Information technology security evaluation – standards, assurance

IA169 – System verification and assurance

Vashek Matyáš

CROCS
Centre for Research on Cryptography and Security

Resources used – this lecture

- *Common Criteria for Information Technology Security Evaluation*, v 3.1, release 5, April 2017
  - http://www.commoncriteriaportal.org/
- *Separation Kernel Protection Profile Revisited: Choices and Rationale*, T.E. Levin et al., 4th Annual Layered Assurance Workshop, 2010
- *Common Criteria Certification in the UK – UK IT security evaluation & certification scheme*, CESG
- *Understanding the Windows EAL4 evaluation*, J.S. Shapiro, IEEE Computer 03/2003
- Security Requirements for Cryptographic Modules, FIPS PUB 140-2
  - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Security threat model

- Two views:
  1) Description of security threats considered when designing a (security) solution/system.
  2) Definition of (all) possible threats to consider.
- Usual security notion:
  - *Assets* to be protected
  - *Vulnerabilities* of assets and relevant systems
  - *Threats* exploiting the vulnerabilities
  - *Countermeasures* (aim to) mitigate the threats

Threat modelling – approaches

- Attacker centric
  - Popular in the research community (following two slides)
- System centric (a.k.a. design/SW centric)
  - Taking over in the past decade or so, e.g. used in the Microsoft Security Development Lifecycle
- Asset centric
  - Business logic

- Defender/owner view getting more prominent

Attacker models – Needham & Schroeder

- attacker can eavesdrop and interfere all communication
  – record/modify/replay/inject messages
- node internal processes are safe
  – secret keys, encryption process, …

- Comms security classics, paper from 1978 – paper Using encryption for authentication in large networks of computers, ACM Communications

Attacker models – Dolev & Yao

- Network = set of abstract machines exchanging messages.
- Message = formal terms. Terms reveal some of the message internal structure to the adversary, but not all.
- Adversary can overhear, intercept, and synthesize any message, is limited by the constraints of the cryptographic methods used.
  - Sometimes put as “the attacker carries the message.”
- Paper “On the security of public key protocols”, IEEE Trans. on Information Theory, 1983

Trusted system/product

- Such one that behaves in a way we expect it to behave
- Can be trusted to only such a functionality that adheres to the relevant security policy
- Trust
  - Belief that (a system…) satisfies given (security) requirements and specifications
  - Chance that (a system…) can breach the (security) policy without leaving any trace of evidence ☺
    - Truly appreciating this caveat is important!

