Common Criteria (*for Information Technology Security Evaluation*)

PV017 – Řízení informační bezpečnosti

Vashek Matyáš

CROCS
Centre for Research on Cryptography and Security

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- 7 úrovní záruky (EAL) – Společná kritéria
- Zajímavý příklad s Win2K
- Závěr

Kritéria hodnocení bezpečnosti

- USA – konec 60. let a 70. léta – potřeba minimalizace nákladů na individuální hodnocení
- 1985 – Trusted Computer System Evaluation Criteria – “Orange Book”
  - Třída D – žádná bezpečnost
  - A1 – nejvyšší bezpečnost (matematický formalismus)

Vývoj kritérií

- Evropa – ITSEC – oddělení funkčnosti a záruk (plus metodologie – ITSEM)
- Kanada – CTCPEC – funkčnost rozdělena do skupin důvěrnost, integrita, zodpovědnost a dostupnost (plus krypto)
- US – Federal Criteria – vývoj zastaven
- **Společná kritéria** (Common Criteria) – celosvětový standard
  – ISO/IEC 15408

Pojmy

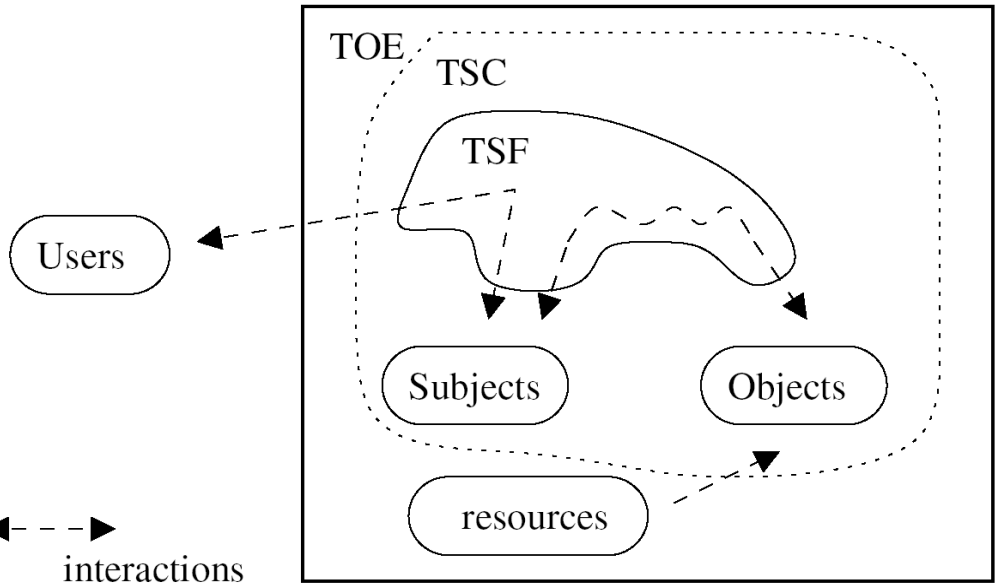
- **Akreditace** – oficiální souhlas (pověření) s prováděním určité činnosti
- **Certifikace** – vydání daného osvědčení na základě provedeného hodnocení
- **Hodnocení** (evaluace) – ověření shody deklarovaných vlastností (dle kritérií)
- **Validace** – ověření platnosti/souladu, v US terminologii „hodnocení“ – viz výše

