding through Standards Work.**
For example:
 - ▶ DCE Security Service (Registry)
 - ▶ System Management API (SM-API)
 - ▶ Generic Audit Service API (GAS-API)

© Copyright IBM Corporation, 1995

Figure 96. Security Management Strategy

Key Points

- Security management is major facility of the IBM Security Architecture.
- Security management is also an important part of the IBM SystemView Discipline and IBM Blueprint.
- Security Management Standards are evolving to address DCE registry administration and common interfaces for system management and audit.

Presentation Script

The strategy for security management calls for tools that will simplify the administrative tasks and provide a single system image of an organization's security systems. The approach for security management is to follow the strategic systems management approach that has been defined by the IBM SystemView Framework and IBM Open Blueprint.

Security Management definitions are proceeding through standards work such as the DCE Security Service (Registry), the Generic Audit Service API (GAS-API) and the System Management API (SM-API).

9.3 System Management (SystemView)

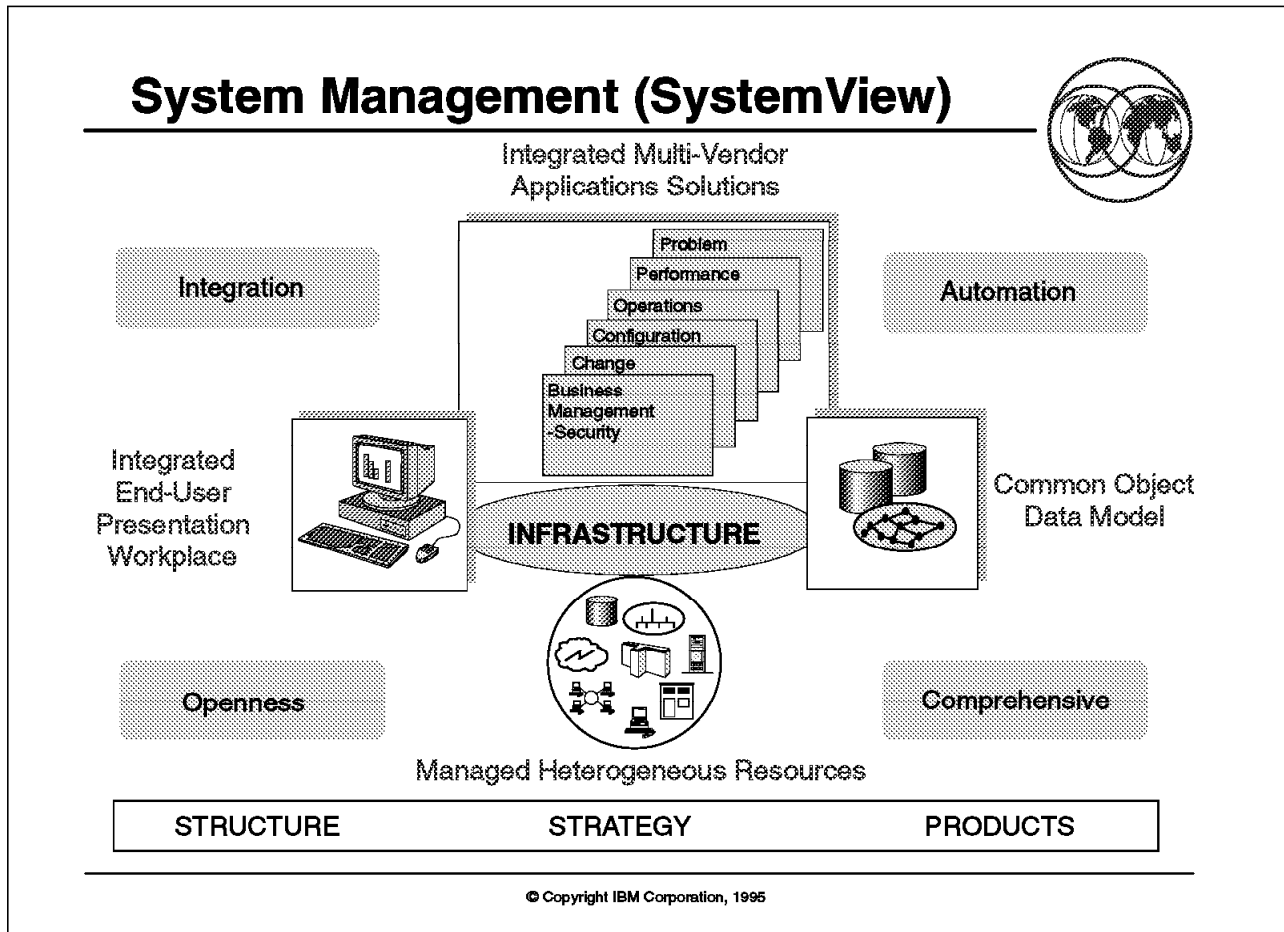


Figure 97. System Management (System View)

Key Points

- Security management is under the business management discipline of SystemView.
- SystemView is IBM's solution to our customers' problem managing their increasingly complex multi-platform, multivendor, heterogeneous networked information technology environments.

Presentation Script

Security management manages the registration or enrollment of people and programs to access controlled information system resources. Usage control and accesses are the basis for the enterprise's access control policy. The security management process is detailed as follows.

Security Policy Planning and Definition: Security policy planning and definition defines the guidelines for an installation's policies on how it identifies and resolves security problems.

Security Implementation: Security implementation provides the services and mechanisms that should be made available within any given environment. They are expected to support and enforce the security policies defined for the

organization. Some of the security services and mechanisms will be shown on the following foil. Typical services include identification, access control and data integrity. Typical mechanisms include passwords, cryptography, single signon facilities, and so forth.

Security Administration: Security administration provides the facility to register and enroll users, to define rules associated with resource access control, and to manage security administrative authorities.

Audit and Alert Management: Audit and alert management provides the necessary information to support on-going reviews of the security process, to recognize violations and trends, and to establish the process that ensures on-going effective security.

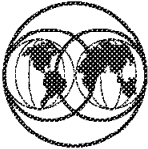
Audit readiness requires an independent review of system generated information regarding all security related events, for the purpose of:

- Testing the adequacy of the mechanisms and services
- Providing a means of ensuring compliance with policy
- Providing for the detection of breaches in security
- Enabling the recommendation of changes to policies and controls

Risk Analysis: Risk analysis is the on-going process of balancing requirements and costs. Each level of security implemented costs the organization both in terms of expenditures and in terms of lost productivity to perform the security activities.

Risk analysis determines the probability that security events will occur, and the level of security needed to control these probabilities.

Security Management Solutions



- **Enterprise Security - DSM Family:**
 - ▶ Addresses the complex problem of managing security administration tasks for users and resources in a distributed environment
- **MVS - RACF Remote Sharing Facility:**
 - ▶ Provides automatic synchronization of local and remote RACF databases
- **Database - DataHub:**
 - ▶ Provides DB administration and manages DB security authorizations
- **Cryptographic Keys - DKMS:**
 - ▶ Provides distributed cryptographic key management

© Copyright IBM Corporation, 1995

Figure 98. Security Management Solutions

Key Points

There are a number of new security management products and security oriented features on existing system management/security products, which include:

- Distributed Security Manager Family for security administration
- RACF Remote Sharing Facility for synchronizing RACF administration
- DataHub for database security administration
- Distributed Key Management System for cryptographic keys

Presentation Script

DSM Family: The IBM Distributed Security Manager family of products includes the IBM Distributed Security Manager for MVS (DSM/MVS), DSM for AIX, and DSM for OS/2 for providing consistent function for other managing platforms. Family members will differ in the platform on which the managing function runs and on the initial set of target systems.

