ISO/IEC JTC 1 SC 27 WG 3

Security Evaluation, Testing and Specification

Physical security attacks, mitigation techniques and security requirements

WG3 Mission

Security Evaluation, Testing and Specification

The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. The following aspects may be distinguished:

a) security evaluation criteria;

b) methodology for application of the criteria;

c) security functional and assurance specification of IT systems, components and products;

d) testing methodology for determination of security functional and assurance conformance;

e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

Buzzwords

CIBERSECURITY

Defense in depth

INFORMATION SECURITY MANAGEMENT SYSTEMS

STANDARDS

Risk analysis

Conformance Testing

Commercial Off-The-Shelf

Computer Emergency Readiness Team

Product Security Evaluation

Mutual Recognition Agreements

Idealism

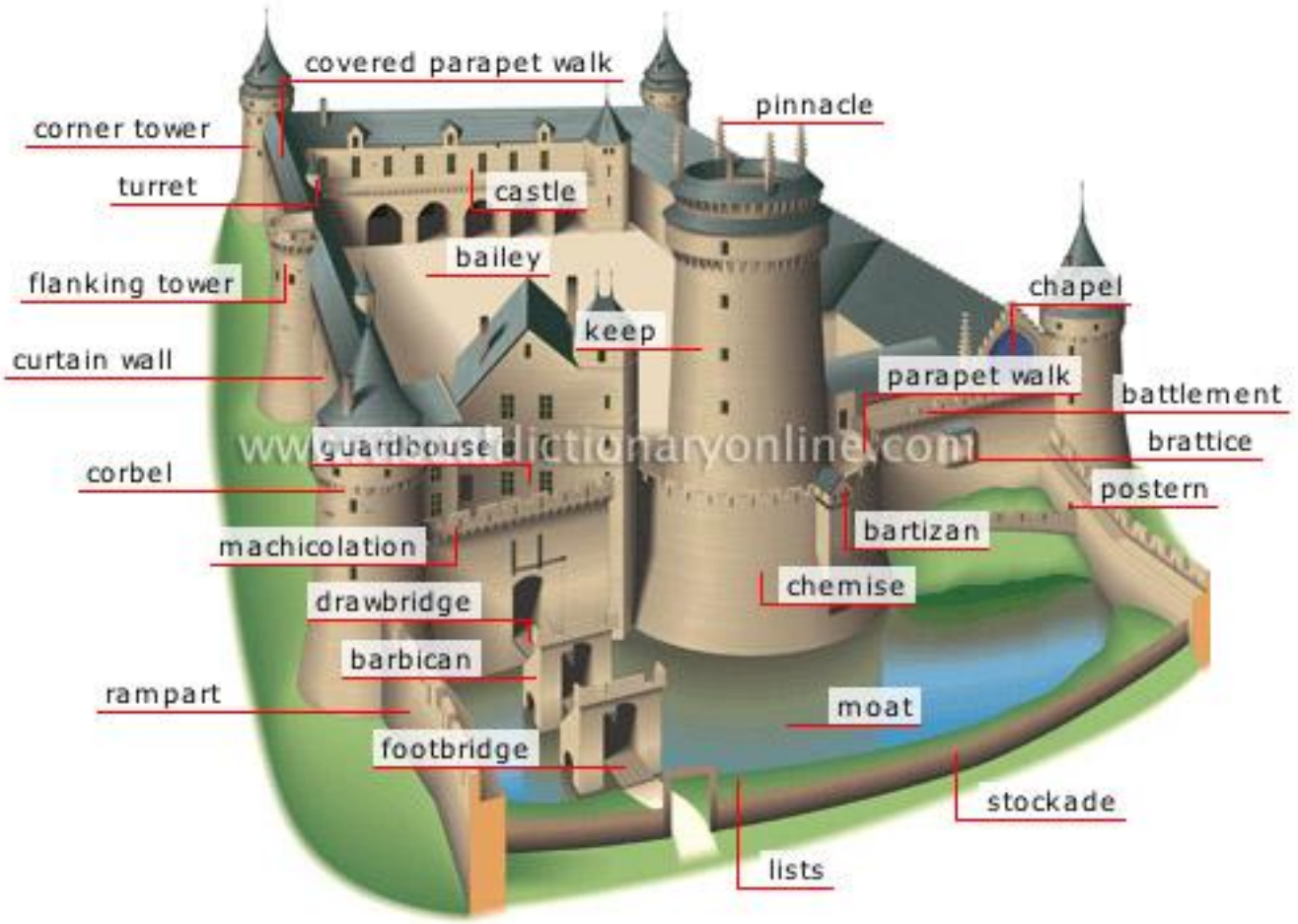
“Idealism is the philosophical theory which maintains that experience is ultimately based on mental activity. In the philosophy of perception, idealism is contrasted with realism, in which the external world is said to have an apparent absolute existence. Epistemological idealists (such as Kant) claim that the only things which can be directly known for certain are just ideas (abstraction). In literature, idealism refers to the thoughts or the ideas of the writer.”
(source wikipedia.org)

