International standardization activities in SC 27 regarding Security Assurance and Evaluation

ICCC

September 2005

Mats Ohlin

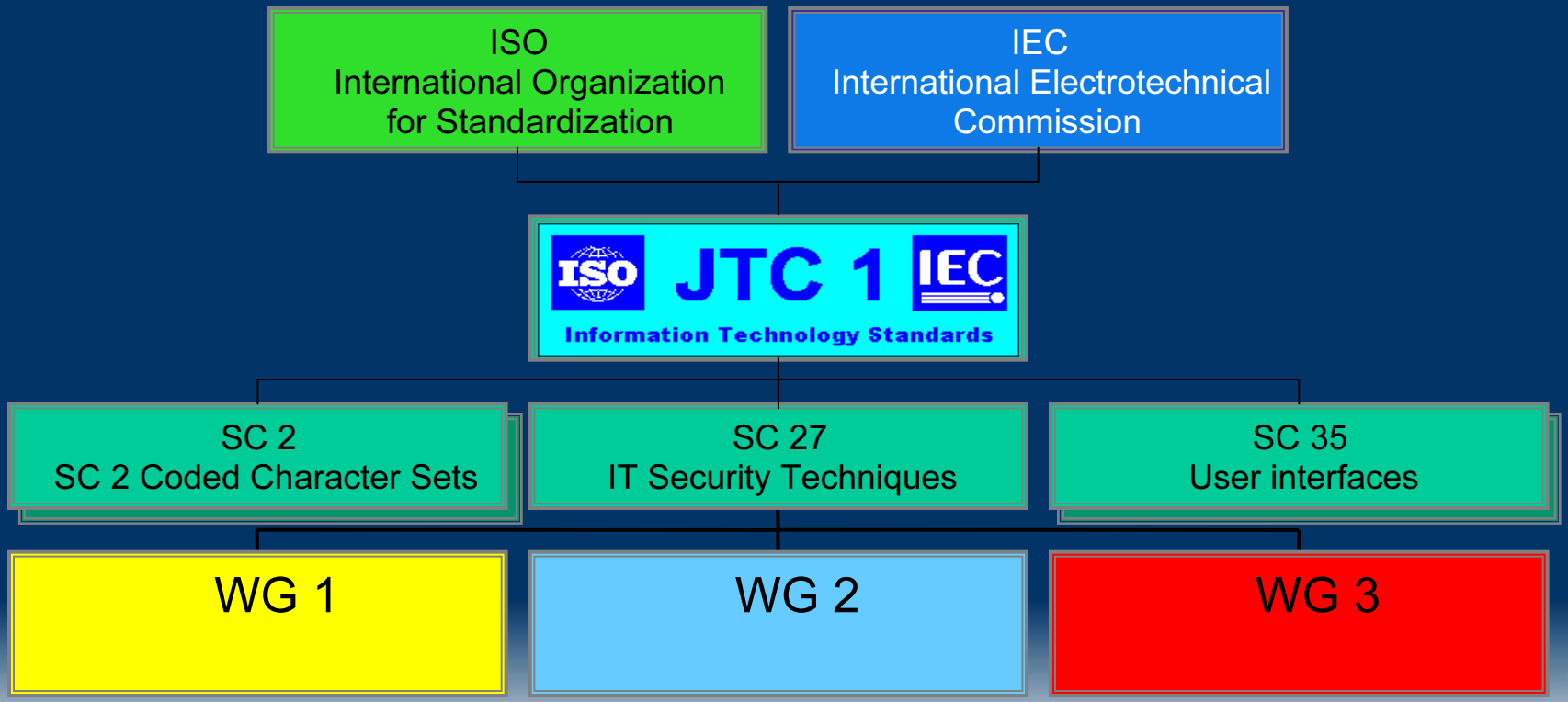
ISO/IEC JTC 1/SC 27/WG 3 Convener

Swedish Defence Materiel Administration

Common Criteria

ICCC

Organization of Standardization Work



SC 27 - Organisation

SC 27 home page:
www.iso.ch:8080/jtc1/sc27/
www.din.de/ni/sc27/

WG 3 home page:
www.gammassl.co.uk/ist33/

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Chairman Mr. W. Fumy
<Walter.Fumy@icn.siemens.de>