RRSF: The RACF Remote Sharing Facility (RRSF) provides customers with the capability to maintain and administer RACF databases that are distributed throughout an enterprise. This function was introduced with RACF Version 2

Release 2 and has the capability to communicate, via the MVS Advanced Program-to-Program Communication (APPC) function, with other RACF/MVS systems to automatically maintain remote RACF databases. Once an RRSF environment is established, new enhancements can be exploited including password synchronization and the ability to direct RACF TSO commands to execute on other systems.

The Remote Sharing Facility creates a framework for greater flexibility in managing system security. It provides the capability of centralized administration and synchronization without requiring the RACF database reside on DASD shared among multiple systems.

DataHub: The main function of the DataHub product is relational database administration, yet this overlaps with security administration; therefore, DataHub could also be considered a security management product. DataHub provides a single point of control to perform relational database administration across an enterprise. The control point on an OS/2 workstation manages DB2 on IBM platforms. The control point on an AIX/6000 workstation manages DB2 and other relational databases on IBM and non-IBM platforms.

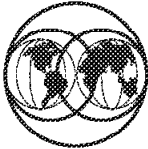
The primary security function of DataHub is the administration of authorizations for end users to access the relational database resources. The DataHub product uses the SQL Grant and SQL Revoke calls to perform these security administration functions.

For more information see *DataHub User's Guide*, SC26-3045.

DKMS: The Distributed Key Management System (DKMS) is IBM's solution for cryptographic key management. DKMS manages cryptographic keys for Transaction Security System and ICRF/ICSF from a central location with an easy to use, menu driven interface. Refer to section Chapter 6, "Cryptographic Security" on page 149 for more details.

9.5 IBM DSM Family

IBM DSM Family



- **The IBM Distributed Security Manager Family:**
 - ▶ DSM/MVS
 - ▶ DSM/OS/2
 - ▶ DSM/AIX

- **DSM family characteristics:**
 - ▶ Centralized security control
 - ▶ Centralized and/or distributed security administration

- **DSM/MVS is oriented toward customers:**
 - ▶ With MVS
 - ▶ Who want their central security control on MVS

- **DSM/OS/2 & DSM/AIX are oriented toward customers:**
 - ▶ With distributed local servers
 - or-
 - ▶ Who want their central security control on OS/2 or AIX

© Copyright IBM Corporation, 1995

Figure 99. IBM DSM Family

Key Points

The DSM Family consists of:

- DSM/MVS for host oriented cross platform administration
- DSM/AIX and DSM/OS/2 for distributed local security server administration

Presentation Script

The IBM Distributed Security Manager family includes the announced IBM Distributed Security Manager for MVS (DSM/MVS), DSM for AIX, and DSM for OS/2 for providing consistent function for other managing platforms.

DSM is designed such that it can provide for either centralized or decentralized administration.

DSM/MVS has been developed for customers who have multiple MVS systems, as well as other target platforms, and who want to manage their security environment from the MVS platform.

DSM/OS2 or DSM/AIX should be used for administration on either an OS2 or AIX platform in a distributed local security server environment.

Family members will differ in the platform on which the managing function runs and on the initial set of target systems. IBM recognizes the need to continue to expand the coverage of each family member to address additional needs of its target customer set, and will make maximum use of open, standard interfaces and infrastructures to achieve this. This approach is consistent with IBM's SystemView objectives.

Openness will be achieved through support of documented interfaces, support of standards, and use of OSF's Distributed Computing Environment (DCE) security services and object-oriented design and code. The strategy is that the family will share documented client and agent interfaces. These interfaces will also enable customers to use their own or third party code to complement or replace IBM's support for client platforms and managed systems and resources.

9.5.1 IBM Distributed Security Manager/MVS Offering

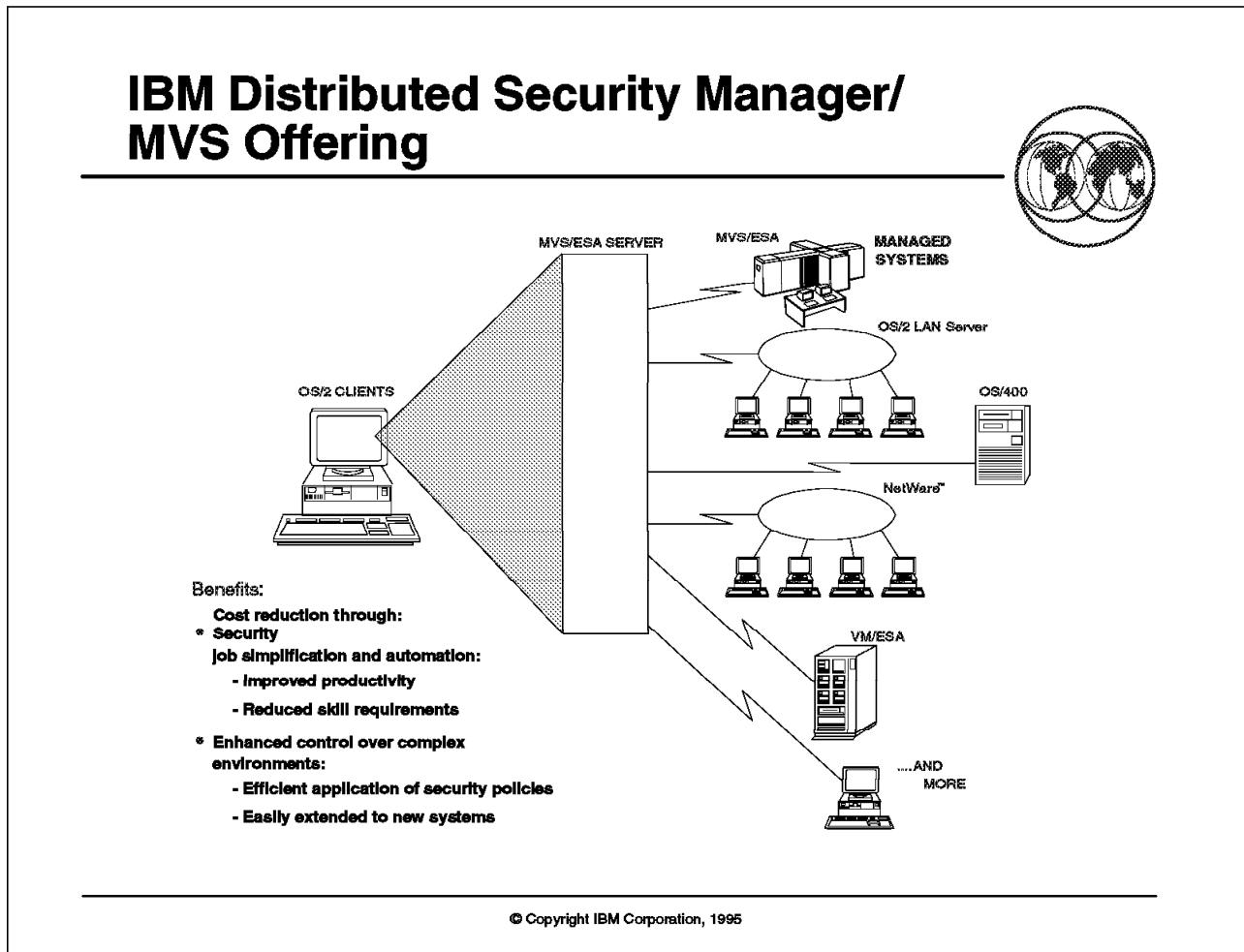


Figure 100. IBM Distributed Security Manager/MVS Offering

Key Points

The MVS member of the DSM family provides:

- Central host-oriented point of administration
- Focus on high frequency administrative tasks
- Administration GUI (OS/2 Presentation Manager Client)
- Coordination with personnel database

Presentation Script

DSM/MVS addresses the complex problem of managing security administration tasks for people and resources in a distributed, heterogeneous environment. A single, common graphical user interface is provided for security administrators, managers and delegates, to do high-frequency tasks such as:

- Reset passwords
- Add, modify, or delete user IDs
- Add, modify, or delete special privileges and authorizations to business resources
- Clone authorities from one user to another

- Transfer a user ID to another person
- Review a person's authorities in the enterprise

DSM/MVS uses an OS/2 client to initiate these tasks as requests to a server on (MVS/ESA-CICS). The server utilizes a database (DB2 tables), with information about people and the resources that they are authorized to use, to turn the requests into command streams appropriate to the specific security system. Initial support is for resources operating on MVS/ESA, VM/ESA, OS/400, OS/2 LAN servers and Novell NetWare servers. Also supported are security products, like RACF, and subsystems such as DB2, CICS, TSO, DB2/2, OfficeVision/VM and Office/Vision/400, and programs that use these products for their security.

Features of DSM/MVS include:

- All user IDs are associated with a person; linking people and their access to resources can quickly determine who has access to what.
- The end-user interface is a simple point-and-click interface on any authorized workstation capable of running OS/2 2.1.
- If one administration request requires a chain of authorizations, these are automatically initiated.
- No changes are required in the resources managed. A small segment of code is added to each target system to receive the request from the server and interface with the security management product on the target.
- Electronic approval is supported.
- Automatic actions are triggered when data indicates a person has left the company. The actions include password reset, transfer of user IDs to an appropriate person, and notification to that person of the transferred user IDs and the new passwords.
- The server maintains a single audit trail of all administrative actions initiated via DSM/MVS.
- Support is included for initial loading of the database and to periodically reconcile it with external databases.

For more information on DSM/MVS, see *Distributed Security Manager for MVS, General Information*, GC28-1511.

9.5.2 IBM Distributed Security Manager/AIX & OS/2

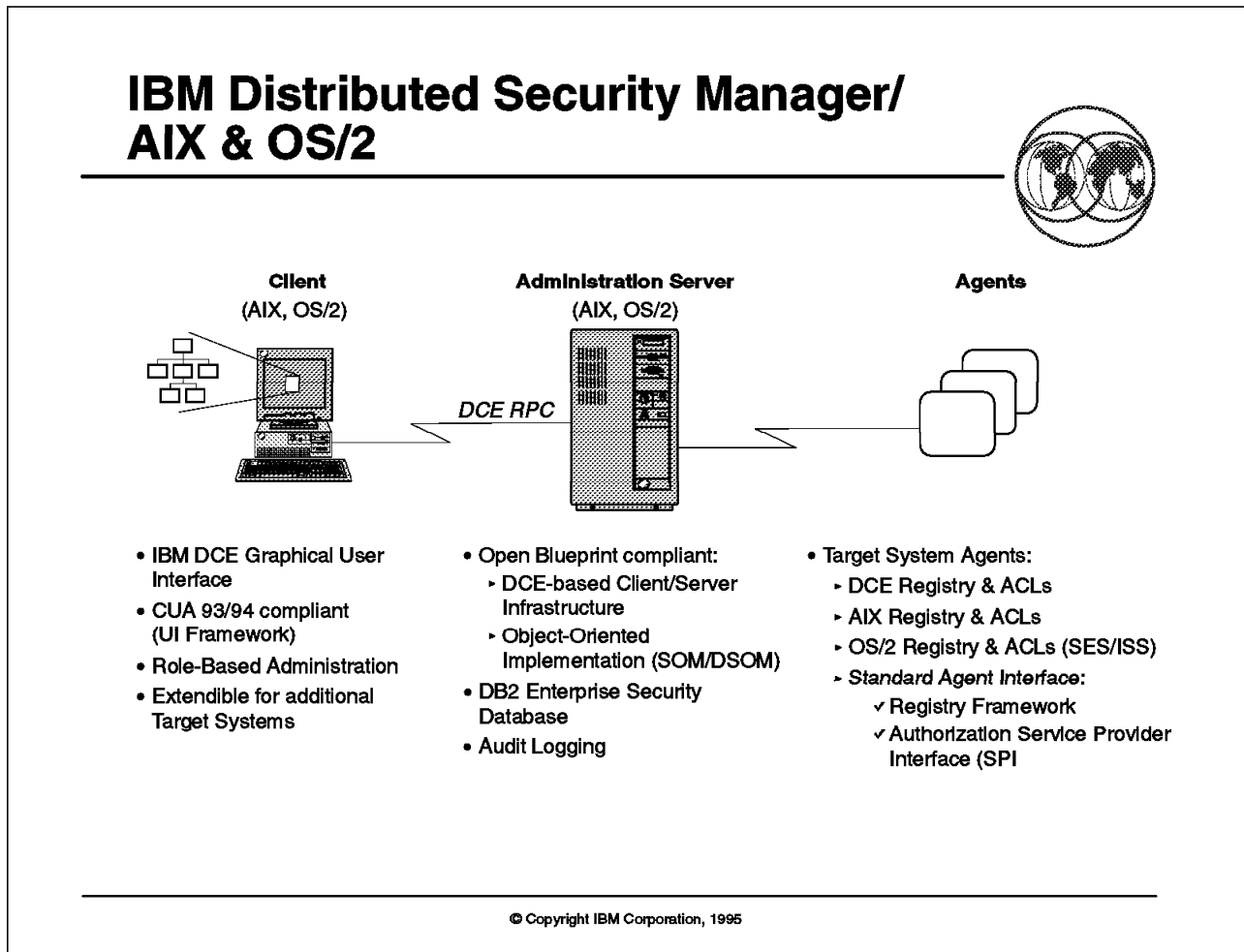


Figure 101. IBM Distributed Security Manager/AIX & OS/2

Key Points

The LAN-based members of the DSM Family provide:

- Security administration for large open distributed environments
- Exploitation of DCE security
- Role-based administration
- Object-oriented implementation (SOM/DSOM)

Presentation Script

DSM/AIX & OS/2 is the LAN-based member of the Distributed Security Manager family of products. DSM clients and servers may reside on either an AIX or an OS/2 platform.

DSM Client: The DSM client has the following features:

- IBM DCE Graphical User Interface
- CUA 93/94 compliant (UI Framework)
- Role-Based Administration

The security officer assigns role privileges to staff groups according to an organization policy and business processes. With role privileges in place throughout the organization, security administration may be performed more accurately and with greater efficiency.

- May be extended for additional target systems

DSM Administration Server: The DSM server has the following features:

- Open Blueprint compliant:
 - DCE-based client/server infrastructure
 - Object-oriented implementation (SOM/DSOM)
- Enterprise security database is DB2
- Provides audit logging

Target System Agents: DSM uses agent programs to communicate with the security systems it manages. For example, a DSM client issues a request to the server to grant a person access to an AIX file. An agent program for AIX translates this request into a format that AIX can process. DSM supplies agent programs for AIX and DCE. In addition, DSM has a Service Programming Interface (SPI) for customers who want to develop agent programs for other systems in a distributed environment.

