

From Common Criteria to Elliptic Curves – ISO/IEC JTC 1/SC 27 IT Security Techniques

a report by

Walter Fumy

*Chairman, International Organization for Standardization and International Electrotechnical Commission
Joint Technical Committee 1, Standards Committee 27, IT Security Techniques (ISO/IEC JTC1/SC27)*



Dr Walter Fumy is Chairman of the International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee 1, Standards Committee 27, IT Security Techniques (ISO/IEC JTC1/SC27). He is also Vice President of Technologies, Trusted Networks and Applications at Siemens AG where his work ranges from cryptographic research to security consulting and participation in international security forums. For many years, he has been involved actively in the standardisation of security techniques and is Vice Chairman of ETSI TC Security. Dr Fumy has published more than 60 papers and books in these areas. He has served on numerous program committees and was Program Chair of Eurocrypt '97.

Introduction

Absolutely secure information technology (IT) products or systems do not exist. IT security is an appropriate risk management strategy that identifies, controls, eliminates or minimises uncertain events that may affect IT system resources and information assets adversely. In practice, levels of IT security are established initially through an understanding of the essential security requirements of consumers and business users. These requirements range from best practice guidelines on how to conduct a security risk assessment and evaluation of IT systems and products to the employment of specific cryptographic techniques and mechanisms. Appropriate levels of security are then achieved by implementing a suitable set of information management policies in addition to adequate sophisticated assurance methods as well as suitable cryptographic technologies.

This is the approach that has been adopted by the International Organization for Standardization and the International Electrotechnical Commission/Joint Technical Committee 1 Standards Committee 27 (ISO/IEC JTC 1/SC 27) IT Security Techniques. Established in 1989, this subcommittee today has members from almost 40 countries and has become a primary resource for international standards on application-independent IT security techniques for use by industry and other standardisation groups. The technical work is carried out in three Working Groups:

- WG 1 requirements, security services and guidelines;
- WG 2 security techniques and mechanisms; and
- WG 3 security evaluation criteria.

These Working Groups are responsible for over 50 International Standards and Technical Reports and more than 30 current work items, most of which are due to be completed within the next two years. Recent SC 27 publications include the following.

- ISO/IEC 9796-3: digital signature schemes giving message recovery –
Part 3: discrete logarithm-based mechanisms.

- ISO/IEC 9797-2: message authentication codes (MACs) –
Part 2: mechanisms using a dedicated hash-function.
- ISO/IEC 10118: hash functions –
Part 1: general, second edition; and
Part 2: hash-functions using an n-bit block cipher algorithm, second edition.
- ISO/IEC TR 13335: guidelines for the management of IT security –
Part 4: selection of safeguards.
- ISO/IEC TR 14516 (= ITU-T X.842) – guidelines on the use and management of trusted third-party (TTP) services.
- ISO/IEC 15816 (= ITU-T X.841) – security information objects for access control.
- ISO/IEC 15945 (= ITU-T X.843) – specification of TTP services to support the application of digital signatures.
- ISO/IEC 15946 – cryptographic techniques based on elliptic curves –
Part 1: general;
Part 2: digital signatures; and
Part 3: key establishment.
- ISO/IEC 17799: Code of Practice for Information Security Management.

(A detailed summary and catalogue of SC 27 projects and standards is available to download from <http://www.din.de/ni/sc27/>)

IT Security Management

Information that is held by IT products or systems is a critical resource that enables organisations to succeed in their mission. In addition, individuals have a reasonable expectation that their personal information which is stored in IT products or systems will remain private, be available to them as needed and not be subject to unauthorised modification. IT products or systems should perform their functions

while exercising proper control of the information to ensure that it is protected against hazards such as unwanted or unwarranted dissemination, alteration or loss. The term 'IT security management' is used to cover prevention and mitigation of these and similar risks.

SC 27 has completed a number of projects that are related to the management of IT security and to the establishment of trust services. For those organisations conducting risk assessment, there is a Technical Report ISO/IEC TR 13335-3, 1998, entitled *Guidelines for the Management of IT Security (GMITS)*. For organisations that have carried out a risk assessment and want to know how to go about selecting a set of safeguards, there is another Technical Report (ISO/IEC TR 13335-4) in the same series, which describes a generic process for making such a selection. A recently approved new work item addresses the security issues that are related to information and communication networks and the risks that could arise from interconnecting systems.

In 1993, a number of sponsoring national organisations pooled their efforts and began a joint activity to align their approaches into a single set of IT security criteria that could be used widely. This activity was named the Common Criteria (CC) Project. Recognising the business need and opportunity, SC 27 helped to provide the impetus and input for the CC Project to be developed into an international standard for IT security evaluation criteria. Through an active liaison process, the CC Project became, in effect, SC 27's editing arm, providing the extensive resources that are needed for public reviews, evaluations, trial use and associated revisions to the specification.

In June 1999, the ISO/IEC National Bodies accepted CC version 2.0 with minor changes as ISO/IEC 15408: evaluation criteria for IT security, more commonly known for historical and continuity purposes as 'Common Criteria' (CC). Since then, a number of work items related to implementing the criteria and to IT security assurance have been underway.