SC 27 Sekretariat DIN
Ms. K. Passia
<Krystyna.Passia@din.de>

Working Group 1

Requirements, security services, guidelines

Convener
Mr. T. Humphreys

Working Group 2

Security techniques and mechanisms

Convener
Mr. K. Naemura

Working Group 3

Security evaluation criteria

Convener
Mr. M. Ohlin
<Mats.Ohlin@itsec.fmv.se>

Common Criteria

ICCC

SC 27 - Membership

- 32 P-members (voting)
  - Austria, Australia, Belgium, Brazil, Canada, China, Czech Republic, Denmark, Finland, France, Germany, India, Italy, Japan, Kenya, Republic of Korea, Luxembourg, Malaysia, The Netherlands, New Zealand, Norway, Poland, Russian Federation, Singapore, South Africa, Spain, Sri Lanka, Sweden, Switzerland, UK, Ukraine, USA
- 11 O-members (observers)
  - Argentina, Estonia, Hungary, Indonesia, Ireland, Israel, Lithuania, Romania, Serbia&Montenegro, Slovakia, Turkey

SC 27 - Scope

- Standardization of generic IT security services and techniques, including
  - identification of generic requirements for IT system security services,
  - development of security techniques and mechanisms (*cryptographic* and non-cryptographic),
  - development of security guidelines,
  - development of management support documentation and standards,
  - development of criteria for IT security evaluation and certification of IT systems, components, and products.

Projects within WG 3

15408:1999	Evaluation criteria for IT Security, revision
15292:2001	Protection Profile registration procedure
15446:2004	Guide on the production of Protection Profiles and Security Targets (PPST Guide)
15443:	A framework for IT security assurance (FRITSA)
18045:	Methodology for IT security evaluation (CEM)
19790:	Security requirements for cryptographic modules
19791:	Security assessment of operational systems
19792:	A framework for security evaluation and testing of biometric technology
21827:2002	Systems security engineering - Capability maturity model (SSE-CMM)
[TBD]	Test requirements for cryptographic modules

ISO/IEC 15408:2005

- IS 15408-1: Evaluation criteria for IT Security - Part 1: Introduction and general model
- IS 15408-2: Evaluation criteria for IT Security - Part 2: Security functional requirements
- IS 15408-3: Evaluation criteria for IT Security - Part 3: Security assurance requirements

What Makes Security So Special?

- Security Field is characterised by two special circumstances:
- Testing of functional conformance is relatively easy; security is concerned with *non-existence* [of vulnerabilities].
- The assumption of an active, probing intellect which strives to find a suitable, exploitable weakness…

Common Criteria

ICCC

Quotation

Today's operating systems

do not need hackers…

they fall apart
all by themselves

Peter Neumann, SRI

Evaluation Fundaments

- Basic Aspects of Evaluation
  - Aims to eliminate/reduce risk for existence of exploitable vulnerabilities
  - *More is better*
    - There is always a residual risk - 100 % security does not exist
  - Challenge is to find an effective (optimal) method, according to given costs, to find as many flaws as possible.
  - Assume qualified adversaries may make same kind of analysis, planning an attack
  - Make his task more difficult/expensive; reduce our risk.
- Long time goal
  - Ensure that the developer does the right things right from start (c.f. Dijkstra on handling bugs)

15408 Highlights

- Toolbox for specifying security requirements
  - Functional
  - Assurance
- A Protection Profile (PP) intended to describe the needs for a generic product within a user group, community of interest etc.
- A Security Target (ST) summarizes the evaluation background and goals of what is delivered