Applied to IT security, it mostly explains the subject matters of risk management, CERTs, ISMS, etc.

Pessimism

“Pessimism, from the Latin pessimus (worst), is a state of mind in which one perceives life negatively. Value judgments may vary dramatically between individuals, even when judgments of fact are undisputed. The most common example of this phenomenon is the "Is the glass half empty or half full?" situation. The degree in which situations like these are evaluated as something good or something bad can be described in terms of one's optimism or pessimism respectively. Throughout history, the pessimistic disposition has had effects on all major areas of thinking.” *(source wikipedia.org)*

Applied to IT security, it mostly explains the subject matters of evaluation and vulnerability analysis.


covered parapet walk
corner tower
turret
flanking tower
curtain wall
corbel
machicolation
drawbridge
barbican
rampart
footbridge
castle
bailey
keep
guardhouse
pinnacle
chapel
parapet walk
battlement
brattice
postern
bartizan
chemise
moat
stockade
lists
www.dictionaryonline.com

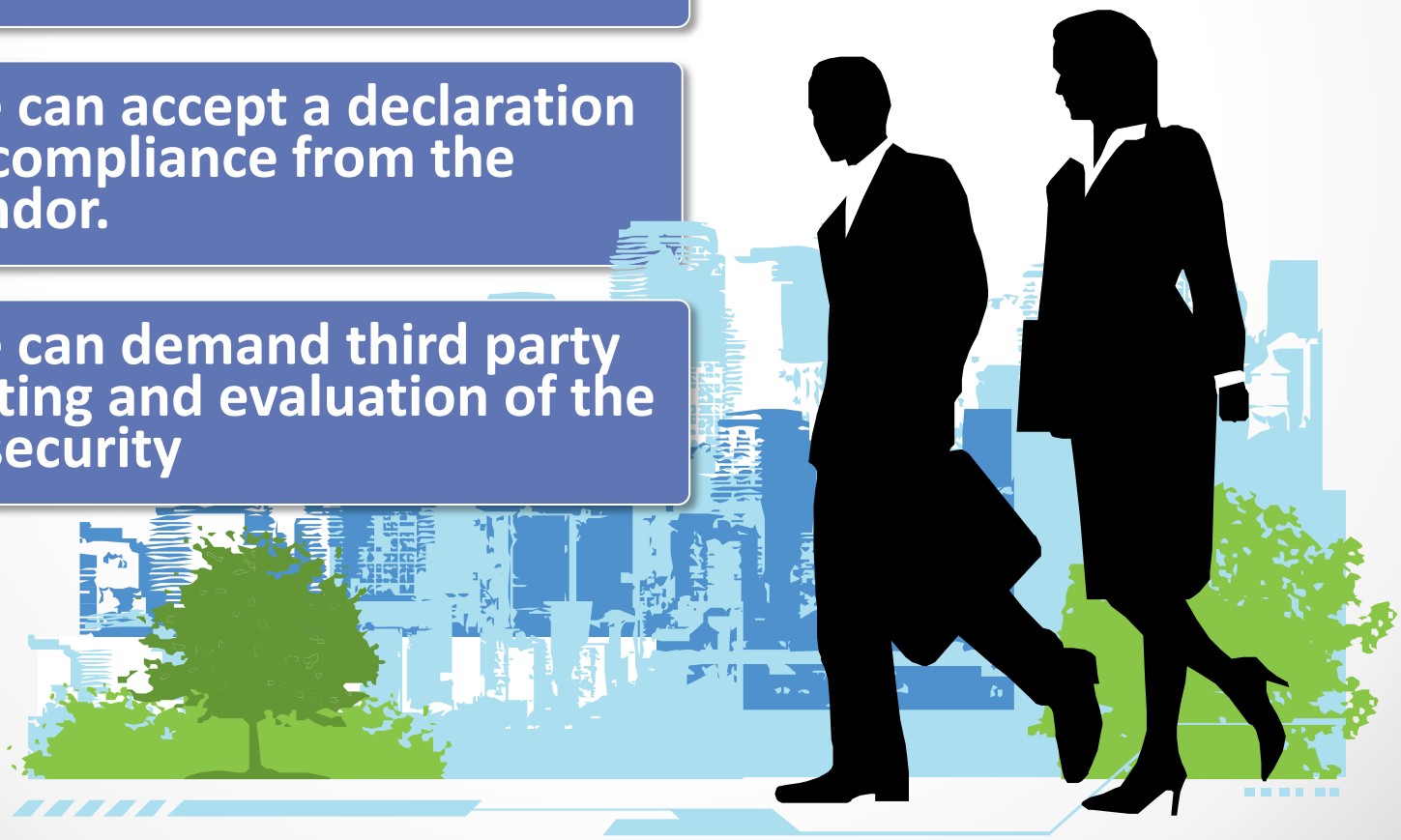
Issues that also need to be addressed when building a castle:

- GROUND QUALITY
- MATERIAL QUALITY AND HARDENING
- SUPPLIER TRUST
- VULNERABILITIES IN SPECIFICATION
- VULNERABILITIES IN CONSTRUCTION
- VULNERABILITIES IN OPERATION


Anonymous uploader

Regarding trust in technology:

- We can happily ignore these issues;
- We can accept a declaration of compliance from the vendor.
- We can demand third party testing and evaluation of the IT security



We are talking about:

Worms/Trojans

Code Injection

Drive-by exploits

Exploit Kits

Botnets

Denial of Service

ENISA Threat Landscape, Mid-year 2013

Reality check of 2012's assessment and more - September 2013


The Back Door Cafe
www.thebdcafe.com
The Back Door CAFE
HOURS
Homemade. Hometown Goodness
Incredible Edible Desserts
Specialty Catering
THE BACK DOOR CAFE 249-4310
ENTRANCE

We are talking about:

Security Functional requirements

Security Assurance requirements

Derived Tests

Vunerability Analysis

Technical competence

Third party assurance

Third Party Assurance

ISO/IEC JTC 1/SC 27 add an additional and critical international dimension.

International cross stakeholders requirements definition

Can we afford not to have secure IT?

Can we afford not to demand it by default?

WG 3 provides standards to ensure security of IT bottom-up, providing building blocks for the final security of systems, processes and services.

We turn sand castles into secure sites.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 15408	Evaluation criteria for IT security	3rd Ed	ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
ISO/IEC TR 15443	A framework for IT security assurance	2nd Ed.	ISO/IEC TR 15443 guides the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel.
ISO/IEC TR 15446	Guide for the production of Protection Profiles and Security Targets	2nd Ed.	ISO/IEC TR15446:2009 provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408.
ISO/IEC 17825	Testing methods for the mitigation of non-invasive attack classes against cryptographic modules	1st CD	This International Standard specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for Security Levels 3 and 4.
ISO/IEC 18045	Methodology for IT security evaluation	2nd Ed.	ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