Důležité pojmy z CC

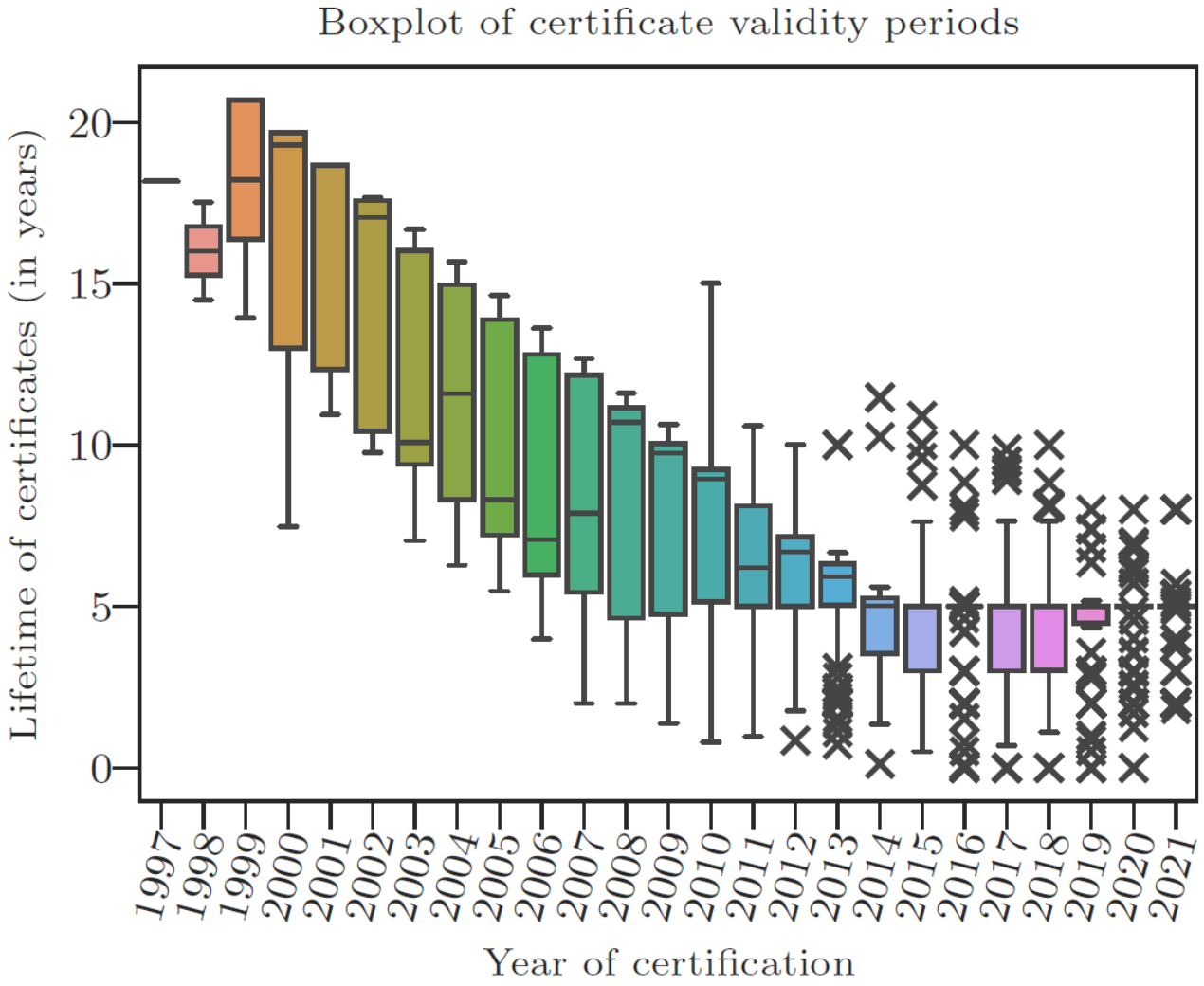
- **Předmět hodnocení** (*Target of Evaluation, TOE*) – produkt nebo systém (nebo jeho část), který je předmětem hodnocení
- **Specifikace bezpečnosti** (*Security Target*, ST) – cílová kombinace komponent spojených s konkrétním produktem nebo systémem
- **Profil bezpečnosti** (*Protection Profile, PP*) – implementačně nezávislá skupina bezpečn. požadavků určité skupiny TOE

