



# *International Standardisation*

## *SC 27/WG 3 – Security Evaluation*

Mike Nash  
Gamma Secure Systems Limited  
Secretary, SC 27 Working Group 3

# Working Group 3 - Evaluation

---

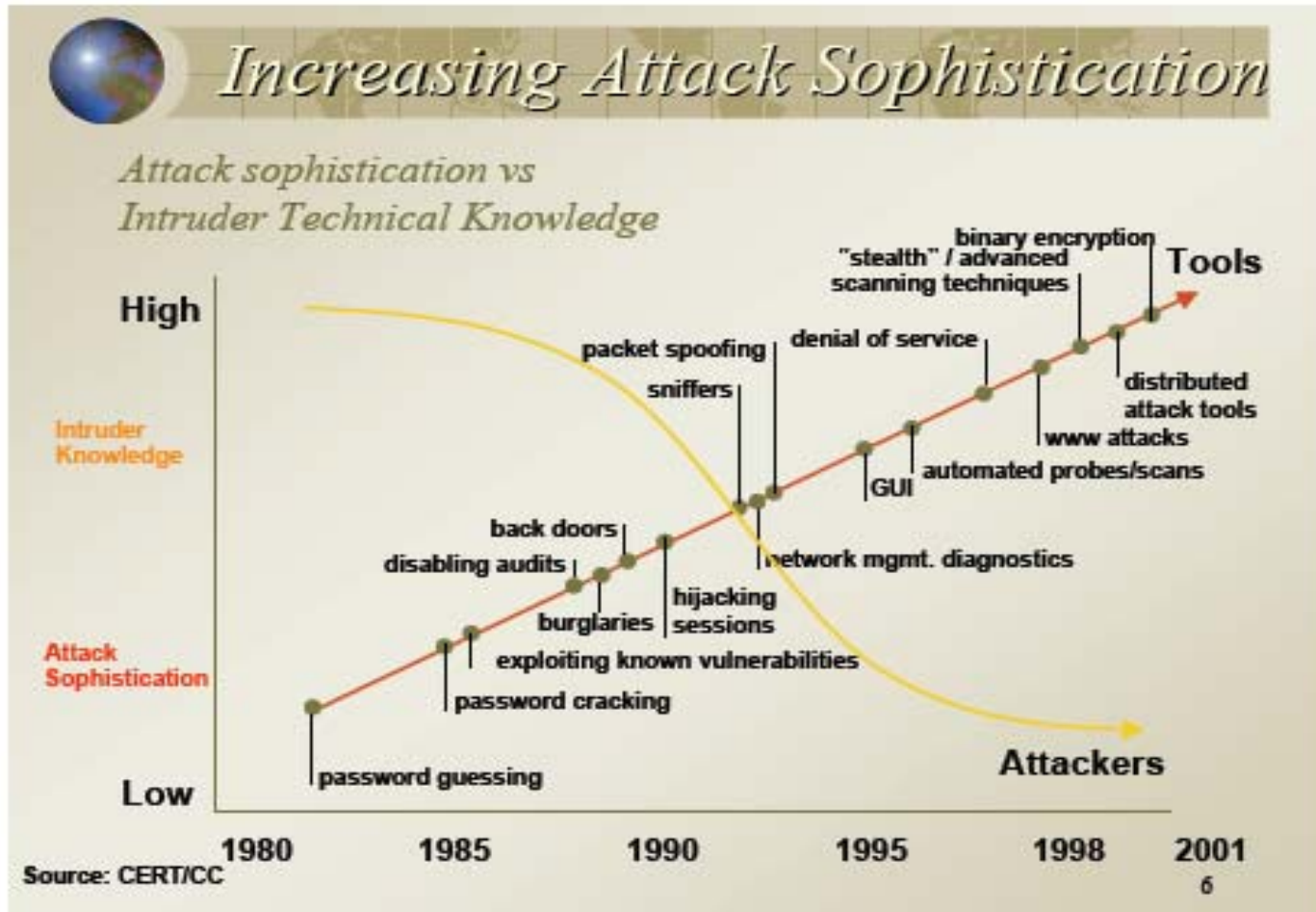
- WG 3 deals with specifications, methodologies and techniques for assessing (evaluating) IT systems and products
- Main thrust is ISO/IEC 15408, Security Evaluation Criteria
  - ➔ *ISO/IEC 15408 is identical to the "Common Criteria" and shares the same XML specification*
- WG 3 also deals with other forms of security evaluation
  - ➔ *e.g. FIPS 140-2, SSE CMM*

# *The Problem...*

---

- Three dimensions of information security
  - ➔ *Management*
  - ➔ *Technology*
  - ➔ *Operations*
  
- How do we measure security?
  - ➔ *How do we measure our trust in the management, the technology, etc.?*
  
- In particular, to what extent can we place trust in technology?

# The threat is not static



# Why security evaluation?

Isolation of untrusted components or complete systems?



Hard to achieve;  
Needs “secure” OS  
Limited external communication \*

\* Increasingly less viable

Extensive operational control?



