TAMÁS SZÁDECZKY MSc[1]

IT SECURITY STANDARDS IN THE FIELD OF MILITARY

KATONAI INFORMATIKAI RENDSZEREK BIZTONSÁGI SZABVÁNYAI

The work gives a global overview of the information technology's industrial civil standards, which are widely used and admired internationally, such as the ISO 27001:2005, which is the new international standard of Information Security Management System, and the ISO 17799 about the practical rules of controlling information safety, BS 7799 about Information Technology Security Evaluation Criteria (ITSEC), Common Criteria for IT Security Evaluation (CC), etc. The presentation also deals with the possibility of applying civil standards in the Hungarian Defence Forces and applying the standards during the actual ongoing development procedures.

A cikk átfogó áttekintést nyújt az informácios rendszerek biztonsági kérdéseiről és a különböző szabványokról. (ISO 27001:2005, ISO 17799, BS 7799 stb.)

1. Foreword

In the eighties it was thought that the very intensive advancement of electronics and computer technology involves the absolute primate of the IT based live. I mean that when the Internet became popular and reachable for everybody not only the governmental organisations, the scientists thought that in the nineties everybody will do the shopping via the Internet, the paper based mailing, procedures and data storing will be done only on computers. Now in the twenty-first century we now that is was just a dream. But why?

The intensive enhancement of the technology, possibilities and purchasing power did not involved the application development at the same rapid pace. By the way the security of the network-based activities did not reached the reassuring level. The enhancement and legal usability of

[1] HDF Signals and IT Command. E-mail: szadeczky.tamas@mil.hu.

public key cryptography and strong secret key algorithms gave the possibility to the computer users for secure communications, but it is still not enough. The security of a computer hardware element, computer system or network depends on the full picture, by the way the weakest part's security determines the security level of the overall system.

The aim is to make the security of the IT elements, systems and networks to the same level in every aspects. This 'making' can be evaluations of the existing systems or designing new ones. The assessment of the security level without standards is possible, but not trustworthy. The IT security standards give a universal framework to our work, making the assessment easier and giving the possibility of using the results elsewhere, for example as a part of a quality management audit.

This work introduces the most important and widely used IT security standards and the possibilities of using them at the Hungarian Defence Forces.

2. TCSEC

The Trusted Computer Systems Evaluation Criteria (TCSEC) was the first notable standard in the field of IT security. It was written by the Department of Defense of the United States of America in 1983. It was revised in 1985. The TCSEC cares with the assessment of the level of computer systems' security. The data on the assayed systems are the subject of state- or service secrets, or in other words classified information. The TCSEC, which was called Orange Book because of the colour of its front cover, was a real military IT security standard which was written in the coldest times in the Cold War. The TCSEC was made mainly for the U. S. Government and the armed forces. For the practical use of TCSEC the different services made their regulations to join the requirements to the concrete situations. The Army Regulation 380-19 can be an example for regulation of services.

The TCSEC punctuated the significance of the security policies, which has to be well-defined and enforced by the system. The policy can be mandatory with full access control or discretionary. The accountability must be also assured in the system. It means that all the activities made in the system have to be bound to a user (called identification), the user's authorization to resources has to be verified (authentication), the logs have to protected and the authorized personnel can easily access and process them (auditing). These requirements certainty are made by assurance mechanisms. The mechanisms can be operational, like the system architecture, integrity, the trusted facility management and trusted recovery. These can be life-cycle assurances like the security testing, design specification and verification, configuration management and the trusted distribution. All of the above mentioned has to be continuously protected against unauthorised changes. In every classes described later different set of documentations are required such as the test documentation and design documentation, the trusted facility manual and the security features user's guide.

The categorisation of the security levels in the TCSEC is divided to four divisions and several classes in the divisions. These categories are the following: [1]

D — Minimal Protection

- ➢ Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division.

C — Discretionary Protection

- ➢ C1 — Discretionary Security Protection
  Separation of users and data
  Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
- ➢ C2 — Controlled Access Protection
  More finely grained DAC
  Individual accountability through login procedures
  Audit trails
  Resource isolation

B — Mandatory Protection

- ➢ B1 — Labeled Security Protection
  Informal statement of the security policy model
  Data sensitivity labels
  Mandatory Access Control (MAC) over select subjects and objects
  Label exportation capabilities
  All discovered flaws must be removed or otherwise mitigated
- ➢ B2 — Structured Protection
  Security policy model clearly defined and formally documented
  DAC and MAC enforcement extended to all subjects and objects

Covert storage channels are analyzed for occurrence and bandwidth

Carefully structured into protection-critical and non-protection-critical elements

Design and implementation enable more comprehensive testing and review

Authentication mechanisms are strengthened

Trusted facility management is provided with administrator and operator segregation

Strict configuration management controls are imposed

- B3 — Security Domains

Satisfies reference monitor requirements

Structured to exclude code not essential to security policy enforcement

Significant system engineering directed toward minimizing complexity

A security administrator is supported

Audit security-relevant events

Automated imminent intrusion detection, notification, and response

Trusted system recovery procedures

Covert timing channels are analyzed for occurrence and bandwidth

An example of such a system is the XTS-300, a precursor to the XTS-400

A — Verified Protection

- A1 — Verified Design

Functionally identical to B3

Formal design and verification techniques including a formal top-level specification

Formal management and distribution procedures

An example of such a system is SCOMP, a precursor to the XTS-400

- Beyond A1

System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).

Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.

Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.

Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.

3. ITSEC

As the European equivalent of TCSEC, Great-Britain, France, the Netherlands and Germany made the Information Technology Security Evaluation Criteria (ITSEC). The ITSEC version 1.2 was experimentally published in 1991 for the European Communities. The ITSEC is quite similar to the TCSEC in its principles and requirements, but the ITSEC defines specific requirements for IT system types.

The ITSEC defines seven evaluation levels in respect of the confidence in the correctness of a Target of Evaluation (TOE). E0 designates the lowest level and E6 the highest.

The seven evaluation levels can be characterised as follows: [2]

Level E0

This level represents inadequate assurance.

Level E1

At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.

Level E2

In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.

Level E3

In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.

Level E4

In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.

Level E5

In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.

Level E6

In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

There are ten Example Functionality Classes in the ITSEC. These are made to give system specific requirements. Example Functionality Classes F-C1, F-C2, F-B1, F-B2, F-B3 have been derived from the functionality requirements of the TCSEC classes.

Example Functionality Class F-IN is for TOEs with high integrity requirements for data and programs. It can be used for example in database systems.

Example Functionality Class F-AV has high availability requirements, it is recommended for industrial controllers.

In Example Functionality Class F-DI the highest priority is the data integrity during data exchange.

Example Functionality Class F-DC is for TOEs which has to give maximal confidentiality during the data exchange, for example these can be cryptographic systems.

Example Functionality Class F-DX is meant for networks with high demands on the confidentiality and integrity of the information to be exchanged. For example, this can be the case when sensitive information has to be exchanged via insecure networks.

4. Common Criteria

Aimed to make an international standard, the European Communities, the United States and Canada made the Common Criteria for Information Technology Security Evaluation, shortly called Common Criteria (CC). Its version 2.0 became an international standard ISO/IEC 15408

„Common Criteria for Information Technology security Evaluation, version 2.0". In Hungary the Inter-Departmental Committee of Informatics (ITB) issued the CC 2.0 as the recommendation no. 16.

The Common Criteria has eleven functionality classes in which are the functional requirements detailed. These are the following: [3]

Class FAU: Security audit
Class FCO: Communication
Class FCS: Cryptographic support
Class FDP: User data protection
Class FIA: Identification and authentication
Class FMT: Security management
Class FPR: Privacy
Class FPT: Protection of the TSF
Class FRU: Resource utilisation
Class FTA: TOE access
Class FTP: Trusted path/channels

There are several families in each class and several components in each families which are indicated like FAU_ARP.1. All the components are expressions about the requirement.

The assurance classes are: [4]

Class APE: Protection Profile evaluation
Class ASE: Security Target evaluation
Class ACM: Configuration management
Class ADO: Delivery and operation
Class ADV: Development
Class AGD: Guidance documents
Class ALC: Life cycle support
Class ATE: Tests
Class AVA: Vulnerability assessment
Class AMA: Maintenance of assurance

The level of security is determined by the Evaluation Assurance Levels (EALs) like the Ex levels in the ITSEC. These are: [4]

EAL1 — functionally tested
EAL2 — structurally tested
EAL3 — methodically tested and checked
EAL4 — methodically designed, tested, and reviewed
EAL5 — semiformally designed and tested

EAL6 — semiformally verified design and tested
EAL7 — formally verified design and tested

5. ITIL

The IT Infrastructure Library (ITIL) was developed by the Central Computing and Telecommunications Agency (CCTA) for supporting high quality cost effective IT services. By the way the ITIL is not only an IT security standard, but it is a best practices collection in the field of services.

The ITIL was developed in the 80's, and the actual version is v3 issued in 2005, and it is constantly developed.

The ITIL Service Management became a British Standard BS 15000 and later an international standard ISO 20000.

There are nine ITIL books, which are the following:

1. Service Delivery (part of IT Service Management);
2. Service Support (part of IT Service Management);
3. ICT Infrastructure Management;
4. Security Management;
5. The Business Perspective;
6. Application Management;
7. Software Asset Management;
8. Planning to Implement Service Management;
9. ITIL Small-Scale Implementation.

6. BS 7799-1 (ISO 17799)

The BS 7799, where the BS stands for British Standard, was issued by the British Standard Institute in 1995. Now this original part is called Part 1. It became an international standard, called ISO/IEC 17799:2000 „Information Technology — Code of practice for information security management". Its latest version is ISO/IEC 17799:2005.

The ISO/IEC 17799:2005 consists of the following chapters: [5]

- Risk assessment and treatment;
- Security policy;
- Organization of information security;

- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance.