IT security is an appropriate risk management strategy that identifies, controls, eliminates or minimises uncertain events that may affect IT system resources and information assets adversely.

Best practices or codes of practice for information security management provide a compilation of the combined experiences of many institutions regarding the way that they manage IT security. ISO/IEC 17799: Code of Practice for Information Security Management is based on British Standard (BS) 7799 and gives guidance and recommendations on good practices in this area. Basing its IT security management on ISO/IEC 17799, a company can be confident that it is following information security practices that are accepted internationally as important and relevant.

IT Security Evaluation and the Common Criteria

In the past, several nations established their own approaches to IT security evaluation, both individually and in groups. They each developed separate criteria for the security evaluation of IT products and systems. While this had certain advantages in terms of speed to market, it raised confusion among potential users and difficulties for product manufacturers who were seeking to sell into the global market.

Security Mechanisms

SC 27 identifies the need and requirements for IT security techniques and mechanisms. In addition, it develops terminology, general models and standard specifications. The scope covers both cryptographic and non-cryptographic techniques including confidentiality, entity authentication, non-repudiation, key management and data integrity such as message authentication, hash functions and digital signatures.

In the area of security mechanisms, highly sophisticated security standards are available largely. SC 27, and organisations in liaison, are working diligently to maintain these standards and to establish new ones in order to keep up with the state of the art.

Recently approved new projects include encryption algorithms, random number generation, prime number generation and time-stamping services and protocols. As a first step in the work on a multipart ISO/IEC standard for Encryption algorithms, a call for contributions was prepared that requested

proposals for encryption algorithms to be included in the standard.

Trust and Digital Signatures

Consumers, businesses and public administrations need an environment of trust that is at least equivalent to that of proven paper-based operations in order to transact business online or to communicate with each other electronically. They need to be able to:

- assume with confidence that all parties are who they claim to be;
- authenticate the identity of other participating entities and, if permitted, verify the role that they play in the transaction, i.e. whether they are acting on their own or on an organisation's behalf;
- be assured of the integrity of information; and
- ensure that business transactions or communications cannot be repudiated at a later stage.

It is well-accepted that cryptographic techniques based on digital signatures and electronic certificates are the best way of providing the level of trust required for e-business exchanges, i.e. public key cryptography has shown itself to be the tool of choice for the design and implementation of scalable secure systems. Many of SC 27's projects are relevant for the important area of electronic signatures, including the multipart ISO/IEC 9796: digital signature schemes giving message recovery and ISO/IEC 14888: digital signatures with appendix.

Elliptic Curve-based Public Key Cryptography

Well-established, asymmetric cryptographic techniques are typically based on hard mathematical problems, such as integer factorisation – for example, the RSA scheme – or discrete logarithms over finite fields – for example, Diffie-Hellman key establishment. Corresponding algorithms are defined as transformations based on computations modulo very large numbers. Due to improvements in integer factorisation and parallel processing, the future may demand very large moduli for these schemes.

Cryptosystems that are based on the elliptic curve discrete logarithm problem provide a promising alternative means of implementing public key cryptography. The primary advantage of elliptic curve cryptosystems is their cryptographic strength relative to the required parameter size, i.e. elliptic curves offer more security per bit than other public key systems.

SC 27 has standardised elliptic curve-based cryptographic techniques in several digital signature and key management documents. In addition, a multipart standard that is dedicated to elliptic curve cryptography is to be published soon, known as ISO/IEC 15946.

Not the Whole Story

Many other standards organisations and industry groups are active in IT security, each addressing specific requirements. Such organisations include Asynchronous Transfer Mode (ATM) Forum, Common Criteria Interpretation Management Board (CCIMB), Institute of Electrical & Electronic Engineers, Inc. (IEEE) P1363, Internet Engineering Task Force (IETF), ISO/TC 68 “Banking and Finance”, International Telecommunication Union Telecommunication sector (ITU-T) SG7, Object Management Group (OMG), SET-II, and Wireless Application Protocol (WAP) Forum. SC 27 as the lead subcommittee for security within ISO/IEC is open to co-operation with all such groups to ensure the timely development of internationally agreed generic IT management guidelines or the associated sophisticated security technology standards. Despite their differences, the common parameter across all of these organisations is that voluntary openness and successful security go hand in hand.

While highly sophisticated security standards are largely available, their broad use in products and services is still in the introductory phase. Progress in the deployment of security techniques also depends on non-technical issues. These include, for example, intellectual property, export controls, legality of digital signatures and acceptability of particular techniques.

The use of IT security techniques and, in particular, of electronic signatures in the operation of business online constitutes a core element for the development of today's competitive environment for Global Information Infrastructure (GII) and e-business. Work is well underway in many regions worldwide to establish infrastructures to enable digital signatures. Appropriate legal and business practices are being introduced to allow the use of electronic signatures, as a replacement for hand-written signatures, in all aspects of public administration services, and in legal proceedings. Within Europe, for example, the European Electronic Signature Standardization Initiative (EESSI) is aiming to complete its work plan before the end of 2001. After this, the use of digital signatures in online business operations will be implemented more easily across the European Community and is likely to become a core element in the further adoption of e-business. ■