For more information on DSM/AIX, see *IBM Distributed Security Manager for AIX, General Information*, GH12-6216.

Chapter 10. IBM Security Support and Services

IBM Security Support and Services

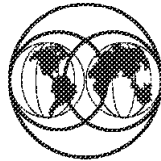


Figure 102. IBM Security Support and Services

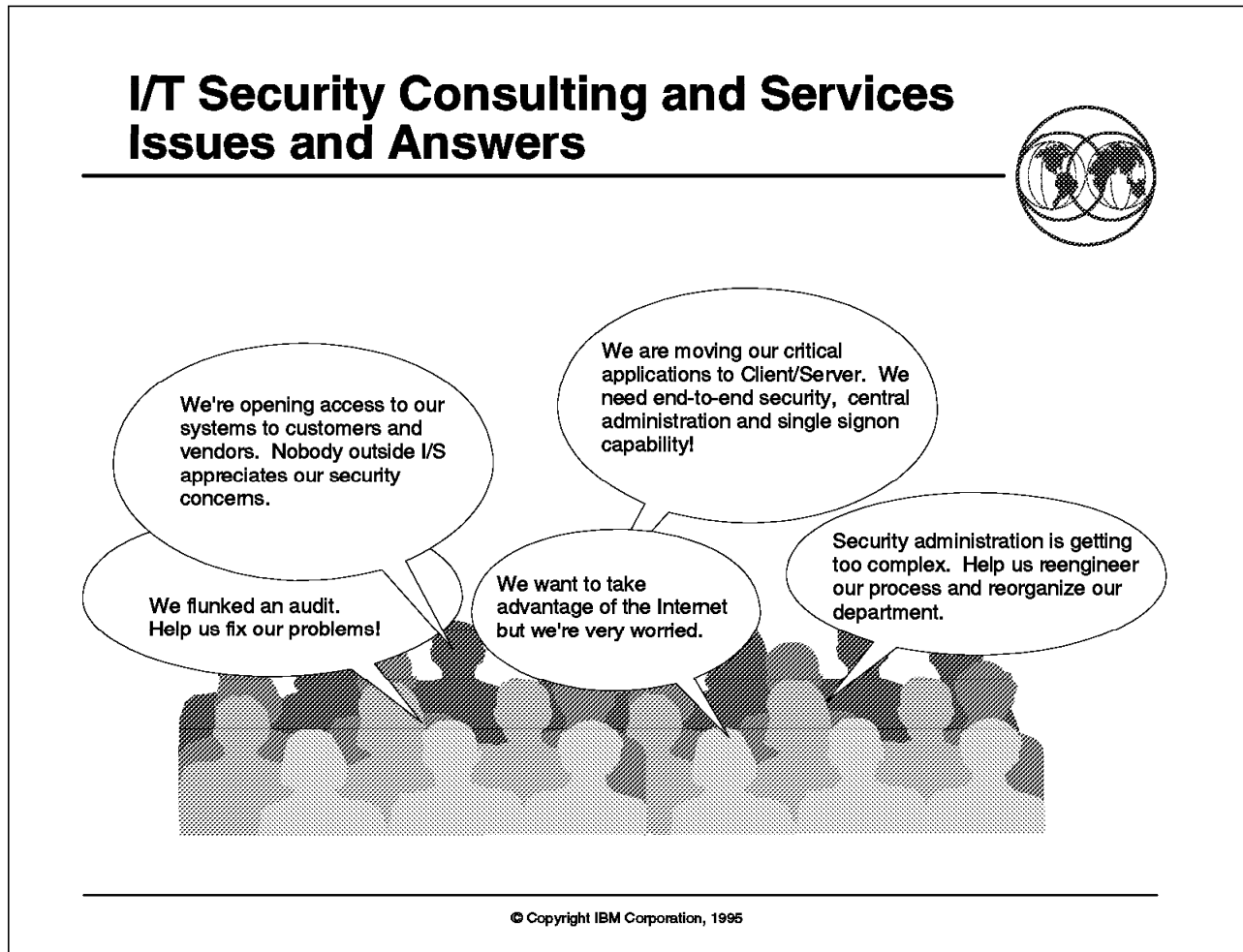


Figure 103. I/T Security Consulting and Services - Issues and Answers

Key Points

IBM has comprehensive Security Consulting and Services capabilities focused to handle issues most customers are facing today which are represented on the chart.

Note: IBM security capabilities change. Before proposing any services to customers, make sure that they are current.

Presentation Script

Transition

As customers move to open systems and distributed environments, new security issues emerge. What worked for the data center is no longer sufficient for today's extended enterprises. IBM's I/T Security Consultants can help clients address concerns such as Internet security, single signon, distributed security administration, client/server security and many others.