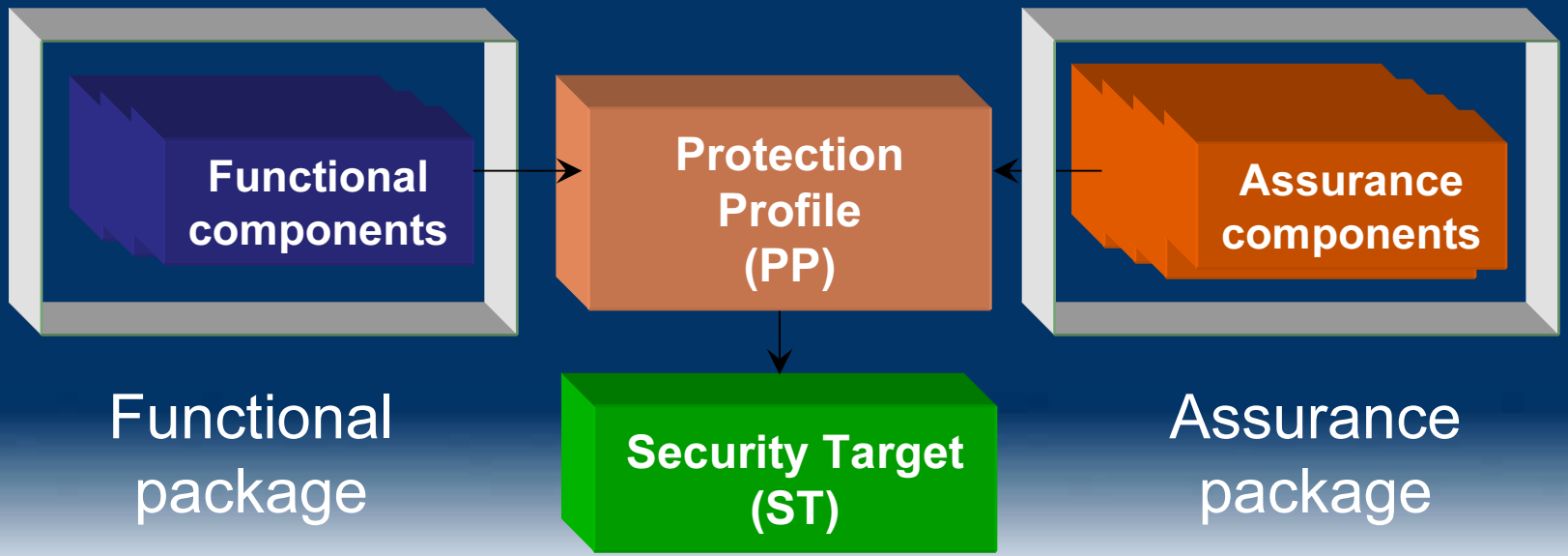
Security Target (ST)

Security Target summarizes the evaluation background and goals:

- TOE description
- TOE Security Environment
- Security Objectives
  - For the Target of Evaluation (TOE)
  - For the Environment
- IT Security Requirements
  - TOE Security Requirements: Functional; Assurance
  - For the IT Environment
- TOE Summary Specifications:
  Security Functions, Assurance Measures
- [PP Claims]
- Rationale (for the 4 preceding sections)

