AIX Security Certification

By Dinesh Vakharia and Salvatore LaPietra

The German IT security certification authority has awarded the European ITSEC E3 security certificate to IBM AIX. This certification supports IBM's outstanding reputation in IT security.

Business has become increasingly dependent on Information Technology (IT). Today, IT systems must meet specific requirements based on business needs, and provide security and protection for the data and IT services.

IT systems need a well-defined level of security with mechanisms to prevent, detect, and recover from possible harm and damage to the information and IT services. Users must feel confident and trust the accuracy and effectiveness of security functions, such as user identification and authentication, access control, and accounting and auditing. Users must also be able to measure and compare the security capabilities of the IT systems and products to ensure that the systems and products meet their expectations.

Users can develop confidence in the IT system in several ways:

- Trust the vendor
- Rely on vendors to test the IT system or components
- Review the technology and test the IT system internally
- Have an independent organization evaluate the IT system according to a well-defined standard

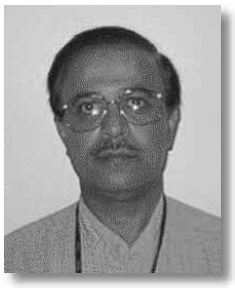
An evaluation based on the IT Security Evaluation Criteria (ITSEC) represents a well-defined level of assurance and confidence in the implementation of the security functions and mechanisms of an IT system.

IBM successfully completed an ITSEC evaluation of the AIX 4.2 Operating System at the E3/F-C2 level of security. An independent evaluation facility accredited by the German government performed the evaluation.

European Security Evaluations Process

Governments have often required products for specific government and military use to have security evaluation and certification. Now, with the increasing dependence on information technologies, businesses also have a heightened need for security and security evaluation.

The European ITSEC established by France, Germany, the Netherlands, and the United Kingdom reflects this concern for security. The European ITSEC defines what is evaluated and the IT Security Evaluation Methodology (ITSEM) provides the description of how the evaluation is performed. Unlike the U.S. Orange Book, ITSEC separates the set of security functions provided by a system from the level of assurance at which these functions are implemented. The final version of ITSEC, published in



Dinesh Vakharia

Salvatore LaPietra

June 1991, proposes ten classes of functions (F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, and F-DX) and six levels of assurance (E1, E2, E3, E4, E5, and E6).

The use of ITSEC has resulted in many security evaluations of products and systems such as operating systems, smartcards, firewalls, antivirus software, and many others.

For AIX certification, the ITSEC schema allowed security functions demanded by corporations to be combined with the E3 level of assurance, which corresponds to the assurance of a B1 system in the Orange Book. E3 enables corporations to benefit from high-assurance systems without the functionality derived from military requirements. Figure 1 shows the evaluation criteria for the U.S. Figure 2 shows the European and U.S.-equivalent criteria.

Trusted Computer System Evaluation Criteria (TCSEC)

Division	Definition	Class	Features and Assurance
D	No Protection	D	No Class in this division
C	Discretionary Protection	C1	Discretionary Protection
		C2	Controlled Access (*)
B	Mandatory Protection	B1	Labeled Security Protection
		B2	Structured Protection
		B3	Security Domain
A	Verified Protection	A1	Verified Design

**AIX certification*

Figure 1. Trusted Computer System Evaluation Criteria (TCSEC) known as the Orange Book

European ITSEC and Related U.S. Criteria

Correctness Level	Definition	Functional Level	
E1	Cumulative Correctness	F-C1	Corresponds to U.S. C1
E2	Configuration Control	F-C2(*)	Corresponds to U.S. C2
E3(*)	Access to Detailed Design and Source Code	F-B1	Corresponds to U.S. B1
E4	Rigorous Vulnerability Analysis	F-B2	Corresponds to U.S. B2
E5	Correspondence between Detailed Design and Source Code	F-B3	Corresponds U.S. B3/A1
		F-IN	Integrity Protection
		F-AV	System Availability
E6	Formal Model and Description and Correspondence between Them	F-DI	Data Integrity during Data Exchange
		F-DC	Data Confidentiality in Communication
		F-DX	Network Security Confidentiality and Integrity

**AIX certification*

Figure 2. European ITSEC and related U.S. criteria

AIX 4.2 Security Evaluation

AIX 4.2 security is evaluated at ITSEC E3 level of assurance and F-C2 function class. The E3 level of assurance is typically found in systems with a security function class of F-B1 or higher. These systems are known as trusted systems, mandatory label systems, multilevel systems, or Compartmental Mode Workstations (CMWs).

The evaluation of AIX on RS/6000 hardware included analysis of the source code and evaluation of the IBM AIX development facility in Austin, Texas, which also complies with the ISO 9000 standard. In addition, site security, the AIX development process, and the distribution procedures were successfully evaluated according to the ITSEC requirements for level E3.

The ITSEC F-C2 function class provides a finely grained, discretionary access control. This makes users individually accountable for their actions through identification procedures, auditing of security-relevant events, and resource isolation.

AIX provides additional security features that map higher classes of function, such as trusted path (F-B2) and access control lists (F-B3). AIX passed extensive security and penetration tests during the evaluation, resulting in an improved level of quality and security. A complete set of security-relevant documentation required for the evaluation is available. Figure 3 shows the AIX certificate.