WG3 Standards

Standard	Title	Status	Abstract
ISO/IEC 18367	Cryptographic algorithms and security mechanisms conformance testing	3rd WD	The purpose of this standard is to address conformance testing methods of cryptographic algorithms and security mechanisms implemented in a cryptographic module.
ISO/IEC 19249	Catalogue of Architectural and Design Principles for Secure Products, Systems, and Applications	1st WD	This Technical Report (TR) provides a catalogue with guidelines for architectural and design principles for the development of secure products, systems, and applications. Applying those principles should result in more secure products, systems, and applications.
ISO/IEC 19790	Security requirements for cryptographic modules	2nd Ed	ISO/IEC 19790:2012 specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems
ISO/IEC TR 19791	Security assessment of operational systems	1st WD Under review	ISO/IEC TR 19791:2010 provides guidance and criteria for the security evaluation of operational systems.
ISO/IEC 19792	Security evaluation of biometrics	1st Ed	ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system.
ISO/IEC TR 20004	Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045	1st WD Under review Subdivision requested	ISO/IEC TR 20004:2012 refines the AVA_VAN assurance family activities defined in ISO/IEC 18045:2008 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation.

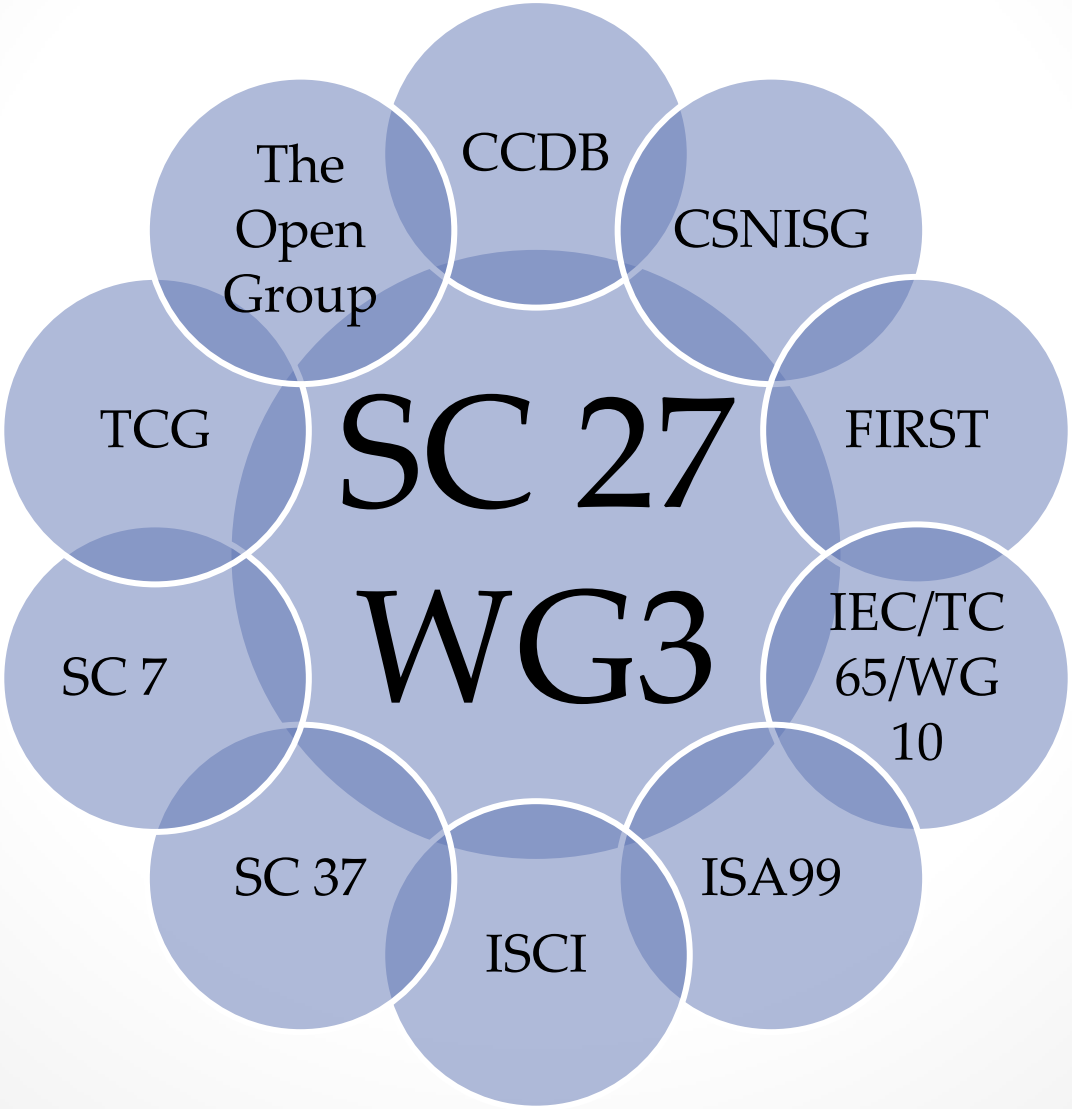
WG3 Standards

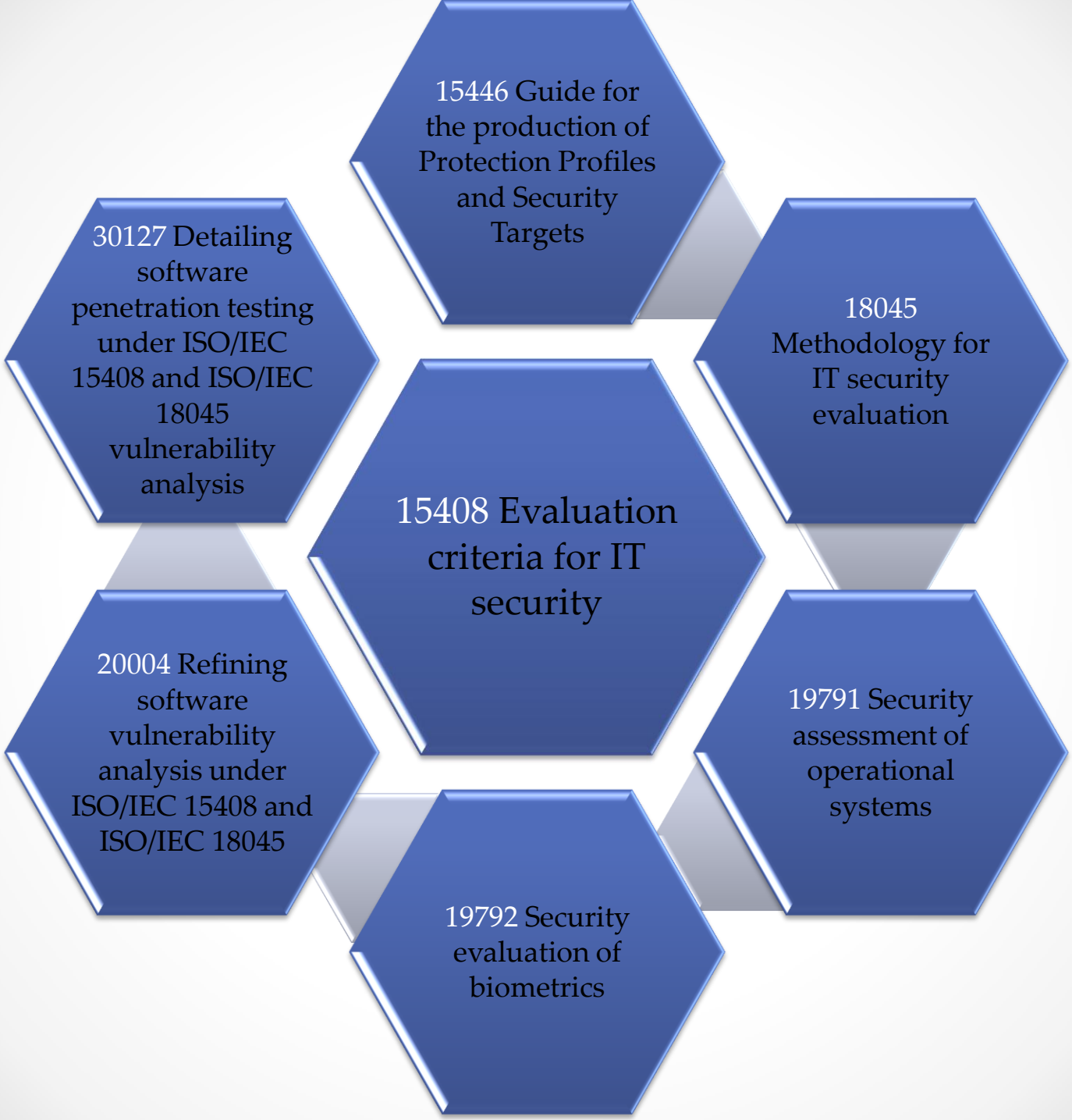
Standard	Title	Status	Abstract