Common Criteria Structure

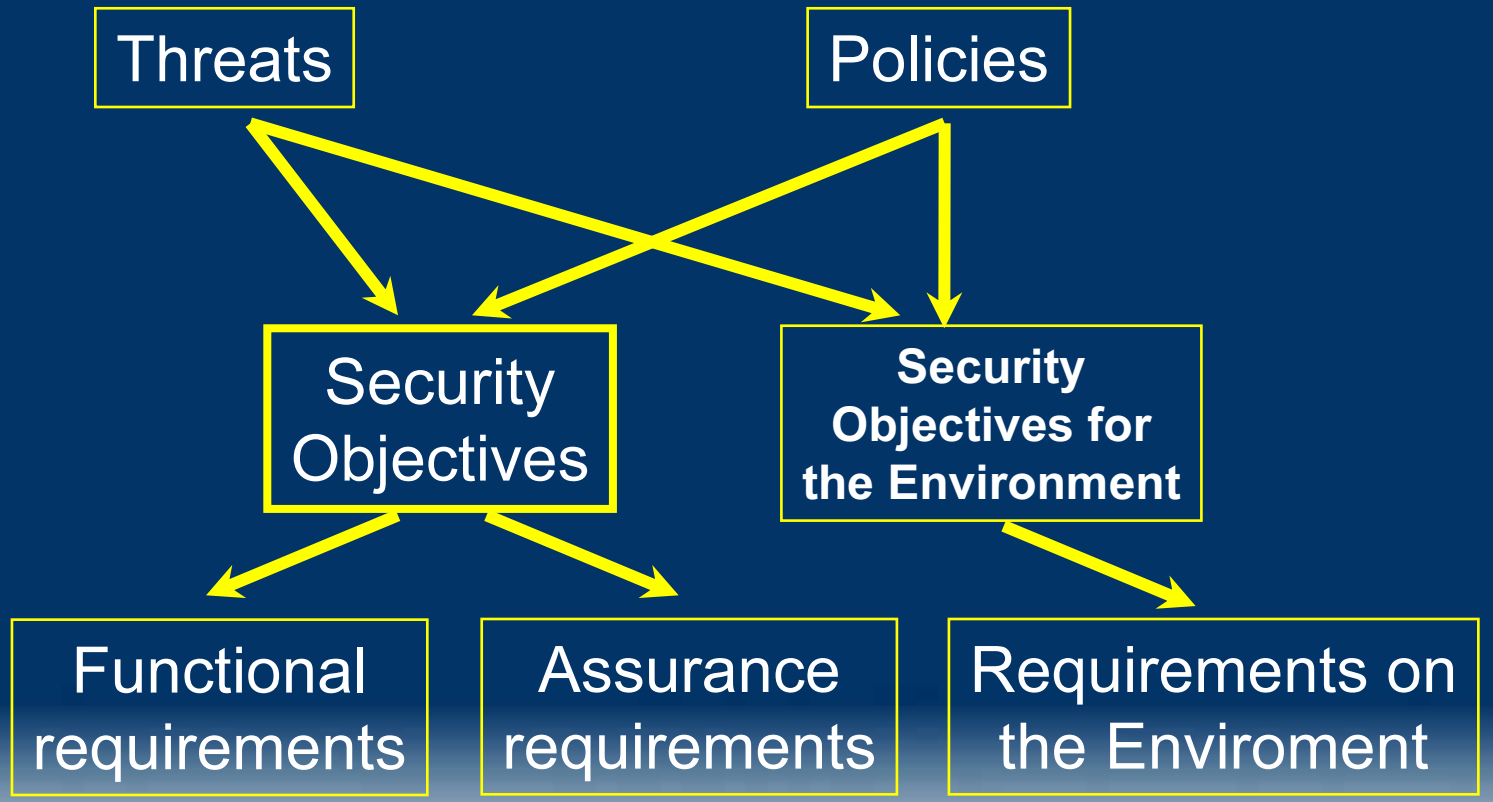
- General Model
  - *Functional Package*, FP
  - *Assurance Package*, AP
  - *Protection Profile* = FP+AP; Generic Security Target
  - *Security Target*



CC Requirements (Classes)

- **Functional**
  - Communication
  - Cryptographic Support
  - Identification&Authentication
  - Security Management
  - Privacy
  - Protection of TSF
  - Resource Utilization
  - Security Audit
  - TOE Access
  - Trusted Path/Channels
  - User Data Protection
- **Assurance**
  - Configuration Management
  - Delivery & Operation
  - Development
  - Guidance Documents
  - Tests
  - Vulnerability assessment
  - Life Cycle Support
  - PP Evaluation
  - ST Evaluation

Tracing of requirements



Where to find Common Criteria

- Common Criteria v. 2.1 = IS 15408:1999
- Common Criteria v. 2.3 contains a number of Interpretations and is a complete version of the IS 15408:2005 currently under publication by ISO/IEC
- Both Downloadable for free from

www.commoncriteriaportal.org

Common Criteria

ICCC

Maintenance of IS 15408

- Large Document; increasing mass of experience
- Re-definition of EALs?
- CCDB/CCIMB support
- SC 27 is closely following CCDB developments targeting CC and CEM v 3.0 (2006)