10.2 I/T Security Consulting and Services - I/T Executive Challenges

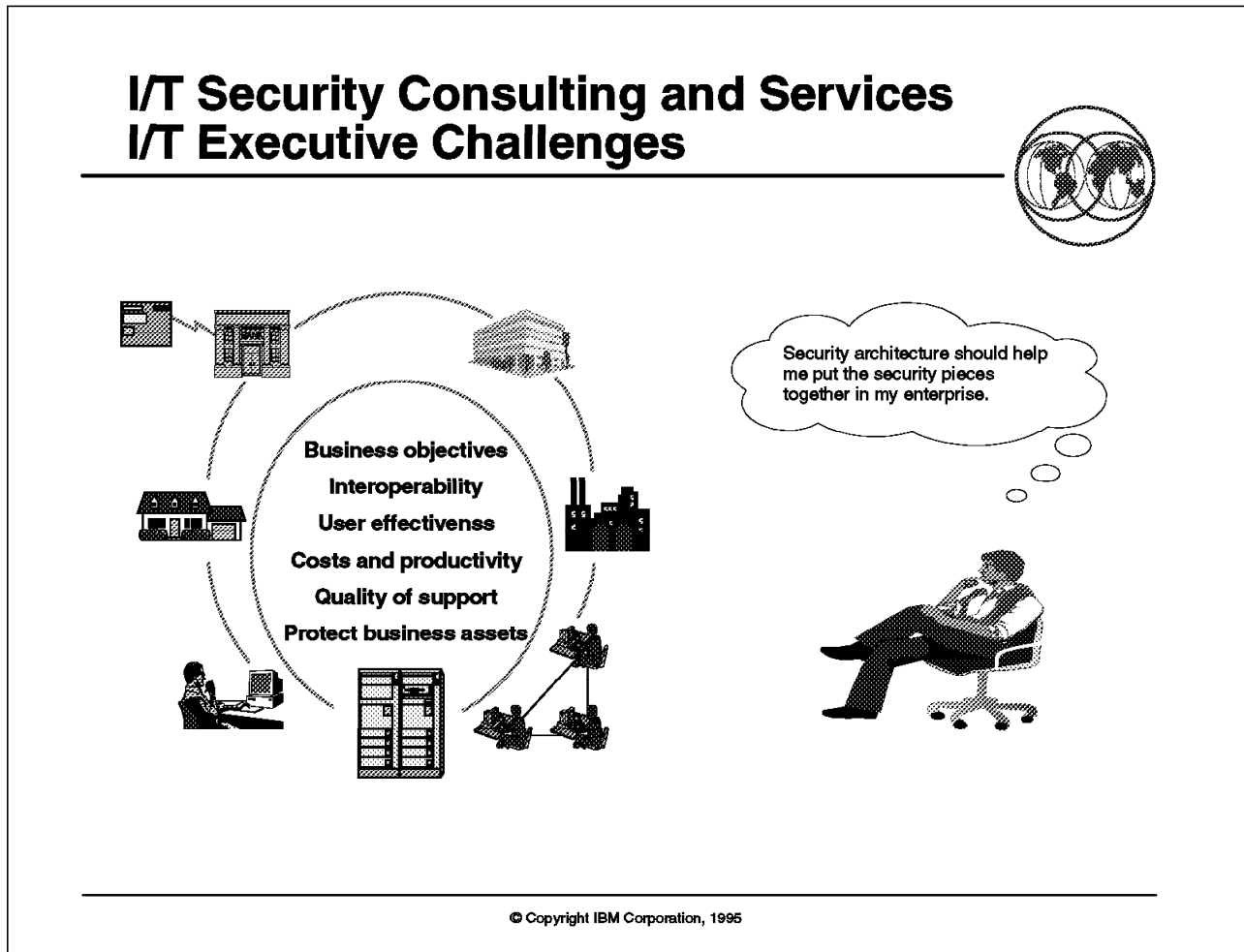


Figure 104. IT Security Consulting and Services - I/T Executive Challenges

Key Points

Demonstrate how Security is linked to the major I/T concerns faced by today's executives. Relate the impact security can have on other business decisions.

Presentation Script

Business Concerns

Today, I/T executives participate with business area executives in making key corporate decisions. I/T executives' roles are being extended beyond the traditional data center into areas where focusing on cost reduction is no longer the only issue. CEO's expect their I/T resources to support business objectives and enable new applications to be quickly deployed to keep up with competition. Productivity of end users, application developers and administration staff must keep pace without jeopardizing corporate assets. I/T resources that have been acquired by independent decision makers over the years need to integrate and interoperate with one another to enable the business to grow, and I/T executives are frequently expected to solve the complex systems management issues of the entire enterprise!

Security Beyond the Data Center

As use of the Internet mushrooms, I/T executives must respond by protecting the enterprise's assets without inhibiting end users from exploiting the expanding capabilities. CEO's want to be assured that their corporate network and data will not be attacked by intruders over the Internet. They also want to prevent employees from using the Internet inappropriately and causing legal or public relations problems that could seriously disrupt the business.

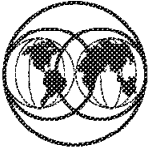
Security policies designed for environments where all assets were centrally located and accessed only through dumb terminals on internal networks are no longer sufficient for most enterprises. Policies and processes need to address virtually all systems and network management areas in planning, development and operations.

Transition

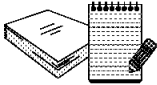
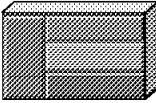


IBM I/T Security Consultants address these key concerns using a four phase methodology based on the IBM Security Architecture model. The methodology ensures that all fifteen elements needed to implement a comprehensive, enterprise-wide security program are addressed to meet a client's business needs.

10.3 I/T Security Consulting and Services - Capabilities & Customized Proposals

I/T Security Consulting and Services Capabilities & Customized Proposals



Our consultants work with you to:

	Assess existing security management policies and processes and formulate recommendations for improvement based on best practices
	Develop a customized security architecture and design solutions by selecting technology that fits with your business, I/T and security strategies
	Design structured security management processes that include continuous self-assessment and quality features that encompass your enterprise
	Assess operations with expert penetration testing to identify exposures and formulate recommendations, including business recovery and emergency response

© Copyright IBM Corporation, 1995

Figure 105. I/T Security Consulting and Services - Capabilities & Customized Proposals

Key Points

Explain the structure of the I/T Security Consulting and Services capabilities. Proposals are always customized to meet individual client needs.

Presentation Script

Four Focus Areas

IBM's Security Consulting and Services capabilities focus on four major areas: management systems, technology design, technology integration and operations and testing.

Management Systems

IBM Consultants review processes related to risks, policies, standards, organizational effectiveness, administration, and audit. Clients receive recommendations for improving protection of their critical assets and for enhancing their policies and processes to meet new threat consistent with business needs.

Technology Design

IBM Consultants will develop an enterprise Security Architecture to enable clients to make I/T decisions that will ensure their business assets are available, accurate and properly used. For clients who have specific needs in areas such as Internet access, Electronic Commerce, Cryptography and Distributed Security, IBM subject matter experts help clients design customized solutions by selecting products that fit a client's existing business and I/T strategies.

Technology Integration

Security technology is changing rapidly in an attempt to meet relatively new threats such as Internet hackers and new strains of computer viruses. Traditional security products are expanding to meet distributed security administration and operation needs and often need customization to maximize their benefits for each situation. IBM consultants assist clients in installing or converting to new security products, customizing products or policies to address new threats, and providing efficient and effective use of the security tools a client chooses.

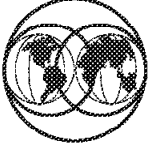
Operations and Testing

The best policies and procedures may still fail to provide the desired protection if not properly implemented. IBM's expert penetration testing is designed to identify weaknesses in systems, networks or telephone systems that are often overlooked. A unique advantage to clients is access to the most advanced tools in the world developed in IBM Research laboratories in New York and Zurich. IBM will also customize proposals to assist a client's staff, or fully operate, such processes as business recovery, virus incident management, employee education and computer emergency response to an outsider or insider attack.

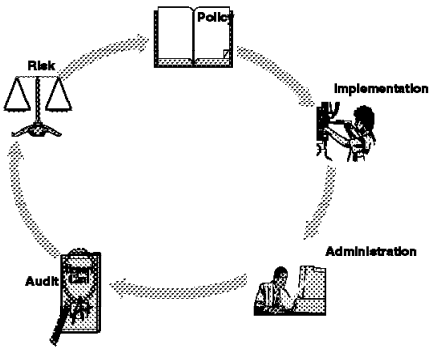
Summary

Many of IBM's security capabilities are unique in the industry. The breadth of skills is unmatched. In addition, IBM has more than 25 years of experience in security, and IBM Consultants have access to internal IBM experts around the world to satisfy the widest range of client needs. References are available.

IBM Security Support and Services Summary



- ◆ I/T Security Consulting and Services
 - ▶ Security Analysis Services
 - ▶ Solution Design & Implementation
 - ▶ Conversion to RACF
 - ▶ Health Checks & Penetration Testing
 - ▶ AntiVirus Emergency Response Team
 - ▶ Business Recovery Services
- ◆ Education - Standard, Tailored
- ◆ Publications - Product, Redbooks
- ◆ IBM I/T Security Home Page
- ◆ World-wide Marketing Security Advocates
- ◆ And more



© Copyright IBM Corporation, 1995

Figure 106. IBM Security Support and Services Summary

Key Points

- IBM has a comprehensive range of security services, education, and publications.
- The IBM I/T security home page is located at:
"http://www.ibm.com/Security."
- For more information on IBM security support and services, customers should contact their local IBM Representative.

Note: IBM security support and services change. Before proposing any services to customers, make sure that they are current.

Presentation Script

I/T Security Consulting and Services: The IBM suite of capabilities offered by I/T Security Consulting is designed to help customers assess, manage, contain and thwart potential system and network security problems for businesses. The security capabilities and services are detailed in the previous foils.

Security Analysis Services: IBM offers a number of predefined services to assist your customers in improving the security of their electronic business information. The services are:

- IBM Security Analysis for Everyone (SAFE)
- System penetration testing
- Data security process analysis
- Management support process analysis
- Application development analysis
- Network security analysis
- LAN security process analysis
- Repair solutions

Security Solution Design and Implementation: IBM Consulting as well as Security Specialists are available to help customers design as well as implement complex, multi-platform solutions.