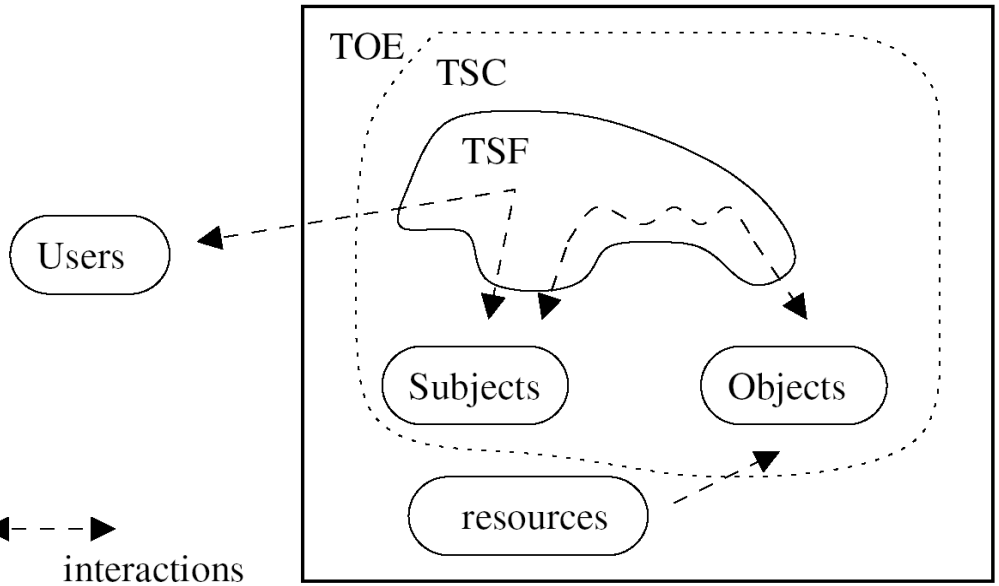
Common Criteria

- Interests of users, manufacturers, evaluators
- *Target of evaluation* (TOE) – what is (to be) evaluated
- *Protection profile (PP)* (smartcards, biometrics, etc.)
  – Catalogued as a self-standing evaluation document
- *Security target* (ST) – theoretical concept/aim
- *Security Functional Requirements* (SFRs) – individual security functions provided by the TOE

- Evaluation of TOE – is the reality corresponding to theory (ST)?

Common Criteria model

- TOE: Target of Evaluation – the evaluated system
- TSF: TOE Security Functions – HW, SW, FW used by the TOE
- TSC: TSF Scope of Control – interactions under the TOE security policy



Study of a particular PP

- PP BSI-PP-0025 – German (BSI) Common Criteria Protection Profile for USB Storage Media
  - Link in the IS
- PP organisation:
  - the TOE description,
  - the TOE security environment,
  - the security objectives,
  - the IT security requirements and
  - the rationale.

PP BSI-PP-0025 – roles in the TOE

- Authorised user (S1)
  - Holds the authentication attribute required to access the TOE protected memory area, in which the confidential data is stored.
  - Can modify the authentication attribute.

PP BSI-PP-0025 – roles in the TOE, cont'd

- Non-authorised user (S2)
  - Wishes to access S1's confidential data in the USB storage medium's memory (examples of confidential data are given in Section 2.5).
  - Does not have the authentication attribute to access the protected data.
  - Can obtain a USB storage medium of the same type. Can try out both logical and physical attacks on this USB storage medium.
  - Can gain possession of the TOE relatively easily since the TOE has a compact form.

PP BSI-PP-0025 – threats (countered)

- T.logZugriff – Assuming that S2 gains possession of the TOE, he/she accesses the confidential data on the TOE. S2 gains logical access by, for example, connecting the TOE to the USB interface of a computer system.
- T.phyZugriff – Assuming that S2 gains possession of the TOE, he/she accesses the TOE's memory by means of a physical attack. Such an attack could take the following form, for example: S2 removes the TOE memory and places it into another USB storage medium which he/she uses for the purpose of logical access to the memory.

PP BSI-PP-0025 – threats, cont'd

- T.AuthÄndern – Assuming that S2 gains possession of the TOE, he/she sets a new authentication attribute, with the result that the data becomes unusable for S1.
- T.Störung – A failure (e.g., power failure or operating system error) stops the TOE operating correctly. As a result, confidential data remains unencrypted or the TOE's file system is damaged.

Common Criteria – two catalogues

- Two catalogues of components for specification of assurance and functionality requirements, with a standard terminology.
- *Functionality* – rules governing access to & use of TOE resources, and thus information and services controlled by the TOE
- *Assurance*
  - grounds for confidence that an entity meets its security objectives (CC v2.3)
  - grounds for confidence that a TOE meets the SFRs (CC v3.1)

Assurance is not robustness

- Assurance
  - grounds for confidence that an entity meets its security objectives (CC v2.3)
  - grounds for confidence that a TOE meets the SFRs (CC v3.1)
- Robustness
  - characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly (US DoD definition)

CC – going for evaluation (in a nutshell)

1. Define the product/system for evaluation
2. Specify its functionality
3. Specify the assurance level claimed
4. See details of evaluation with a certification body
5. Prepare evidence

CC: Functional & Assurance Requirements

Security Functional Requirements (SFRs)

- The core – CC is in a major part a catalogue of security functions
- Same product with different ST => different SFRs
- Correctness of one function can depend on another function