Supervision, Intrusion Detection  
Much more auditing  
More screening (of personnel)  
Rapid remediation of discovered flaws

Staff intensive

Scrutiny of design and implementation of trusted [sub]systems?



Security Evaluation

Cost? Effectiveness?

# Evaluation Fundamentals

---

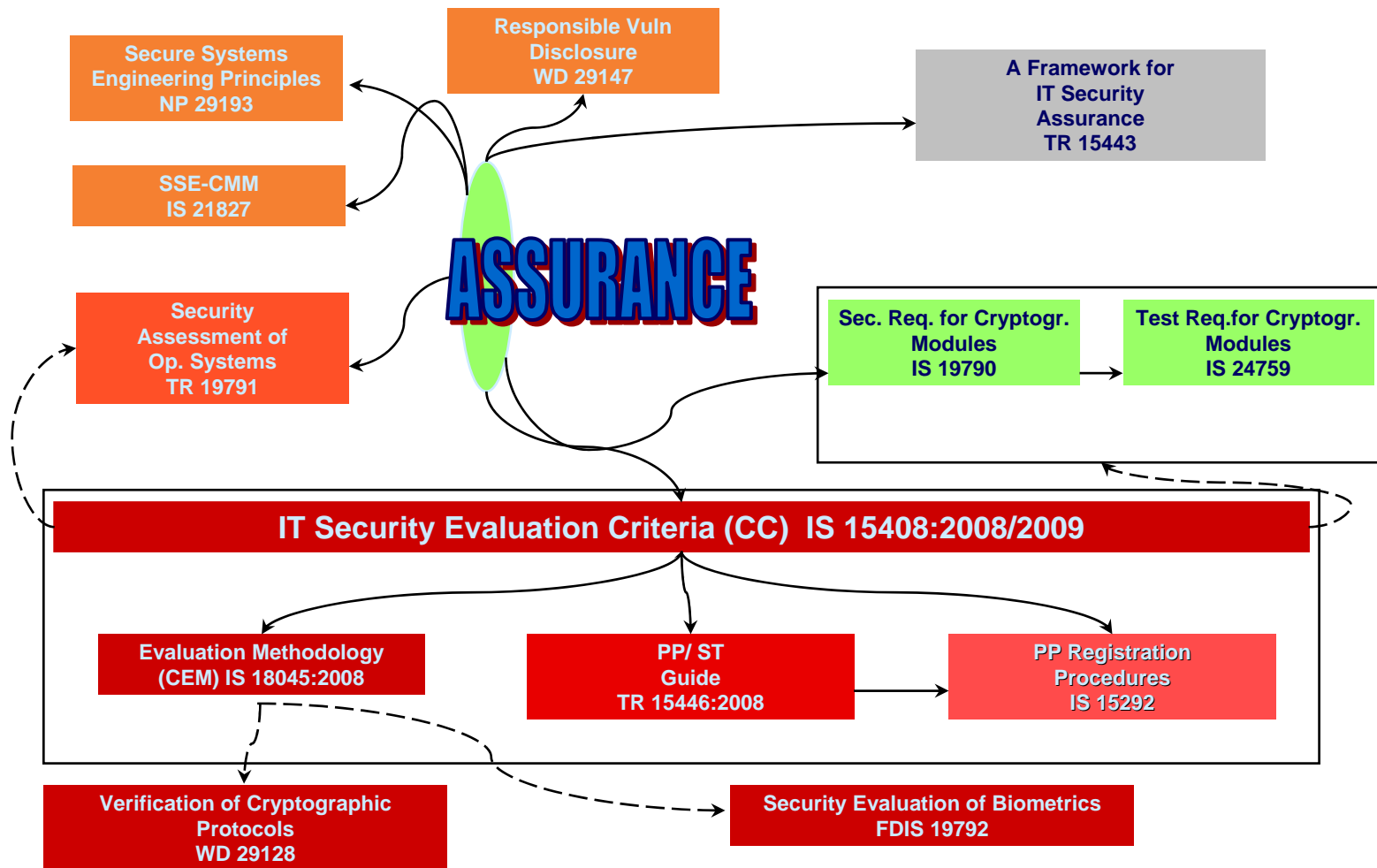
- The objective is to reduce the risk that exploitable vulnerabilities in technology exist
  - ➔ *But there is always a residual risk - 100 % security does not exist*
- More investigation of the technology is better
  - ➔ *Challenge: Find and use effective (optimal) methods, according to given costs, to find as many flaws as possible*
- Assume qualified adversaries may make same kinds of analyses, planning an attack
  - ➔ *Make their task more difficult/expensive; reduce our risk.*

# *WG 3 Projects*

---

- 15408 Evaluation criteria for IT Security
- 18045 Methodology for IT security evaluation
- 15292 Protection Profile registration procedures
- 15443 A framework for IT security assurance (FRITSA)
- 15446 Guide for the production of Protection Profiles and Security Targets (PPST Guide)
- 19790 Security requirements for cryptographic modules
- 19791 Security assessment of operational systems
- 19792 Security evaluation of biometrics
- 21827 Systems security engineering - Capability maturity model
- 24759 Test requirements for cryptographic modules
- 29128 Verification of cryptographic protocols
- 29147 Responsible Vulnerability Disclosure
- 29193 Secure System Engineering Principles
- Study Period on Tamper Protection