Conversion to RACF: Migrating to a new security system can be a complex task, a task that most businesses will only undertake once. IBM's migration services are designed to minimize the time, risk and total cost of making such changes to critical system software. By assisting many customers with such migrations, IBM's Software Migration Project Office (SMPO) has developed the skills, tools and experience that can be used to assure a successful migration.

Health Checks and System Penetration Testing: Health check (audit) services are for determining the state of security on various platforms.

The system penetration test is an integrated set of tests, analysis, and investigations using "hacker" techniques against a company's information systems. The objective is to gain access by exploiting weaknesses in the implementation of the base operating system. Areas of vulnerability will be examined and exposures identified.

Anti-Virus Services and Emergency Response Team: IBM has a subscription-based anti-virus service for customers. IBM's AntiVirus software products will be available on the Internet via IBM's AntiVirus home page and will include updated software and subscription services for customers. The IBM AntiVirus home page is located at <http://www.brs.ibm.com/ibmav.html>.

IBM has established an Emergency Response Service for commercial business, chartered to provide swift, expert incident management skills to clients during and after electronic security emergencies. As part of IBM's services, the emergency response team specializes in electronic disasters that affect data processing capabilities, and is available to customers on a subscription basis. In the event of a break-in, the team helps customers detect, isolate, contain and recover from unauthorized network infiltration. They are on call 24 hours a day, seven days a week around the world.

Business Recovery Services: IBM Business Recovery Consultation Services offers an extensive portfolio of consulting and planning services to help customers design, implement and manage a comprehensive, enterprise-wide business recovery program that accommodates host system data centers, client/server environments, networks, LANs and end-user systems.

Education: IBM offers many standard as well as tailored security education courses.

Publications: There are many IBM publications available on security, in particular, product specific publications and redbooks. Redbooks are published for the main purpose of helping an enterprise implement effective security. Many of these books have been produced as a result of IBM field personnel having implemented/tested security controls.

IBM I/T Security Home Page: IBM has an I/T Security home page, located at <http://www.ibm.com/Security>. The home page provides a range of valuable information services on I/T security, including offerings on protecting the enterprise, news on security issues, information on computer viruses, and more.

World-Wide Marketing Security Advocates: IBM has a list of security advocates. These advocates each have a different variety of skills, and each person should be able to provide marketing personnel with information and guidance relating to your security marketing/services needs. If your advocate is unable to help you, please view the Information Security Contacts listing on INEWS SECURE.

And more ...: This is a comprehensive list of IBM security services. Specific security services may be tailored to customer requirements. Customers should contact their local IBM representative for information on security services.

Chapter 11. Summary

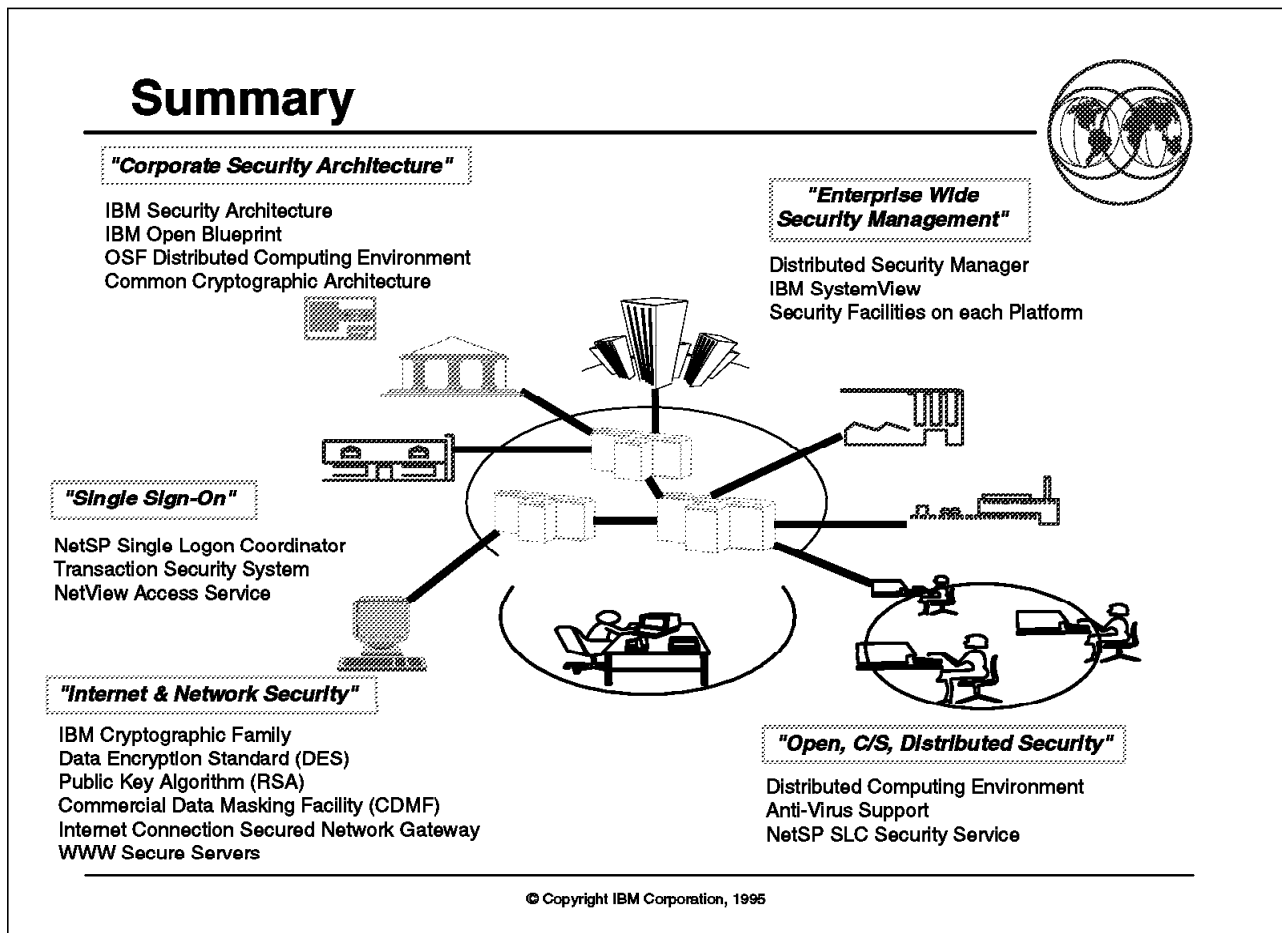


Figure 107. Summary

Key Points

IBM has continued to demonstrate its leadership in the security industry by delivering a combination of security strategies, architectures, products, solutions and services that address the top customer concerns.