Security Assurance Requirements (SARs)

- Measures taken to assure compliance with the claimed functionality
- Design, development, evaluation/verification
- CC provides a catalogue of SARs

CC functional classes

- FAU: SECURITY AUDIT
- FCO: COMMUNICATION
- FCS: CRYPTOGRAPHIC SUPPORT
- FDP: USER DATA PROTECTION
- FIA: IDENTIFICATION AND AUTHENTICATION
- FMT: SECURITY MANAGEMENT
- FPR: PRIVACY
- FPT: PROTECTION OF THE TSF
- FRU: RESOURCE UTILISATION
- FTA: TOE ACCESS
- FTP: TRUSTED PATH/CHANNELS

CC assurance classes

- APE: PROTECTION PROFILE EVALUATION
- ACE: PROTECTION PROFILE CONFIGURATION EVALUATION
- ASE: SECURITY TARGET EVALUATION
- ADV: DEVELOPMENT
- AGD: GUIDANCE DOCUMENTS
- ALC: LIFE-CYCLE SUPPORT
- ATE: TESTS
- AVA: VULNERABILITY ASSESSMENT
- ACO: COMPOSITION

Assurance through evaluation I

a) analysis and checking of process(es) and procedure(s);
b) checking that process(es) and procedure(s) are being applied;
c) analysis of the correspondence between TOE design representations;
d) analysis of the TOE design representation against the requirements;
e) verification of proofs;

Assurance through evaluation II

f) analysis of guidance documents;

g) analysis of functional tests developed and the results provided;

h) independent functional testing;

i) analysis for vulnerabilities (including flaw hypothesis);

j) penetration testing.

CC assurance paradigms

- *assurance based upon an evaluation* (active investigation)

- measuring the validity of the documentation and of the resulting IT product by expert evaluators with increasing emphasis on scope, depth, and rigour
- CC does not exclude, nor does it comment upon, the relative merits of other means of gaining assurance

CC evaluation assurance scale

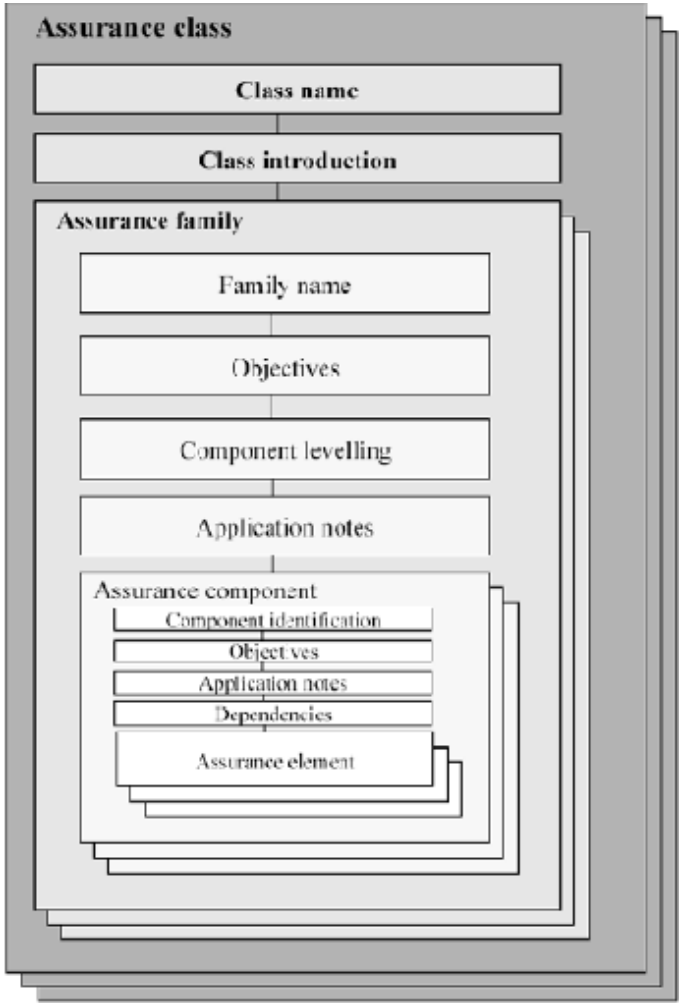
The increasing level of effort is based upon:

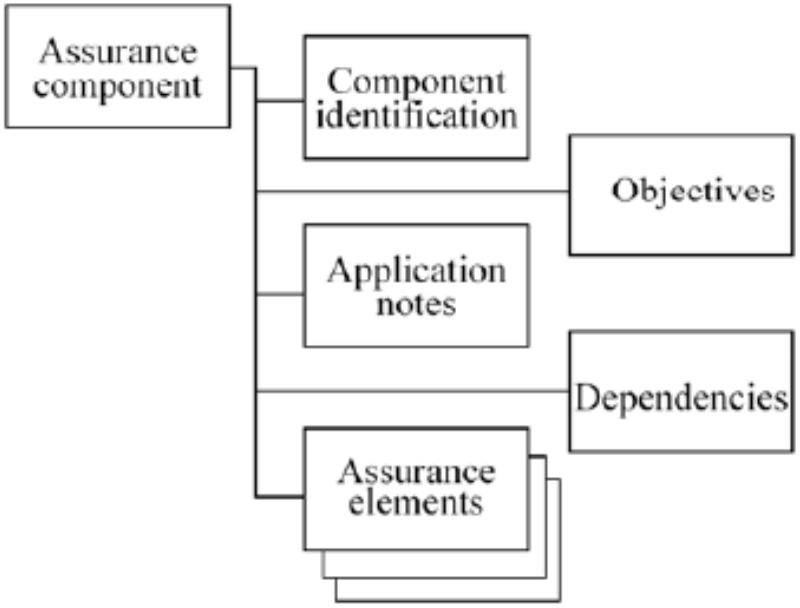
a) *scope* – the effort is greater because a larger portion of the IT product is included;

b) *depth* – the effort is greater because it is deployed to a finer level of design and implementation detail;

c) *rigour* – the effort is greater because it is applied in a more structured, formal manner.

CC – assurance hierarchy & component structure





Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Assurance elements – 3 exclusive classes

1. *Developer action elements*: activities that shall be performed by the developer. Further qualified by evidential material referenced in the following set of elements. Req's marked by "D" at the element No.
2. *Content and presentation of evidence* elements: the evidence required, what the evidence demonstrates, what the evidence shall convey. Marked by "C".
3. *Evaluator action elements*: activities that shall be performed by the evaluator. Marked by "E".

Certified Products by Assurance Level and Certification Date												
EAL	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**Total**
EAL1	0	0	0	0	0	0	3	3	8	6	3	23
EAL1+	0	0	0	0	0	0	1	0	0	1	0	2
EAL2	0	0	0	0	0	5	18	15	26	13	15	92
EAL2+	0	0	1	0	0	8	59	76	66	42	31	283
EAL3	0	0	0	0	0	5	9	1	3	6	9	33
EAL3+	0	0	0	0	0	12	17	19	10	9	1	68
EAL4	0	0	0	0	0	0	0	5	2	9	5	21
EAL4+	1	1	4	2	1	25	56	55	52	49	50	296
EAL5	0	0	0	0	0	0	0	3	1	4	2	10
EAL5+	0	0	0	0	0	12	41	69	69	55	35	281
EAL6	0	0	0	0	0	0	0	0	0	0	0	0
EAL6+	0	0	0	1	2	1	9	8	12	22	16	71
EAL7	0	0	0	0	0	0	0	0	0	1	0	1
EAL7+	0	0	0	0	0	0	0	0	0	1	0	1
Basic	0	0	0	0	0	0	0	0	0	0	0	0
Medium	0	0	0	0	0	0	0	0	0	0	0	0
US Standard	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	13	15	28	89	96	241
Totals:	**1**	**1**	**5**	**3**	**3**	**68**	**226**	**269**	**277**	**307**	**263**	**1423**

7 evaluation assurance levels (EALs)

- Hierarchical system – higher or new components
  - bold faced text in the description for the **added components**

- The following slides present first the EALs in the language of the CC and then from a practical perspective.

