### ISO/IEC JTC 1/SC 27 "IT Security Techniques"

or

# Why Bother About ISO Security Standards ?

## About the Panel

ISO/IEC JTC 1/SC 27 „IT Security Techniques" is a primary resource of international standards on application-independent IT security techniques. Since its foundation in 1990, SC 27 has published more than thirty international standards and technical reports, twelve are expected for 1999. SC 27's area of work is the standardization of generic methods and techniques for IT security. The scope ranges from cryptographic techniques and mechanisms to security guidelines, criteria for IT security evaluation, and management support documentation. Among SC 27's „users" are other standardization groups that adopt SC 27 standards where appropriate and provide a selection of required options. An important means to ensure the timely development of market-oriented IT security techniques is the cooperation with such groups, e.g., ITU-T SG7/Q20, or TC 68 „Banking".

The panel is structured to address questions of interest to the Information Systems Security community. It will discuss scope, organization, publications, and current work plan of ISO/IEC JTC 1/SC 27 „IT Security Techniques". Special attention will be given to security standards that have recently been approved for publication, to new work items, and to collaborative work with other fora.

## SC 27/WG 1: Requirements, Security Services & Guidelines

WG 1 deals with a number of standardization projects related to the security of information technology including the management of security and services providing security. For organizations that need to know what to do about risk assessment WG1 have produced a Technical Report, GMITS (Guidelines for the Management of IT Security) Part 3, which deals with this topic. For organizations that have carried out a risk assessment and want to know how to go about selecting a set of safeguards WG1 have produced another Technical Report, GMITS Part 4, which describes a generic process for making such a selection. One of the key examples of a set of controls that WG 1 uses to apply this generic process to is the information security management standard BS 7799.

For organizations that need to use digital signatures WG1 are producing a standard that specifies a set of trusted third party (TTP) services to support the use of these types of signature. In addition WG 1 is producing a Technical Report which provides advice and guidance on the use and management of TTPs.

WG 1 is also dealing with the security issues related to networks and the risks that could arise from interconnecting systems. This includes development of a standard on intrusion detection, production of a Technical Report that covers network controls such as security gateways and firewalls, and review of future security work on global information infrastructures and electronic commerce.

## SC 27/WG 2: Security Techniques & Mechanisms

WG 2 provides a center of expertise for the standardization of IT Security techniques and mechanisms. It identifies the need and requirements for these techniques and mechanisms and develops terminology, general models and standard specifications. The scope covers both cryptographic and non-cryptographic techniques and mechanisms including confidentiality, entity authentication, non-repudation, key management and data integrity such as message authentication, hash-functions and digital signatures.

This talk will cover the scope and current work items of WG 2, emphasizing the generic nature of the work, the issue of standardizing algorithms for integrity and confidentiality purposes, and the interface with other committees, e.g., TC 68/SC 2, IEEE P1363, ANSI X9.F, ETSI TC Security.

Many of WG 2's projects are relevant for the area of Digital signatures, including the International Standards ISO/IEC 9796: Digital signature schemes giving message recovery (3 parts) and ISO/IEC 14888: Digital signatures with appendix (3 parts). New work items include

- Cryptographic techniques based on elliptic curves (ISO/IEC CD 15946, parts 1 to 3)
- Time stamping services and protocols (ISO/IEC WD 18014)

## SC 27/WG 3: Security Evaluation Criteria

WG 3 was formed in 1991 to develop international standard criteria for the security evaluation of IT products and systems. At that time, various nations individually and in groups had developed their own approaches to security evaluations of IT products and systems. This variation caused difficulties for product manufacturers seeking to sell into the world market and raised confusion for potential users. WG 3's early work helped provide the impetus and input for the Common Criteria (CC) Project, which was a consortium of nations which had developed their own criteria. The CC Project sought to develop IT security criteria that all could use and to work in concert with WG 3 to create the badly-needed international standard. Via active liaison between the two bodies, the CC Project became in effect WG 3's editing arm, providing the extensive resources needed to develop successive drafts of the CC that were submitted to WG 3 and became ISO drafts. In June 1999, the ISO National Bodies accepted the CC version 2.0 with minor changes as ISO/IEC International Standard 15408: Evaluation Criteria for IT Security (Parts 1 through 3).

Additionally, WG 3 has been active in developing a number of work items related to implementation of the criteria and to IT security assurance, including

- Protection Profile Registration Procedures (ISO/IEC WD 15292).
- Guide for Production of Protection Profiles and Security Targets (ISO/IEC WD 15446).
- Framework for IT Security Assurance (ISO/IEC WD 15443).