Presentation Script

Customers have indicated their top security customer concerns to IBM through user groups, customer councils, requirements, white papers, industry specific standards activities, government legislation and individual marketing customer calls:

- Corporate security architecture and policy
- Open, client/server, distributed security with multi-vendors
- Internet and network security
- Enterprise wide security management
- Single sign-on

IBM is working with international standards groups and other commercial computer vendors to address the top customer concerns in today's multi-vendor, heterogeneous, open, client/server, distributed computing environment. IBM continues to be a leader in the security industry delivering a combination of security architecture, strategy, products, solutions and services:

- IBM Security Architecture and Strategy is included in:
 - *IBM Security Architecture: Securing the Open Client/Server Distributed Enterprise* (SC28-8135)
 - *Security in the Open Blueprint* (Open Blueprint Reference Library SBOF-8702)
 - *Secure Distributed Systems: Your Competitive Edge* (CUSSECWP on MKTTOOLS)
- OSF Distributed Computing Environment strategy and platform support on MVS, AIX and OS/2
- Local security support and products for IBM platforms such as RACF, MVS, VM, OS/400, AIX, OS/2 and PR/SM
- IBM Common Cryptographic Architecture with products including Transaction Security System, ICRF, ICSF, Distributed Key Management System
- IBM SystemView with the Distributed Security Manager family, RACF Remote Sharing Facility, DataHub, and the Distributed Key Management System
- Network Security Products: NetSP Secured Logon Coordinator, Internet Connection Secured Network Gateway, NetView Access Services, ACT/VTAM, MQSeries, IBM WWW Secure Servers and IBM AntiVirus Product
- IBM education, publications, marketing security advocates, and consulting services

List of Abbreviations

- AC-API - Access Control API
- ACF/VTAM - Advanced Communications Function for Virtual Telecommunications Access Method
- ACL - Access Control List
- AIX - Advanced Interactive Executive
- ANSI - American National Standards Institute
- API - Application Program Interface
- APPC - Advanced Program-to-Program Communication
- APPN - Advanced Peer-to-Peer Networking
- AS/400 - Application System/400
- BRS - Business Recovery Services
- CAI - Common Application Environment
- CCA - Common Cryptographic Architecture
- CCITT - International Telegraph and Telephone Consultative Committee
- CDMF - Commercial Data Masking Facility
- CERT - Computer Emergency Response Team
- CICS - Customer Information Control System
- CMIP - Common Management Information Protocol
- CMW - Compartmented Mode Workstation
- CPIC - Common Programming Interface for Communications
- CRC - Cyclic Redundancy Code
- DAC - Discretionary Access Control
- DB2 - Database 2
- DCE - Distributed Computing Environment
- DEA - Data Encryption Algorithm
- DES - Data Encryption Standard
- DFS - Distributed File System
- DKMS - Distributed Key Management System
- DME - Distributed Management Environment
- DoD - Department of Defense
- DRDA - Distributed Relational DB Architecture
- DSM - Distributed Security Manager
- DSMON - Data Security Monitor
- DSOM - Distributed System Object Model
- DSS - Digital Signature Standard
- ECMA - European Computer Manufacturers Association
- EDI - Electronic Data Interchange
- EPL - Evaluated Products List
- ERT - Emergency Response Team
- ESM - External Security Manager
- E3/CMW - E3/Compartmented Mode Workstation
- GAS-API - Generic Audit Service API
- GCS-API - Generic Cryptographic Service API
- GSS-API - Generic Security Service API
- GUIDE - Guidance for Users of Integrated DP Equipment
- I&A - Identification and Authentication
- IBM - International Business Machines Corporation
- ICRF - Integrated Cryptographic Feature
- ICSF - Integrated Cryptographic Service Facility
- IEEE - Institute of Electrical and Electronic Engineers
- IETF - International Engineering Task Force
- iKP - Internet Keyed Payment Protocol
- IMS - Information Management System
- IP - Internet Protocol
- ISDN - Integrated Services Digital Network
- ISO - International Organization for Standardization
- ITSEC - Information Technology Security Evaluation Criteria
- ITSO - International Technical Support Organization
- IW - Information Warehouse
- LAN - Local Area Network
- LPARs - Logical Partitions
- MAC - Mandatory Access Control
- MAC - Message Authentication Code
- MDC - Modification Detection Code
- MSFR - Minimum Security Functionality Requirements
- MVS - Multiple Virtual Storage
- NCSC - National Computer Security Center
- NetSP - Network Security Program
- NIST - National Institute of Standards and Technology
- NPT - Non-programmable Terminal
- NSA - National Security Agency
- NV/AS - NetView Access Services

- ODS - Open Distributed Systems
- OMG - Object Management Group
- OOP - Object Oriented Programming
- ORB - Object Request Broker
- OS/2 - Operating System/2
- OS/400 - Operating System for AS/400
- OSF - Open Software Foundation
- OSI - Open Systems Interconnection
- OSSA - Object Security Service Architecture
- PKA - Public Key Algorithm
- POSIX - Portable Operating System Interface for Computer Environments
- PR/SM - Process Resource/System Manager
- PWS - Programmable Workstation
- RACF - Resource Access Control Facility
- RISC - Reduced Instruction Set Computer Cycles
- RPC - Remote Procedure Call
- RRSF - RACF Remote Sharing Facility
- RS/6000 - RISC System/6000
- RSA - Rivest Shamir Adleman
- SAA - Systems Application Architecture
- SAF - System Authorization Facility
- SES - Security Enabling Services for OS/2
- SHARE - Society to Help Avoid Redundant Effort
- S-HTTP - Secure HyperText Transfer Protocol
- SLC - Secured Logon Coordinator
- SM-API - System Management API
- SNA - Systems Network Architecture
- SNG - Secured Network Gateway
- SNMP - Simple Network Management Protocol
- SOM - System Object Model
- SQL - Structured Query Language
- SSL - Secure Socket Layer
- SSLE - SNA Session Level Encryption
- TCB - Trusted Computer Base
- TCP/IP - Transmission Control Protocol / Internet Protocol
- TCSEC - Trusted Computer System Evaluation Criteria
- VM - Virtual Machine
- VTAM - Virtual Telecommunications Access Method
- WAN - Wide Area Network
- WWW - World Wide Web
- XBSS - X/Open Baseline Security Services

Index

Numerics

2620 and 2628 Cryptographic Processors 163
4753 Network Security Processor 163
4754 Security Interface Unit 163
4755 Cryptographic Adapter 163

A

abbreviations 225
access control 35, 37, 45, 46
Access Control API (AC-API) 67
access control list (ACL) 46
ACF/VTAM 143
acronyms 225
administration 23
AIX DCE 119
AIX firewall 182
AIX/6000 104
anti-virus services 219
AntiVirus Product 196
AntiVirus security 191, 194
application security 123
architecture 30, 63, 64, 67, 71
AS/400 102
assurance 32
asymmetric algorithm 152
audit 23, 61
authentication 35, 37, 41, 42

B

business management discipline 203
Business Recovery Services 219

C

certification 44
CICS 124
Commercial Data Masking Facility (CDMF) 52, 152
Common Cryptographic Architecture (CCA) 86, 157, 158
confidentiality 35, 37, 50, 52
consulting 214, 219
control vectors 158
cryptographic algorithms 152
cryptographic keys 155
cryptographic products 161
cryptographic security 149
cryptographic strategy 86, 157
cryptographic threats 150
cryptography 149
customer concerns 3
customer environment 3

customer problems 6
customer requirements 3, 6, 8, 10, 12, 223
customer testimonials 2

D

data administration 137
Data Encryption Algorithm (DEA) 52, 152
Data Encryption Standard (DES) 52, 152
data integrity 35, 37, 54, 55
DataHub 83, 131, 137, 205
DB2 83, 127, 131
DB2/x 134
DCE 75
DCE access control 47
DCE access control list (ACL) 116
DCE access control list facility 116
DCE AIX 119
DCE audit service 116
DCE authentication service 116
DCE directory service 112
DCE Distributed File System (DFS) 112
DCE key management facility 116
DCE login facility 116
DCE MVS 119
DCE Open Edition 122
DCE OS/2 119
DCE OS/400 119
DCE platform support 119
DCE principal ID mapping facility 116
DCE privilege service 116
DCE RACF Interoperation 120
DCE registry service 116
DCE Remote Procedure Call (RPC) 112
DCE security 75, 111, 112
DCE security service 112, 116, 202
DCE structure 112
DCE thread service 112
DCE time service 112
DCE VM 119
DCE Web 187
Department of Defense (DoD) 14, 88
DES 52, 152
digital signature 59, 152
Digital Signature Standard (DSS) 60, 152
directory service 112
discretionary access control (DAC) 46
Distributed Key Management System (DKMS) 170, 172, 205
Distributed Relational DB Architecture (DRDA) 131
Distributed Security Manager (DSM) 207
Distributed System Object Model (DSOM) 77
DSM family 205, 207
DSM for AIX 207, 211