EAL1 – functionally tested

- some confidence in correct operation is required, but the threats to security are not viewed as serious
  - sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, etc. through security objectives;
  - analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.
  - This EAL provides a meaningful increase in assurance over unevaluated IT.

EAL2 – structurally tested

- assurance by a full security target (with given SFRs);
- analysis of the SFRs, using *functional* and *interface specs*, *guidance documentation* and *basic TOE architecture* description to understand the security behaviour;
- configuration management system and evidence of secure delivery procedures;
- independent confirmation of the developer test results, vulnerability analysis (based upon the *above in italics*) demonstrating resistance to penetration attackers with a basic attack potential.

EAL3 – methodically tested and checked

- architectural description of the TOE design;
- development environment controls
- improved testing coverage of the security functionality and mechanisms and/or procedures that provide some confidence that the TOE was not tampered with during development.

EAL4 – methodically designed, tested, and reviewed

- complete interface specification, description of the basic modular design of the TOE, implementation representation for the entire TSF;
- demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential;
- additional TOE configuration mgmt incl. automation.

EAL5 – semiformally designed and tested

- modular TSF design;
- comprehensive TOE configuration management;
- semiformal design descriptions, a more structured (and hence analysable) architecture.

EAL6 – semiformally verified design and tested

- formal model of select TOE security policies;
- semiformal presentation of the functional specification and TOE design;
- modular layered and simple TSF design;
- structured development process, development environment controls, and comprehensive TOE configuration mgmt incl. complete automation;
- more comprehensive analysis, more architectural structure (e.g. layering), more comprehensive independent vulnerability analysis.

EAL7 – formally verified design and tested

- structured presentation of the implementation;
- implementation representation, complete independent confirmation of the developer test results;
- comprehensive analysis using formal representations and formal correspondence, and comprehensive testing.

CC certified products by country & EAL

Certified Products by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	20	28
Canada	2	0	10	112	0	0	0	0	0	0	0	0	0	0	0	0	0	49	173
Germany	1	0	7	6	3	11	4	82	0	58	0	41	0	0	0	0	0	7	220
Spain	2	0	6	13	3	4	1	20	0	8	0	0	0	0	0	0	0	9	66
France	0	0	0	1	0	16	2	96	5	179	0	15	1	0	0	0	0	0	315
India	1	0	4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	6
Italy	4	2	1	3	0	0	0	23	1	0	0	0	0	0	0	0	0	0	34
Japan	0	0	4	96	8	25	0	2	0	0	0	0	0	0	0	0	0	19	154
Republic of Korea	7	0	5	8	0	0	0	2	0	7	0	0	0	0	0	0	0	14	43
Malaysia	0	0	17	16	0	2	0	3	0	0	0	0	0	0	0	0	0	0	38
Netherlands	0	0	6	3	1	1	1	23	0	17	0	15	0	1	0	0	0	1	69
Norway	1	0	1	16	2	5	7	13	1	9	0	0	0	0	0	0	0	0	55
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	5	0	12	2	12	4	5	3	3	0	0	0	0	0	0	0	0	12	58
Singapore	0	0	3	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	4
Turkey	0	0	9	1	3	0	1	11	0	0	0	0	0	0	0	0	0	0	25
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	109	109
Totals:	**23**	**2**	**89**	**281**	**33**	**68**	**21**	**279**	**10**	**278**	**0**	**71**	**1**	**1**	**0**	**0**	**0**	**240**	**1423**

EAL1 – functionally tested

- analysis supported by independent testing of a sample of the security functions;
- applicable where confidence in correct operation is required but the security threat assessment is low.