ISO/IEC 21827	Systems Security Engineering -- Capability Maturity Model® (SSE-CMM®)	2nd Ed	ISO/IEC 21827:2008 specifies the Systems Security Engineering - Capability Maturity Model® (SSE-CMM®), which describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.
ISO/IEC 24759	Test requirements for cryptographic modules	DIS In publication	ISO/IEC 24759:2008 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006.
ISO/IEC 29128	Verification of cryptographic protocols	1st Ed	ISO/IEC 29128:2011 establishes a technical base for the security proof of the specification of cryptographic protocols.
ISO/IEC 29147	Vulnerability Disclosure	FDIS ballot	This International Standard gives guidelines for the disclosure of potential vulnerabilities in products and online services.
ISO/IEC TR 30104	Physical security attacks, mitigation techniques and security requirements	3rd PDTS	This Technical Report addresses how security assurance can be stated for products where the risk of the security environment requires the support of physical protection mechanisms.
ISO/IEC 30111	Vulnerability handling processes	DIS In publication	This International Standard describes processes for vendors to handle reports of potential vulnerabilities in products and online services.
ISO/IEC 30127	Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis	Cancellation requested	This Technical Report provides guidelines for the planning, development and execution of penetration testing under ISO/IEC 15408 and ISO/IEC 18045 Vulnerability Assessment for software targets of evaluation.