# Or to put it another way...





---

# *Information Technology Security Evaluation Criteria*

ISO/IEC 15408

Editors: Fiona Pattinson (US), Mike Nash (UK),  
Miguel Bañón (Spain)

# 15408 - Evaluation Criteria

---

- Long established and widely used standard
- Identical technically to the Common Criteria (CC)
- CC Project and WG 3 work closely in developing the criteria
  - ➔ *CC Project has greater resources, WG 3 has greater participation*
- CC Project usually leads work
  - ➔ *But not current revision of Part 1*



---

# *Common Evaluation Methodology*

ISO/IEC 18045

Editor: Miguel Bañón (Spain)

# 18045



- 
- Supporting standard to 15408/CC
  - Methodology for performing evaluations
  - Identical in technical content to CC Project CEM



---

# *Protection Profile Registration Procedures*

IS 15292

Editor: Mike Nash (UK)

# *International PP Register*

---

- Products are usually evaluated against standard specifications (Protection Profiles)
- 15292 defines an International Register of PP Specifications
- Official ISO Register, but to be hosted by the Common Criteria Portal



---

# *A Framework for IT Security Assurance*

TR 15443

Editors: Aaron Cohen (Canada), Hans Daniel  
(Germany), John Hopkinson (Canada)

# *Assurance Framework*

---

- Technical Report in three parts
- Categorises assurance approaches
- Provides common point of reference
- Theoretical underpinning of WG 3 work



---

# *Guide for the Production of Protection Profiles and Security Targets*

TR 15446

Editors: Mike Nash (UK), Helmut Kurth (US)

# *PP/ST Guide*

---

- Technical Report
- Provides practical help in preparing for evaluation
- Written by experts in preparing products for evaluation
- No Common Criteria equivalent



---

# *Security Requirements for Cryptographic Modules*

IS 19790

Editor: Randall Easter (US)

# *Crypto Modules Standard*

---

- International version of FIPS 140-2
- Editor works for NIST
- Co-editors from France and Canada
- Permits international algorithms
- New version being developed in parallel with FIPS 140-3



# *Test Requirements for Cryptographic Modules*

IS 24759

Editor: Randall Easter (US)

# *Module Test Standard*

---

- Complements 19790/FIPS 140 by providing test requirements
- Based on NIST derived test requirements
- Co-editors from France and Germany
- No official FIPS equivalent



---

# *Security Assessment of Operational Systems*

TR 19791

Editors: Haruki Tabuchi (Japan), Mike Nash (UK)

- Extends CC/15408 to systems as well as products
- Japanese initiative
- Being updated to CC V3/15408:2008



---

# *Security Evaluation of Biometrics*

FDIS 19792

Editor: Nils Tekampe (Germany)

# *Biometric Device Evaluation*

---

- Addresses specialist problems of evaluating biometric devices
  - ➔ *Repeatability, false acceptances, subterfuge, etc.*
- Close liaison with Biometrics Standards Committee
- Difficult technical area
  - ➔ *Co-editors from France and Japan*
- Undergoing final ballot



---

# *Systems Security Engineering – Capability Maturity Model*

IS 21827

Editor: John Hopkinson (Canada)

# *SSE-CMM*

---

- Applies capability maturity concepts to security engineering
- Direct equivalent of ISSEA model



---

# *Verification of Cryptographic Protocols*

WD 29128

Editors: Akira Otsuka, Shin'ichiro Matsuo,  
Kunihiko Miyazaki (Japan)

# *Protocol Verification*

---

- Just because key materials are correctly generated, it doesn't mean that they are distributed correctly and securely
  - ➔ *Correct implementation of protocols needs to be verified*
- Several new types of attack found recently by WG 2
- Advancing to Committee Draft Level



---

# *Responsible vulnerability disclosure*

WD 29147

Editor: Faud Khan (Canada)

- 
- If during evaluation you find a serious flaw in a product, you have to handle the knowledge responsibly
  - Divergent views
    - ➔ *Reveal or conceal*
  - Still at Working Draft level



---

# *Secure System Engineering Principles*

NP 29193

Editors: Fiona Pattinson (US), Anne Coat (France)

# *Secure Systems Engineering*

---



- CC/15408 evaluation is heavily dependent on good design and good design documentation
- New Project in WG 3
- Precise scope and objectives discussed in Beijing, first draft to be ready for next meeting



---

# *Tamper Protection Requirements and Evaluation*

Study Period

Rapporteur: Miguel Bañón (Spain)

# *Tamper Protection*

---

- Evaluation of physical protection of secure software and hardware
- Physical protection is usually assumed in CC/15408 evaluation
- Currently at study stage, seeking expressions of interest and/or contributions

# *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 Lecture, CACM February 1981*



---

*Thank You*

Mike Nash  
Gamma Secure Systems Ltd