Protection Profile Registration Procedures

IS 15292

Editor: Mike Nash

Common Criteria

ICCC

Highlights of 15292

- Objectives:
  - Single, Internationally Recognised, Protection Profile Registry promoting the use and availability of Protection Profiles and Packages
  - Compatible with IS 15408 (Common Criteria)
  - Registrar Appointed by ISO and IEC
  - Suitable for Legal and other Mandatory References
- Structure:
  - Formalised in an International Standard
  - Open to All to Submit Entries
  - Registry Entry Details Available to All via the Web at No Charge
  - Public Procedures for Defect Notification, Appeals etc.
- IS 15292 was Reconfirmed in 2004
- Revision necessary to align with CC v.3

Facilities

- Both Packages and Profiles Accepted on Register
- Incomplete Entries Can be Registered During Development
- Sponsorship of Entries Can Be Transferred
- Problems can be Notified and Recorded
- Regular, Three-Yearly Review of Status of All Entries
- France (AFNOR) has established a web based ISO Registry
  - **http://comelec.afnor.fr/iso/profile**

A Framework for IT Security Assurance (FRITSA)

[TR] 15443

Editors:
Aaron Cohen
Hans Daniel
John Hopkinson

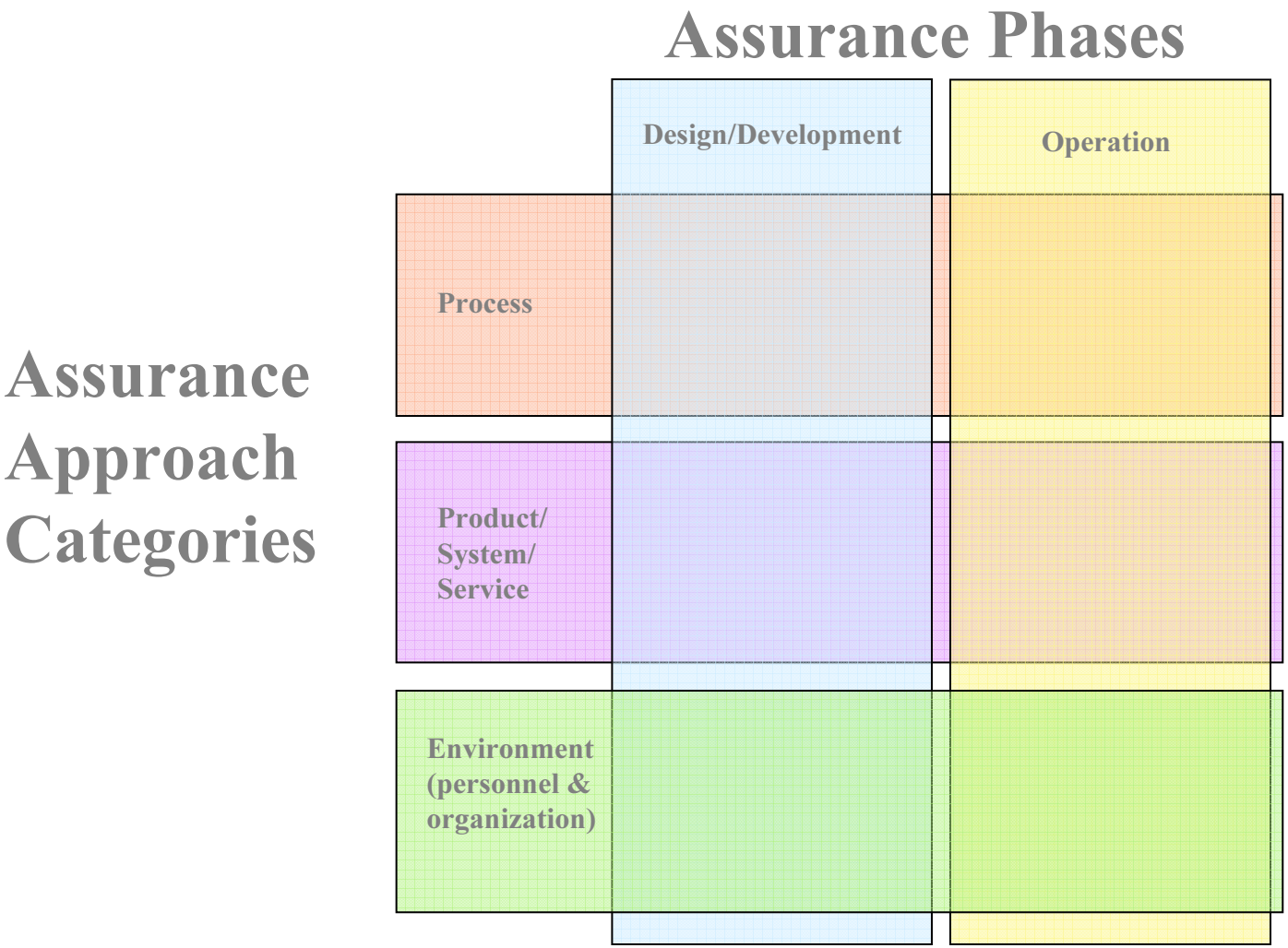
Common Criteria

ICCC

Introduction

- Highlights
  - Type III Technical Report (TR)
    Parts 1 and 2 published; part 3 under development
  - Categorize assurance approaches
  - Provide common point of reference
  - Facilitate combining assurance approaches
- Why Is ISO In The Security Assurance Game
  - Common Criteria as Approach and Framework
  - Several ISO and other assurance methods exist
  - Different assurance approaches exist
  - Assurance still not well understood
  - Potential for combined assurance approach

Assurance Approach vs Assurance Phase



Guide on the production of Protection Profiles and Security Targets