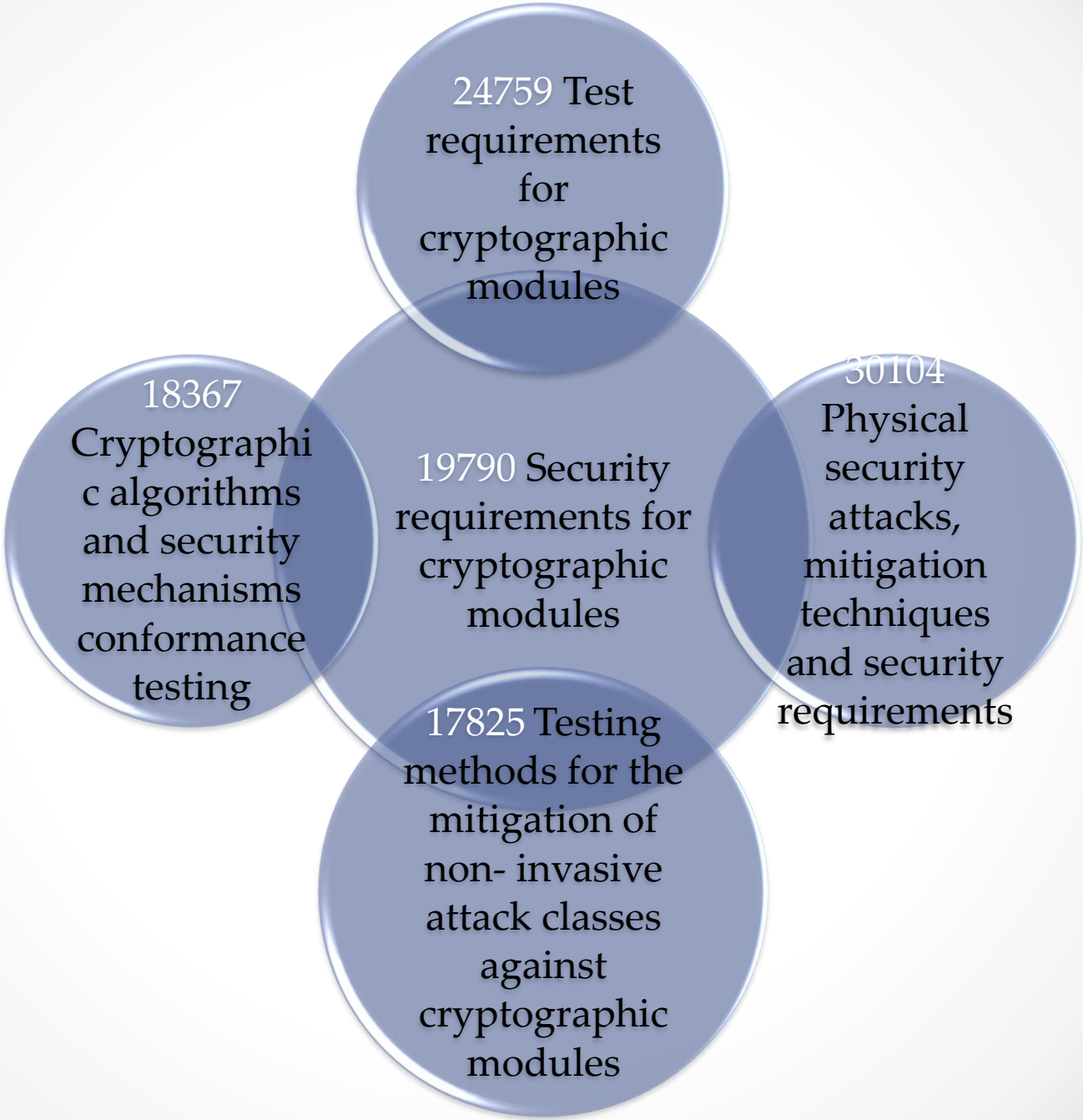
WG3 Standards

Study Periods	New Work Items
Security evaluation of anti spoofing techniques for biometrics	Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
High Assurance	
Competence requirements for security evaluators, testers, and validators	
Operational test guideline of cryptographic module in environment	