The WG 3 work is very closely related to the CC activities. Early in the life of the CC Project, an official "Category C" liaison was established between SC 27 and the Project. This liaison channel has been very useful in providing WG 3 delegates and the ISO National Bodies they represent the opportunity to mold the CC into a document that was acceptable as an ISO International Standard. At the same time, it has helped the CC Project obtain needed input from the IT security community of manufacturers and users. That relationship has also been instrumental in furthering other WG 3 work items, including the Framework for IT Security Assurance (originally a CC Project activity), and the Guide for Production of Protection Profiles and Security Targets.

## TC 68/SC 2: Security Management & General Banking Operations

ISO TC 68/SC 2 is charged, inter alia, with providing technical standards and other guidance to the financial services community in the area of security. Achieving an effective working relationship with ISO/IEC JTC 1/SC 27 is key to future success of SC 2.

This talk will cover a brief history of SC2, describe the working arrangement as it exists today, and forecast the likely shape of future cooperation.

## Biographical Information

**Walter Fumy** has received his Ph.D. in computer science from the University of Erlangen, Germany. Since 1986 he is employed at Siemens AG where his work involves cryptographic research, security consulting and participation in international security standards forums. He has published more than 50 papers in the field of ICT security, including books on cryptography and on security standards and patents.

Since many years Walter Fumy is active in the standardization of security techniques and has been the editor of several standards. Currently he is serving as vice-chairman of ETSI TC Security, and as chairman of ISO/IEC JTC 1/SC 27 "IT Security Techniques".

**Ted Humphreys** is the Convenor of WG1. He has spent over 20 years in the information security business. During this time he has worked for many commercial and government organisations around the world dealing with both telecommunications and computer system security issues. He is the author of many technical and management publications in this field including the Financial Times Report covering a detailed review of “Security of Internet and Business Networking”. He has also been the editor of many standards including the recently published 1999 version of BS 7799 the standard on Information Security Management, a standard being published by many countries in the world.

**Marijke De Soete** studied mathematics at the State University of Ghent (Belgium) where she received her Ph.D. in 1984. She joined Philips in 1989 where she worked as a security adviser. She was responsible for the design and implementation of cryptographic protocols, algorithms and key management systems for applications in the area of telecommunications and secure office communications. Since February 1995 she is employed by Europay International and currently heads the department Payment System Security. Her responsibilities include research & development covering all security aspects of magnetic stripe or chip cards based applications such as debit, credit, purse, electronic commerce as well as the development of the supporting security services such as key management. Furthermore, the department is also responsible for the operation of these security services including a Public Key Certification Infrastructure.

She is also active in the standardisation committees ISO/IEC JTC 1/SC 27 and ISO TC 68. Since 1993 she is convener of Working Group 2 of ISO/IEC JTC 1/SC 27 IT Technology, Security techniques and mechanisms and was editor of some of the authentication standards produced by that group. Dr. De Soete is a member of the IACR (International Association for Cryptographic Research) and has written several articles in the field.

**Eugene F. (Gene) Troy** is a long-time computer scientist with NIST, specializing in computer security. He has been active as a US delegate to SC27/WG3 for many years and is the Project Editor of International Standard 15408-1 (CC Part 1). Gene is one of the organizers of the Common Criteria (CC) Project and was an original member of the CC Editorial and Implementation Boards, which wrote CC versions 1.0 and 2.0. For several years he was the Liaison Officer between SC27/WG3 and the CC Project. Gene is also Chair of the recently-formed Smart Card Security Users Group, which is developing CC-based security requirements and evaluation methods for smart card technology.

**Gerard A. (Jerry) Rainville** holds a Doctor of Jurisprudence, a Master of Business Administration and a Bachelor of Science in Mathematics degrees. He also has completed advanced studies at MIT, the Kennedy School of Government at Harvard, Magdalene College Oxford, University of Paris (Sorbonne) and the Law Schools of Kings College (London), University of Grenoble, and James Mason University.

Jerry was the founder of the National Security Agency’s Center for Standards and has served as its director from its inception to the present. As the director, he is responsible for managing the activities of approximately 100 employees engaged in standards development. He represents NSA on the Department of Defense Technical Architecture Steering Group and Defense Standardization Council.

In the commercial standards world, Jerry serves as the Vice-Chairman of the Banking Security Subcommittee within the International Organization for Standardization. He also leads the working group responsible for security guidelines for financial institutions worldwide. He is the NSA representative to Accredited Standards Committee X9, Financial Services and serves on numerous working groups supporting financial information security needs.

While not engaged in standards activities, Jerry enjoys cooking, reading, playing the organ, and travelling. Jerry is married to Kathleen Sullivan who teaches French and Latin. Their sons are grown and have flown the nest.