- This EAL is particularly suitable for legacy systems as it should be achievable without the assistance of the developer.

EAL2 – structurally tested

- analysis exercises a functional and interface specification and the high-level design of the subsystems of the TOE;
- independent testing of the security functions;
- evidence required of developer 'black box' testing and development search for obvious vulnerabilities.

- EAL2 is applicable where a low to moderate level of independently assured security is required.

EAL3 – methodically tested and checked

- analysis supported by 'grey box' testing, selective independent confirmation of the developer test results and evidence of a developer search for obvious vulnerabilities;
- development environment controls and TOE configuration management are also required.

- EAL3 for a moderate level of independently assured security, with a thorough investigation of the TOE and its development, without incurring substantial re-engineering costs.

EAL4 – methodically designed, tested, and reviewed

- analysis supported by the low-level design of TOE modules and a subset of the implementation;
- testing supported by an independent search for obvious vulnerabilities;
- development controls supported by a life-cycle model, identification of tools and automated configuration management.

- EAL4 for a moderate to high level security, where some additional security-specific engineering costs may be incurred.

EAL5 – semiformally designed and tested

- analysis includes all of the implementation;
- supplemented by a *formal model*, a *semiformal presentation of the functional specification* and high level design and a *semiformal demonstration of correspondence*;
- search for vulnerabilities must ensure resistance to penetration attackers with a moderate attack potential;
- covert channel analysis and modular design required.
- EAL5 for a high level of security in a planned development coupled with a rigorous development approach.

EAL6 – semiformally verified design and tested

- analysis supported by a *modular approach to design* and a structured presentation of the implementation;
- independent search for vulnerabilities must ensure resistance to penetration attackers with a high attack potential;
- a systematic search for covert channels;

- EAL6 where a specialised security TOE is required for high risk situations.

EAL7 – formally verified design and tested

- the formal model is supplemented by a *formal presentation of the functional specification and high level design, showing correspondence*;
- evidence of developer 'white box‘ testing and complete independent confirmation of developer test results.

- EAL7 where a specialised security TOE is required for extremely high risk situations.

CC certified products by country & EAL

Certified Products by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	0	0	20	28
Canada	2	0	10	112	0	0	0	0	0	0	0	0	0	0	0	0	0	49	173
Germany	1	0	7	6	3	11	4	82	0	58	0	41	0	0	0	0	0	7	220
Spain	2	0	6	13	3	4	1	20	0	8	0	0	0	0	0	0	0	9	66
France	0	0	0	1	0	16	2	96	5	179	0	15	1	0	0	0	0	0	315
India	1	0	4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	6
Italy	4	2	1	3	0	0	0	23	1	0	0	0	0	0	0	0	0	0	34
Japan	0	0	4	96	8	25	0	2	0	0	0	0	0	0	0	0	0	19	154
Republic of Korea	7	0	5	8	0	0	0	2	0	7	0	0	0	0	0	0	0	14	43
Malaysia	0	0	17	16	0	2	0	3	0	0	0	0	0	0	0	0	0	0	38
Netherlands	0	0	6	3	1	1	1	23	0	17	0	15	0	1	0	0	0	1	69
Norway	1	0	1	16	2	5	7	13	1	9	0	0	0	0	0	0	0	0	55
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	5	0	12	2	12	4	5	3	3	0	0	0	0	0	0	0	0	12	58
Singapore	0	0	3	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	4
Turkey	0	0	9	1	3	0	1	11	0	0	0	0	0	0	0	0	0	0	25
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	109	109
Totals:	**23**	**2**	**89**	**281**	**33**	**68**	**21**	**279**	**10**	**278**	**0**	**71**	**1**	**1**	**0**	**0**	**0**	**240**	**1423**

Famous issue – Windows 2000

- Windows 2000 operating system was certified (Common Criteria) at EAL-4 in 2002.
  - with SP3 and one patch;
  - EAL-4, augmented with ALC_FLR.3 (Systematic Flaw Remediation);
  - Microsoft invested millions of dollars and three years of effort to gain the certification. (S. Bekker, Redmond Magazine).
- Controlled Access Protection Profile (CAPP)

CAPP assumption A.PEER

"Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

The TOE is applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain.