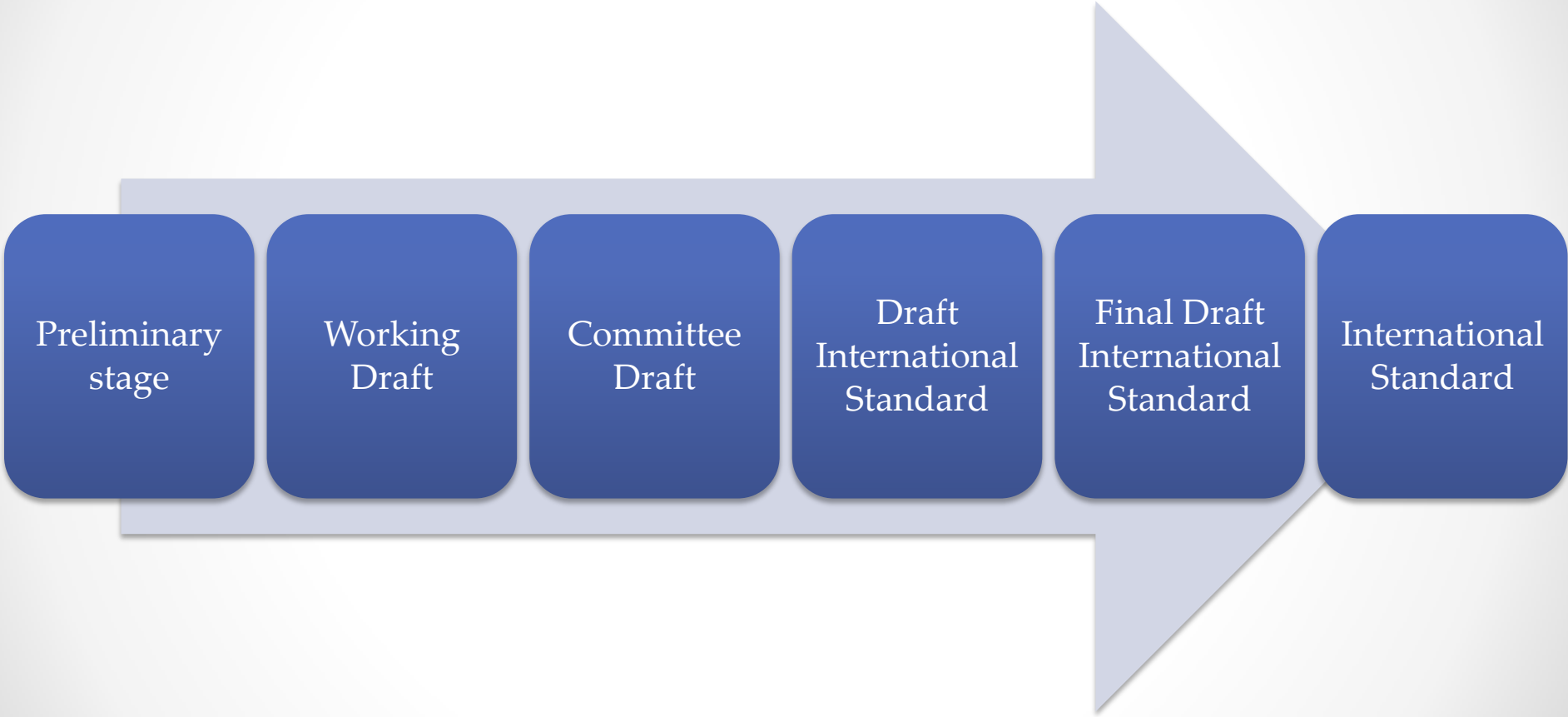
WG3 Liaisons




15446 Guide for the production of Protection Profiles and Security Targets
30127 Detailing software penetration testing under ISO/IEC 15408 and ISO/IEC 18045 vulnerability analysis
18045 Methodology for IT security evaluation
15408 Evaluation criteria for IT security
20004 Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
19791 Security assessment of operational systems
19792 Security evaluation of biometrics


24759 Test requirements for cryptographic modules
18367 Cryptographic algorithms and security mechanisms conformance testing
19790 Security requirements for cryptographic modules
30104 Physical security attacks, mitigation techniques and security requirements
17825 Testing methods for the mitigation of non- invasive attack classes against cryptographic modules

Stages of a project



ISO/IEC 2nd PDTS 30104
Physical security attacks, mitigation techniques and security requirements

WD	PDTS	DTS	FDIS	TS
11-01	12-04	13-04		13-10

Physical security mechanisms are employed by cryptographic modules where the protection of the modules sensitive security parameters is desired.

This Technical Report addresses how security assurance can be stated for products where the risk of the security environment requires the support of such mechanisms.

This Technical Report addresses the following topics:

- a survey of physical security attacks directed against different types of hardware embodiments including a description of known physical attacks, ranging from simple attacks that require little skill or resource, to complex attacks that require trained, technical people and considerable resources;

- guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks; and