7. BS 7799-2 (ISO 27001)

The British Standard Institute attached a second part to BS 7799 in 1999, it's name is BS 7799-2 or BS 7799 Part 2 "Information Security Management Systems - Specification with guidance for use." The International Organization for Standardization and the IEC adopted it to an international standard ISO/IEC 27001:2005.

The standard determines the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) and specifies requirements for the management of the implementation of security controls.

The ISO/IEC 27001 aligns with quality assurance standards like ISO 9001 or ISO 14001. It is recommended to use this standard together with ISO/IEC 17799:2005.

8. COBIT

In 1992 the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) issued the Control Objectives for Information and related Technology (COBIT), which is a framework for IT management.

The controlled processes [6] by the COBIT are the following.

Domain		*Process*
Planning & Organisation	PO1	Define a strategic IT plan
	PO2	Define the information architecture
	PO3	Determine technological direction
	PO4	Define the IT organisation and relationships
	PO5	Manage the IT investment
	PO6	Communicate management aims and direction
	PO7	Manage human resources
	PO8	Ensure compliance with external requirements
	PO9	Assess risks
	PO10	Manage projects
	PO11	Manage quality
Acquisition & Implementation	AI1	Identify automated solutions
	AI2	Acquire and maintain application software
	AI3	Acquire and maintain technology infrastructure
	AI4	Develop and maintain procedures
	AI5	Install and accredit systems
	AI6	Manage changes
Delivery & Support	DS1	Define and manage service levels
	DS2	Manage third-party services
	DS3	Manage performance and capacity
	DS4	Ensure continuous service
	DS5	Ensure systems security
	DS6	Identify and allocate costs
	DS7	Educate and train users
	DS8	Assist and advise customers
	DS9	Manage the configuration
	DS10	Manage problems and incidents
	DS11	Manage data
	DS12	Manage facilities
	DS13	Manage operations
Monitoring	M1	Monitor the processes
	M2	Assess internal control adequacy
	M3	Obtain independent assurance
	M4	Provide for independent audit

9. Applying standards in the HDF

The Hungarian Defence Forces are going through a permanent transformation from the change of the political system in 1989. [7] The next step was joining the North Atlantic Treaty Organization in 1998. The requirements are high in all fields. The IT security is not yet harmonised with standards, just with NATO regulations. Now the Hungarian Defence Forces does not use any international industrial IT security standards for the design, installation and implementation of the military networks, just inner regulations which are secure, but these does not make possible to determine their security level.

In my opinion the possible later use of international industrial IT security standards can make the interoperability with other NATO or civil networks.

From the standards detailed above the TCSEC, ITSEC and the Common Criteria could only be used for evaluating hardware and software elements, but not for complex IT systems. For the complex evaluation the ITIL, the ISO/IEC 17799 and the COBIT can be used.

The ITIL is the most complicated standard. In several times the ISO/IEC 17799 and the COBIT got part from the ITIL, but nowadays it is not so popular as the others. Because of the decreasing popularity less documentations and materials are accessible.

The COBIT was published in the United States by experts caring with financial informatics. This is why it can be used very good in the field of finance (for example banking informatics), but not really fits military requirements.

Because of its structure, approach, and details the ISO/IEC 17799 together with the ISO/IEC 27001 are the best recommended for using as IT security standard for designing and implementing secure systems and networks for IT experts. Nowadays the ISO/IEC 17799 seems to be the most popular IT security standard. Since the correlations of army's requirements and the pure IT security needs and the popularity of this pair of standards makes them recommended to use in the Hungarian Defence Forces.

BIBLIOGRAPHY

[1] Department of Defense Trusted Computer Systems Evaluation Criteria. Department of Defense Standard, December 1985.

[2] Information Technology Security Evaluation Criteria (ITSEC). Department of Trade and Industry, United Kingdom, London, June 1991.

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999.

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999.

[5] Magyar Szabvány MSZ ISO/IEC 17799 Informatika. Az informatikai biztonság menedzselésének eljárásrendje. MSZT, 2002.

[6] COBIT 3rd Edition Audit Guidelines, COBIT Steering Committee–IT Governance Institute, July 2000.

[7] Horváth, László–Szádeczky, Tamás: Thoughts about the transformation of the armed forces.

[8] Becz Tamás et al.: Az informatikai hálózati infrastruktúra biztonsági kockázatai és kontrolljai, IHM–MTA SZTAKI, Budapest, 2006.

[9] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.1, August 1999.

[10] KÜRT Computer Rendszerház Rt.: Informatikai tanúsítás és audit megvalósítása Magyarországon. Budapest, 2002.

[11] Magyar Szabvány MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények. MSZT, 2006.

[12] Muha Lajos: Szabványok és ajánlások az informatikai biztonság területén. VIII. Országos (Centenáriumi) Neumann Kongresszus, 2003.

[13] Wikipedia, the free encyclopedia. http://en.wikipedia.org (09/14/2006)