There are no security requirements that address the need to trust external systems or the communications links to such systems."

Controlled Access Protection Profile

- Level of protection appropriate for an assumed non-hostile and well-managed user community
  - requiring protection against threats of inadvertent or casual attempts to breach the system security.
- The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security.
- CAPP does not fully address the threats posed by malicious system development or administrative personnel.

Windows 2000 EAL-4 certification

- EAL4 rating means that you did a lot of paperwork related to the software process, but says absolutely nothing about the quality of the software itself. (J.S. Shapiro)
- System disconnected from networks (at different security level), disabled media drives, etc.
- Don't hook this to the internet, don't run email, don't install software unless you can 100 percent trust the developer, and if anybody who works for you turns out to be out to get you, you are toast. (J.S. Shapiro)

And Now for Something Completely Different… about Assurance viewed by…

- Customer – what level of guarantee do I get that security has been implemented in the product?
- Developer – what (inputs and cooperation) will my team have to provide for the evaluation?
- Evaluator – did I get all required inputs and did all tests run OK to confirm the claim?
- Operator – what assumptions can I build on when preparing for my actions?

Security Requirements for Cryptographic Modules

- Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2)
- published May 2001 and last updated Dec 2002
  - FIPS 140-3 (Draft) – proposed revision, hanging in the air since 2009 (!)
- 4 levels, hierarchical levelling
- 11 functions (requirements):
  - Cryptographic module specification; Cryptographic module ports and interfaces; Role, services, and authentication; Physical security; Operational environment; Cryptographic key management; Mitigation of other attacks; …

FIPS 140-2 Annexes (drafts)

- Annex A: Approved Security Functions (Draft 2011)
- Annex B: Approved Protection Profiles (Draft 2007)
- Annex C: Approved Random Number Generators (Draft 2010)
- Annex D: Approved Key Establishment Techniques (Draft 2011)

FIPS 140-2 levels I

Level 1

- basic security requirements (e.g., certified algorithm);
- no specific physical security mechanisms.

Level 2

- features that show evidence of tampering – physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module
  - including tamper-evident coatings or seals that must be broken to attain,
- or pick-resistant locks on covers or doors to protect against unauthorized physical access.

FIPS 140-2 levels II

Level 3

- high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module;
- may include the use of strong enclosures and tamper detection/response circuitry that zeroes all plain text CSPs when the removable covers/doors of the cryptographic module are opened.

FIPS 140-2 levels III

Level 4

- physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access;
- protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature;
- for operation in physically unprotected environments.

FIPS 140-2

- Level 2 – operating system at EAL2+
- Level 3 – operating system at EAL3+
  – and additional req.: Security Policy Model (ADV_SPM.1)
- Level 4 – operating system at EAL4+

Nice standards and theory, but…

- OpenSSL derivative FIPS-certified, found flawed
  - that particular one de-certified, others including the flaw not
- Dual EC DRBG defective by design mandated for FIPS 140-2
- IBM 4758 (with CCA API) – level 4
  - easy/fast logical attacks on CCA API
- Safenet Luna CA^3
  - disassembling showed no potting material
  - undocumented API functions
  - functionality in breach of security policy

Study of another PP development

- Security kernel – used to simulate a distributed environment, introduced by J Rushby (1981) as a solution to the difficulties and problems that had arisen in the development and verification of large, complex security kernels that were intended to "provide multilevel secure operation on general-purpose multi-user systems."
- U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, v 1.03
- Study paper "Separation Kernel Protection Profile Revisited: Choices and Rationale", T.E. Levin et al., URL: http://fm.csl.sri.com/LAW/2010/law2010-03-Levin-Nguyen-Irvine.pdf