TR 15446

Editor: Mike Nash

Common Criteria

ICCC

PP/ST Guide

- **Technical Report Type III**
- **Available at no cost at**

  http://isotc.iso.org/livelink/livelink/fetch/2000/2489/lttf_Home/ITTF.htm
  (select “freely available standards” and page through list)

- **Guidance on how to produce PPs and STs**
- **Discussion on composition (PPs, STs, Component TOEs)**
- **Considerable interest in this document already during its development**
- **Based on IS 15408:1999**
- **Revision initiated to update to CC v.3**

Common Criteria

ICCC

Methodology for IT Security Evaluation

IS 18045:2005 (to be published)

Editor: Miguel Bañón

Common Criteria

ICCC

Purpose of 18045

- A companion document to the IS 15408, Common Criteria for Information Technology Security Evaluation.
- Will describe the minimum actions to be performed by an evaluator using the criteria and evaluation evidence defined in IS 15408.

History of 18045

- Project started in 2001
- CCDB contribution (CEM)
- Important document supporting Evaluators
- Essential for Mutual Recognition
- Aligned with 15408:2005 (CC v. 2.3)
- Early revision planned for update to CEM v.3 aligned with CC v.3

Security Requirements for Cryptographic Modules

FCD 19790

Editor: Randall Easter

Co-editors: Mike Chawrun, Jean-Pierre Quemard

Common Criteria

ICCC

Highlights of 19790

- A *cryptographic module* is a set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
- Will specify the technical requirements for cryptographic modules used to protect sensitive information in computer and telecommunication systems (including voice systems) in *four increasing, qualitative levels of security*.
  - The levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed.
- The security requirements cover areas related to the secure design and implementation of a cryptographic module.