DSM for OS/2 207, 211
DSM/MVS 207, 209

E

E3/CMW for AIX 104
education 219
Emergency Response Team 219
encipherment/decipherment 38, 52
evaluation criteria 17, 88

F

firewall 178, 182
firewall security options 180

G

Generic Audit Service API (GAS-API) 67, 202
Generic Cryptographic Service API (GCS-API) 67, 157
Generic Security Service API (GSS-API) 67, 115
government 12
GUIDE 2, 10

H

health check 219
history 19
Home Page xvii, 219

I

identification and authentication (I&A) 35, 37, 41, 42
implementation 23
IMS 127
industry sectors 12
Information Technology Security Evaluation Criteria (ITSEC) 14, 88
Information Warehouse (IW) 83
Integrated Cryptographic Feature (ICRF) 168, 170
Integrated Cryptographic Service Facility/MVS (ICSF/MVS) 168
interfaces 64
Internet 176
Internet Connection Secured Network Gateway 182
Internet Keyed Payment Protocol (iKP) 189
Internet security 175
Internet Security Home Page xvii, 219
IP tunnel 180, 182
ISO 13, 17, 30, 64
ISO 9000 16

K

Kerberos 114
key management 170, 172

L

label 46
LU6.2 Bind Security 143

M

mandatory access control (MAC) 47
mechanisms 37
message authentication code (MAC) 38, 55
Minimum Security Functionality Requirements (MSFR) 14, 69
modification detection code (MDC) 38, 55
MQSeries 141
multi-vendor 12
MVS 93, 96
MVS DCE 119, 120

N

National Institute of Standards and Technology (NIST) 14, 69
National Security Agency (NSA) 14
NetSP Secured Logon Coordinator (SLC) 146
NetView Access Services (NV/AS) 145
Network Security Product Secured Logon Coordinator 146
non-repudiation 35, 37, 58, 59

O

Object Management Group (OMG) 69, 77
object oriented 77
Object Security Service Architecture (OSSA) 69
objects 39
Open Blueprint 12, 72, 202
Open Edition 96
Open Edition DCE 122
Open Software Foundation (OSF) 13, 17, 64, 112
Orange Book 14, 88
OS/2 107
OS/2 DCE 119
OS/2 Security Enabling Services (SES) 107
OS/2 Warp 107
OS/400 102
OS/400 DCE 119

P

packet filter 180, 182
PassTicket 146
penetration testing 219
Personal Security Card 163
platform security 92
POSIX 96, 122
POSIX access control 48
POSIX Access Control List (ACL) 114
PR/SM 109

Process Resource/Systems Manager (PR/SM) 109
products 19, 223
proxy server 180, 182
public key algorithm (PKA) 59, 152
publications 219

R

RACF 93, 96, 98
RACF DCE 120
RACF PassTicket 146
RACF Remote Sharing Facility 205
Remote Procedure Call (RPC) 112
requirements 3, 6, 8, 10, 12, 223
risk management 23
Rivest Shamir Adleman (RSA) 59, 152
role-based administration 211
RS/6000 104

S

Secure HyperText Transfer Protocol (S-HTTP) 187
Secure Socket Layer (SSL) 187
Secured Logon Coordinator (SLC) 146
Secured Network Gateway (SNG) 182
security administration 23
security analysis 219
security architecture 30, 63
security audit 23
security consulting 214, 219
security evaluation 88
security history 19
security implementation 23
security incidents 6
security label 46
security management 61, 81, 199
security management challenges 200
security management products 205
security management strategy 202
security mechanisms 37
security objects 39
security policy 22, 61, 194
security process 23
security products 19, 223
security requirements 3, 6, 8, 10, 12, 223
security services 35, 213
security services summary 219
security standards 12, 17, 67
security standards implementation 64
security strategy 26
security threats 8, 12
services 35, 213
SHARE 2, 10
Signature Verification Feature 163
SNA Session Level Encryption (SSLE) 143
SOCKS server 180, 182
standards 17, 64, 67
strategy 26, 71

Structured Query Language (SQL) 83, 139
summary 223
symmetric algorithm 152
System Authorization Facility (SAF) 100
system integrity 32, 93
system management 81, 203
System Management API (SM-API) 67, 202
System Object Model (SOM) 77
SystemView 81, 199, 202, 203

T

third party authentication 42, 146
threats 8, 12
Transaction Security System 163, 170
trust 32
Trusted Computer System Evaluation Criteria (TCSEC) 14, 88

U

user groups 2, 10, 12

V

virus 16, 191, 192
virus security 194
VM 98
VM DCE 119

W

Web servers and browser 187
World Wide Web (WWW) 185
WWW Security 187
WWW Security Home Page xvii, 219

X

X/Open 13, 17, 64, 67
X/Open Baseline Security Services (XBSS) 69

**International Technical Support Organization
Enterprise-Wide Security Architecture and
Solutions Presentation Guide
November 1995**

Publication No. SG24-4579-00

Your feedback is very important to help us maintain the quality of ITSO Bulletins. **Please fill out this questionnaire and return it using one of the following methods:**

- Mail it to the address on the back (postage paid in U.S. only)
- Give it to an IBM marketing representative for mailing
- Fax it to: Your International Access Code + 1 914 432 8246
- Send a note to REDBOOK@VNET.IBM.COM

**Please rate on a scale of 1 to 5 the subjects below.
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)**

Overall Satisfaction	_____		
Organization of the book	_____	Grammar/punctuation/spelling	_____
Accuracy of the information	_____	Ease of reading and understanding	_____
Relevance of the information	_____	Ease of finding information	_____
Completeness of the information	_____	Level of technical detail	_____
Value of illustrations	_____	Print quality	_____

Please answer the following questions:

- a) If you are an employee of IBM or its subsidiaries:
- | | | |
|--|----------|---------|
| Do you provide billable services for 20% or more of your time? | Yes_____ | No_____ |
| Are you in a Services Organization? | Yes_____ | No_____ |
- b) Are you working in the USA? Yes_____ No_____
- c) Was the Bulletin published in time for your needs? Yes_____ No_____
- d) Did this Bulletin meet your needs? Yes_____ No_____

If no, please explain:

What other topics would you like to see in this Bulletin?

What other Technical Bulletins would you like to see published?

Comments/Suggestions: (THANK YOU FOR YOUR FEEDBACK!)

Name

Address

Company or Organization

Phone No.



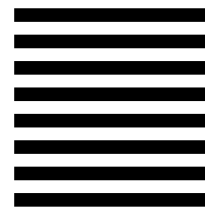
Fold and Tape

Please do not staple

Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES



BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM International Technical Support Organization
Mail Station P099
522 SOUTH ROAD
POUGHKEEPSIE NY
USA 12601-5400



Fold and Tape

Please do not staple

Fold and Tape



Printed in U.S.A.

SG24-4579-00