- guidance on the evaluation or testing of hardware tamper protection mechanisms and references to current standards and test programs that address hardware tamper evaluation and testing.

The information in this Technical Report is useful for product developers in the designing hardware implementing anti-tampering mechanisms and the testing or evaluation of the final product.

The intent is to match protection methods with the attack methods in terms of complexity, cost and risk to the assets being protected. In this way cost effective protection can be produced across a wide range of systems and needs.

- Physical security
  - Physical security invasive mechanisms
  - Tamper proof
  - Tamper resistant
  - Tamper responding
  - Tamper evident
  - Some additional physical security considerations
  - Size and weight
  - Mixed and Layered Systems

Physical security invasive attacks and defenses

- Attacks
- Internal Probe attacks
- Machining methods
- Shaped charge technology
- Energy attacks
- Environmental
- Defenses
- Tamper resistant
- Tamper evident
- Tamper responding sensor technology
- Tamper responding
- Opacity

Physical security non-invasive mechanisms

- Mixed and Layered Systems

Physical security non-invasive attacks and defenses

- Attacks
- External Probe attacks
- External EME attacks
- Timing analysis
- Defenses

Development, delivery and operation considerations

- Development
- Functional test and debug
- Security testing
- Environmental testing
- Factory installed keys
- Delivery
- Documentation
- Packaging
- Delivery verification
- Operation
- Implementation feedback
- Feedback during attack

More information at

http://isotc.iso.org/livelink/livelink/open/jtc1sc27

Thanks!

Miguel Bañón
Epoche & Espri
mbp@epoche.es