AIX 4.2 Security Features

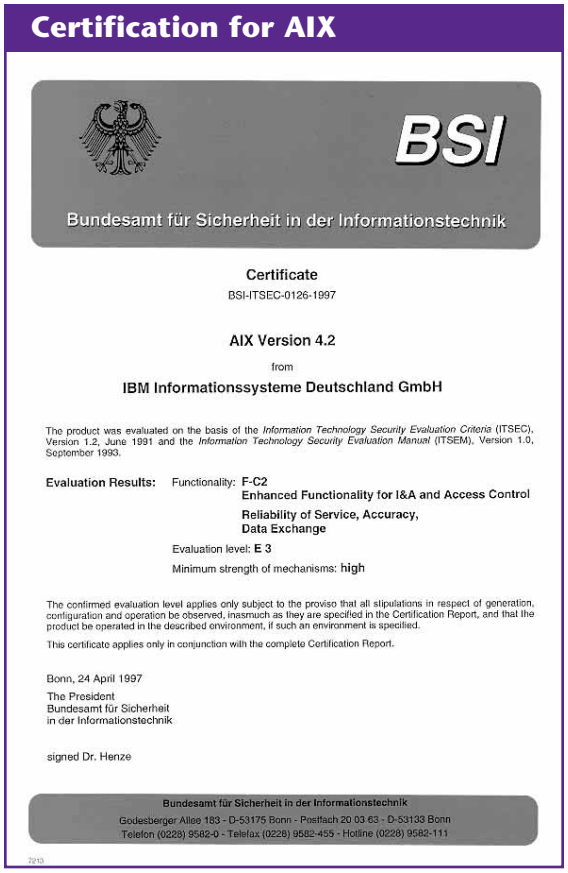
Although hardware protection is available with any RS/6000 system, AIX exceeds the F-C2 security function class with these features:

- Enhanced user identification and authentication
- Data protection through access control lists in addition to the normal UNIX permissions
- Protected password and security databases
- Trusted Path, which prevents applications from trapping the user name and password sequence

AIX passed extensive security and penetration tests during the evaluation, resulting in an improved level of quality and security.

- Login and port control
- User and port restriction capability
- User and port lockout after several failed authentication attempts to log in to the system
- User and port time restriction
- Extensive object-oriented audit subsystem with more than 133 auditable events plus customer configurable events
- Password management
  - —Password minimum age
  - —Password lifetime
  - —Password composition and length
  - —Password reuse
  - —Password triviality checking, including checks against dictionaries of weak passwords
  - —Password expiration warning that can be set
- Security and user management through System Management Interface Tool (SMIT)
- Trusted Computing Base (TCB)
- Integrity of security-sensitive databases, files, and commands
- Trusted shell

Certification for AIX



BSI

Bundesamt für Sicherheit in der Informationstechnik

Certificate

BSI-ITSEC-0126-1997

AIX Version 4.2

from

IBM Informationssysteme Deutschland GmbH

The product was evaluated on the basis of the *Information Technology Security Evaluation Criteria* (ITSEC), Version 1.2, June 1991 and the *Information Technology Security Evaluation Manual* (ITSEM), Version 1.0, September 1993.

Evaluation Results: Functionality: F-C2
Enhanced Functionality for I&A and Access Control
Reliability of Service, Accuracy, Data Exchange
Evaluation level: E 3
Minimum strength of mechanisms: high

The confirmed evaluation level applies only subject to the proviso that all stipulations in respect of generation, configuration and operation be observed, inasmuch as they are specified in the Certification Report, and that the product be operated in the described environment, if such an environment is specified.

This certificate applies only in conjunction with the complete Certification Report.

Bonn, 24 April 1997
The President
Bundesamt für Sicherheit
in der Informationstechnik

signed Dr. Henze

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Hotline (0228) 9582-111

7210

Figure 3. Certification received for AIX

- Customized authentication enabling customers to incorporate and use an alternative authentication mechanism, such as smartcards
- Two-person rule authentication: two users must authenticate to allow a third user to log on
- Single-user level password
- Single sign on for Distributed Computing Environment (DCE)
- User resource limitations
- Security Application Programming Interface (API)
- Journal log of the file system
- Enhanced availability through the mirroring capability of the Logical Volume Manager (LVM)
- Online security documentation through InfoExplorer™

The flexibility of AIX security enables it to grow with your company, because it is compatible with previous and future technology. It is also available on all RS/6000 products. Because the security is integrated, extra packages and recompilation are not necessary. During installation you can choose whether to install TCB to run integrity checks.

Conclusion

AIX now has an ITSEC evaluation and certification that was performed by an independent third party and certified by a governmental authority. Secure and reliable, AIX will enable customers to preserve the availability, integrity, and confidentiality of their information and IT resources. The E3 security certificate makes AIX one of only a few commercial UNIX systems evaluated at this level.

For more information see the IBM AIX Web site at http://www.rs6000.ibm.com or the IBM UBG Security Web site (available to IBM employees only) at http://w3.munich.ibm.com/ubg-security/.

***Dinesh Vakharia**, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Mr. Vakharia is a senior programmer/manager in the AIX Security System. His current responsibilities include the functionality of the AIX base operating system security. He holds a Masters in Electrical Engineering from Washington State University.*

***Salvatore LaPietra**, IBM Unternehmensberatung GmbH, Munich, Germany. Mr. LaPietra is an IT security senior consultant with over 10 years experience with IT security. He has a BS in Computer Science from the University of Torino in Italy.*