Contents

- Cryptographic module security levels
- Functional security objectives
- Security requirements
- Cryptographic module specification
- Cryptographic module ports and interfaces
- Roles, services, and authentication
- Finite state model
- Physical security
- Operational environment
- Cryptographic key management
- Self-tests
- Design assurance
- Mitigation of other attacks

Important base document: FIPS 140-2

Important referenced Work: FDIS 18031 Random Bit Generation

- Annex A (normative) Documentation requirements
- Annex B (normative) Cryptographic module security policy
- Annex C (informative) Approved security functions
- Annex D (informative) Approved key establishment methods
- Annex E (informative) Recommended software development practices
- Annex F (informative) Examples of mitigation of other attacks

Security Assessment of Operational Systems

DTR 19791

Editor: Haruki Tabuchi

Common Criteria

ICCC

Background

- This work aims to define an approach to the assessment of the security of a specific composite IT system
- Operational, composite systems typically:
  - are under the *control of a single entity*, the system owner
  - are built against *specific needs*, for a specific type of operation
  - contain a *large number of components*
  - one or more components have a large number of possible *configuration alternatives*
  - enable the system owner to *balance technical* (and specifically IT) *and non-technical* security measures
  - *change frequently*; either in technical set-up and/or in operational requirements (e.g. new threats)
  - contain multiple components with *different degrees and types of assurance*

Justification

- System owners may have specific *time and cost restrictions* for deploying new IT systems.
  - Thus the processes involved when doing the technical part of the approval to operate (sometimes called site certification as part of a system accreditation) need to be *adaptable* to actual needs.
- When composing a system there is a need to describe *interfaces and dependencies* between components and between components and the [technical] system's environment (e.g. users, external systems).
  - The *trust relations* between those components need to be defined as well as the security requirements on the interface (communication) links between them.
- The value of using *evaluated* components and its contribution to the overall system-wide risk assessment should be expressed.

A Framework for Security Evaluation of Biometric Technology

[IS] WD 17972

Editor: Nils Tekampe

Co-editors: Eric Saliba, Masahiro Mimura

Common Criteria

ICCC

Purpose of 19792

- Biometric systems including their techniques and algorithms:
  - belong to a new and growing area of technology which allows the identification and authentication of human beings
- This requires evaluation and testing against extensive security measures for achieving the appropriate security
- The project is intended to provide the appropriate criteria and measurements for both evaluating and security testing of biometric systems
- A *strong liaison* with JTC1 SC 37 and SC 17 is established
- Internal Study Group on Biometric Security Standardization initiated

Systems Security Engineering - Capability Maturity Model (SSE-CMM)

IS 21827:2002

Editor: John Hopkinson

Common Criteria

ICCC

Goals of SSE-CMM

- To advance security engineering as a defined and measurable discipline
- Describes the characteristics of an organization's security engineering process

The SSE-CMM model and methods developed to enable

- Focused investments in security engineering tools, training, process definition, management practices
- Focuses on the maturity of an engineering group's security practices and processes
- Defining capability levels and associated programmatic risks

Scope & Use of SSE-CMM

- The scope of the SSE-CMM
  - Security engineering activities that include the complete life cycle
  - Includes concept definition, requirements analysis, design, development, integration, installation, operations, maintenance, and decommissioning.
- The SSE-CMM is intended to be used as
  - Tool to evaluate security engineering practices and define improvements to them
  - Basis for security engineering evaluation organizations (e.g., system certifiers and product evaluators) to establish organizational *capability-based* confidences (as an ingredient to system or product security assurance)
  - Standard mechanism for customers to evaluate a provider's security engineering capability
- Revision initiated 2005

SC 27 Liaisons

- Other JTC 1 SCs
  - SC 17 - Smart Cards and trade documents
  - SC 25 - Home electronic
  - SC 37 – Biometrics systems
- ISO TCs
  - TC 68 - Banking & Financial Services
  - TC 154 - E-commerce
  - TC 215 - Healthcare
- Other SDOs
  - ITU-T - International Telegraph & Telecomm. Union
- Others
  - IETF - Internet Engineering Task Force
  - CCDB – Common Criteria Development Board
  - ISSEA – International Systems Security Engineering Association

Final words

I draw the conclusion that there are two ways to construct a system:

One way is to make it so simple that there are obviously no deficiencies.

The other way is to make it so complicated that there are no obvious deficiencies.

C. Hoare, Turing Award Lecture, CACM February 1981