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



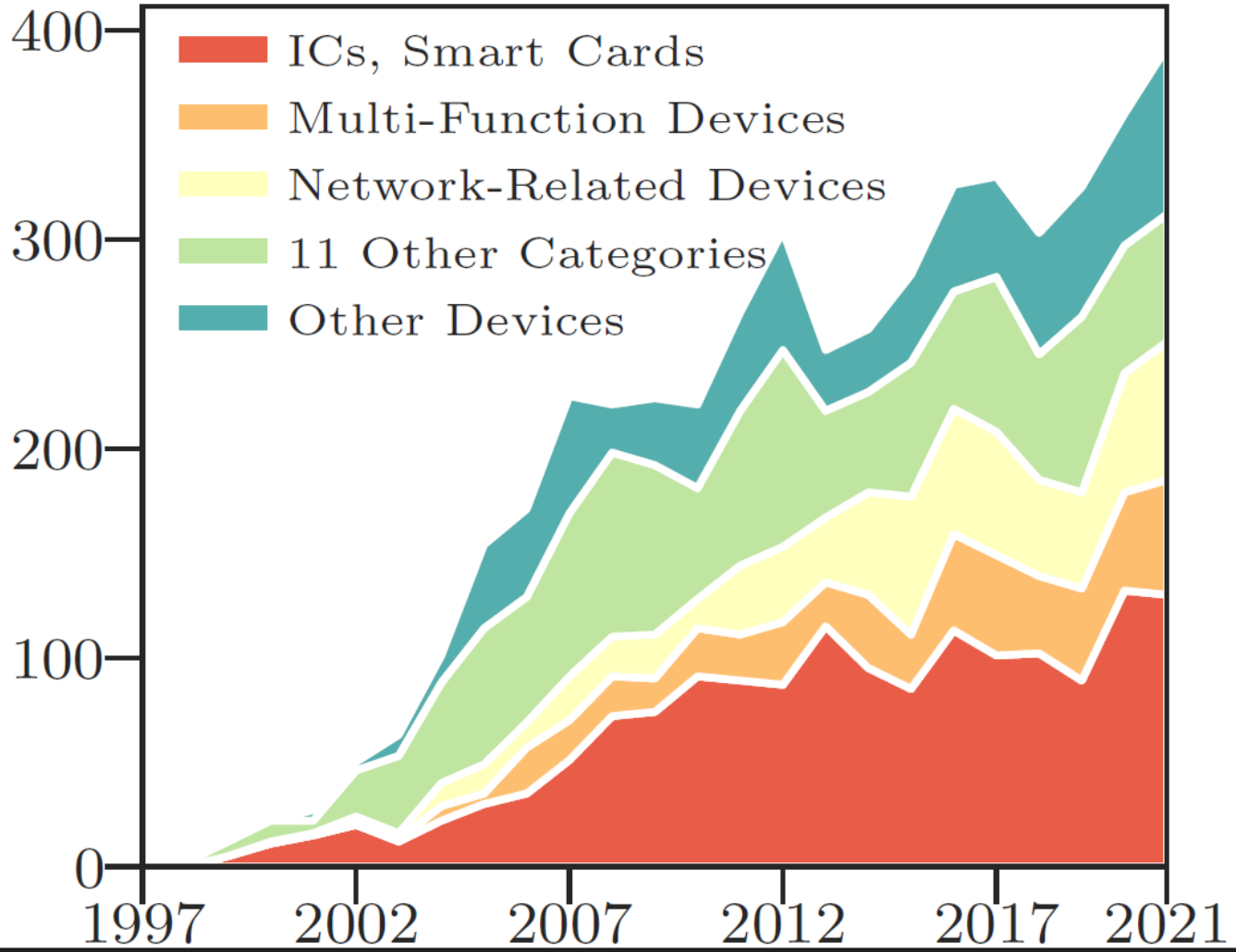
Platnost CC certifikátů



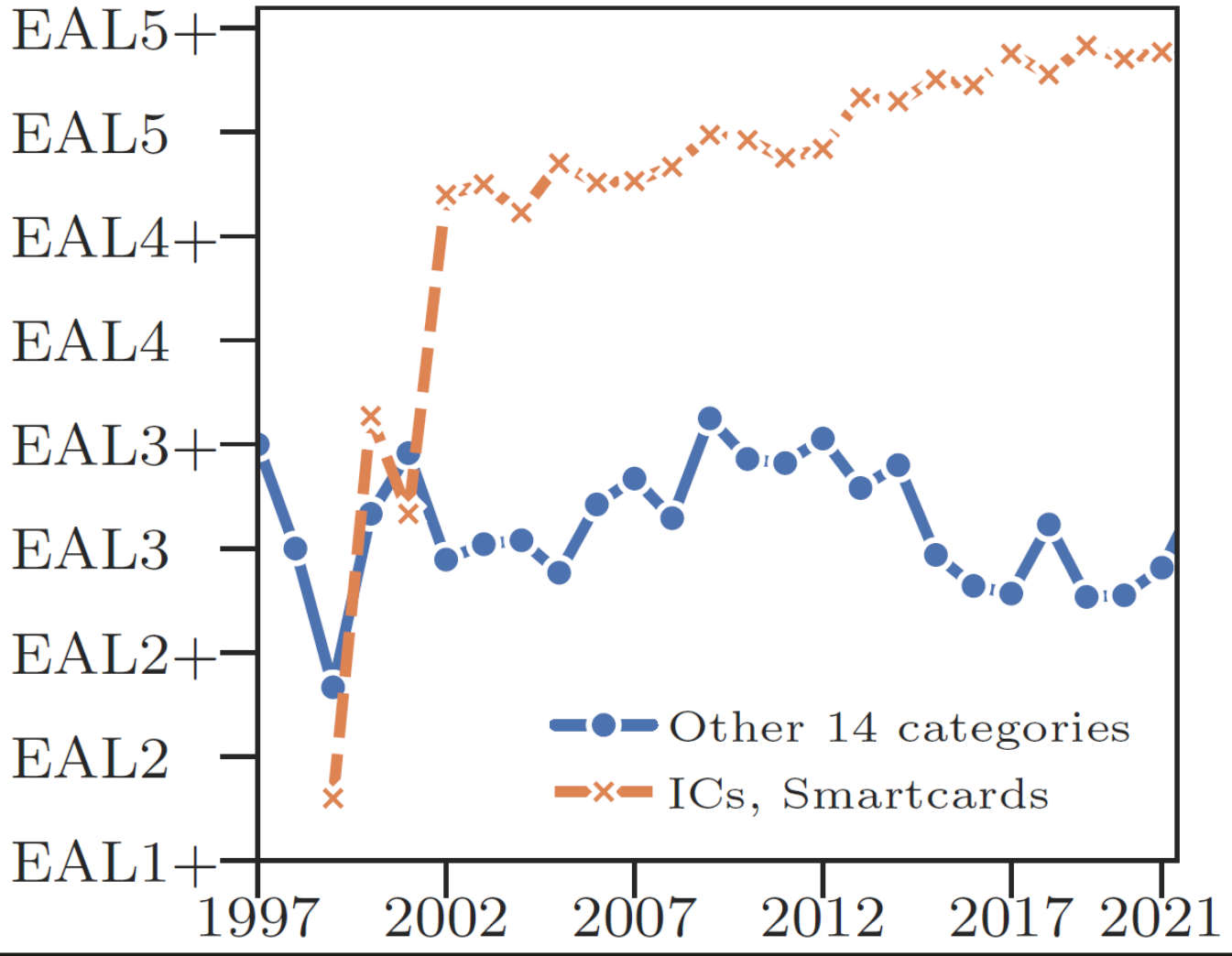
Společná kritéria

- Zájem uživatelů, výrobců, hodnotitelů
- Profil bezpečnosti (čipové karty, biometriky, DBMS, poštovní razítkovače ap.)
  - „Minikritéria“ – katalogovány jako samostatný hodnotitelský dokument
  - Popisy bezpečnostních potřeb často různorodé ☹
- Security target (ST) – teoretický koncept/cíl
- Hodnocení TOE = odpovídá realita teorii (ST)?
- Požadavky na *funkčnost* (angl. functionality) a *záruky* (angl. assurance)

Certifikovaná zařízení (dle CC)



Certifikovaná zařízení (dle CC) – pokr.



Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- 7 úrovní záruky (EAL) – Společná kritéria
- Zajímavý příklad s Win2K
- Závěr

Study of a particular PP

- PP BSI-PP-0025 – German (BSI) Common Criteria Protection Profile for USB Storage Media
- 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.

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- 7 úrovní záruky (EAL) – Společná kritéria
- Zajímavý příklad s Win2K
- Závěr

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)

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 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

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

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".

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- 7 úrovní záruky (EAL) – Společná kritéria
- Zajímavý příklad s Win2K
- Závěr

Certified Products by Assurance Level and Certification Date

EAL	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Basic	0	0	0	0	0	0	0	0	0	0	1	5	38	37	81
EAL1	0	0	0	0	0	0	0	0	1	4	4	3	2	0	14
EAL1+	0	0	0	0	0	0	0	0	0	0	1	0	2	2	5
EAL2	0	0	0	0	0	0	0	1	1	18	15	39	12	6	92
EAL2+	0	0	0	0	0	2	1	5	2	31	43	35	30	26	175
EAL3	0	0	0	0	0	2	0	0	2	10	9	5	0	2	30
EAL3+	0	0	0	0	0	3	1	0	1	5	12	18	29	10	79
EAL4	0	0	0	0	0	0	3	0	6	8	5	3	2	2	29
EAL4+	1	0	0	0	1	3	7	5	11	46	62	68	73	76	353
EAL5	0	0	0	0	0	0	1	0	0	1	2	0	4	2	10
EAL5+	0	0	0	0	2	2	5	17	17	47	69	45	40	55	299
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	1	1	2
EAL6+	0	0	0	0	0	1	0	0	1	21	20	30	33	33	139
EAL7	0	0	0	0	0	0	0	0	1	0	1	0	1	0	3
EAL7+	0	0	0	0	0	0	0	0	0	0	0	1	0	1	2
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	4	61	44	83	84	100	376
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Totals:	**1**	**0**	**0**	**0**	**3**	**13**	**18**	**28**	**47**	**252**	**288**	**335**	**351**	**353**	**1689**

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 from a practical perspective.

CC certified products by country & EAL

Certified Products by Scheme and Assurance Level

Scheme	B	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	M	N	S	Total
Australia	0	0	0	5	4	0	0	0	0	0	0	0	0	0	0	0	15	0	24
Canada	6	0	0	1	31	0	0	0	4	0	0	0	0	0	0	0	81	0	123
Germany	4	1	1	17	10	14	37	7	93	2	25	0	55	0	1	0	1	0	268
Spain	2	0	0	7	12	2	6	3	18	0	13	0	1	0	0	0	10	0	74
France	1	0	0	0	10	0	11	2	78	5	180	2	50	3	0	0	0	0	342
India	1	2	0	9	2	1	0	0	0	0	0	0	0	0	0	0	1	0	16
Italy	3	1	2	1	11	0	0	2	23	0	2	0	0	0	0	0	12	0	57
Japan	47	0	0	5	35	0	0	0	2	0	1	0	0	0	0	0	48	0	138
Republic of Korea	0	4	1	3	1	0	0	0	2	0	4	0	0	0	0	0	35	0	50
Malaysia	0	1	0	16	11	0	1	0	2	0	0	0	0	0	0	0	0	0	31
Netherlands	1	0	0	5	14	1	9	2	91	2	65	0	33	0	1	0	0	0	224
Norway	0	1	0	1	12	2	5	9	13	1	8	0	0	0	0	0	0	0	52
Poland	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Qatar	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	16	3	1	18	13	9	10	4	7	0	0	0	0	0	0	0	16	0	97
Singapore	0	1	0	2	8	0	0	0	10	0	0	0	0	0	0	0	0	0	21
Turkey	0	0	0	2	1	1	0	0	10	0	1	0	0	0	0	0	0	0	15
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	157	0	157
Totals:	**81**	**14**	**5**	**92**	**175**	**30**	**79**	**29**	**353**	**10**	**299**	**2**	**139**	**3**	**2**	**0**	**376**	**0**	**1689**

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.

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- 7 úrovní záruky (EAL) – Společná kritéria
- Zajímavý příklad s Win2K
- Závěr

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.

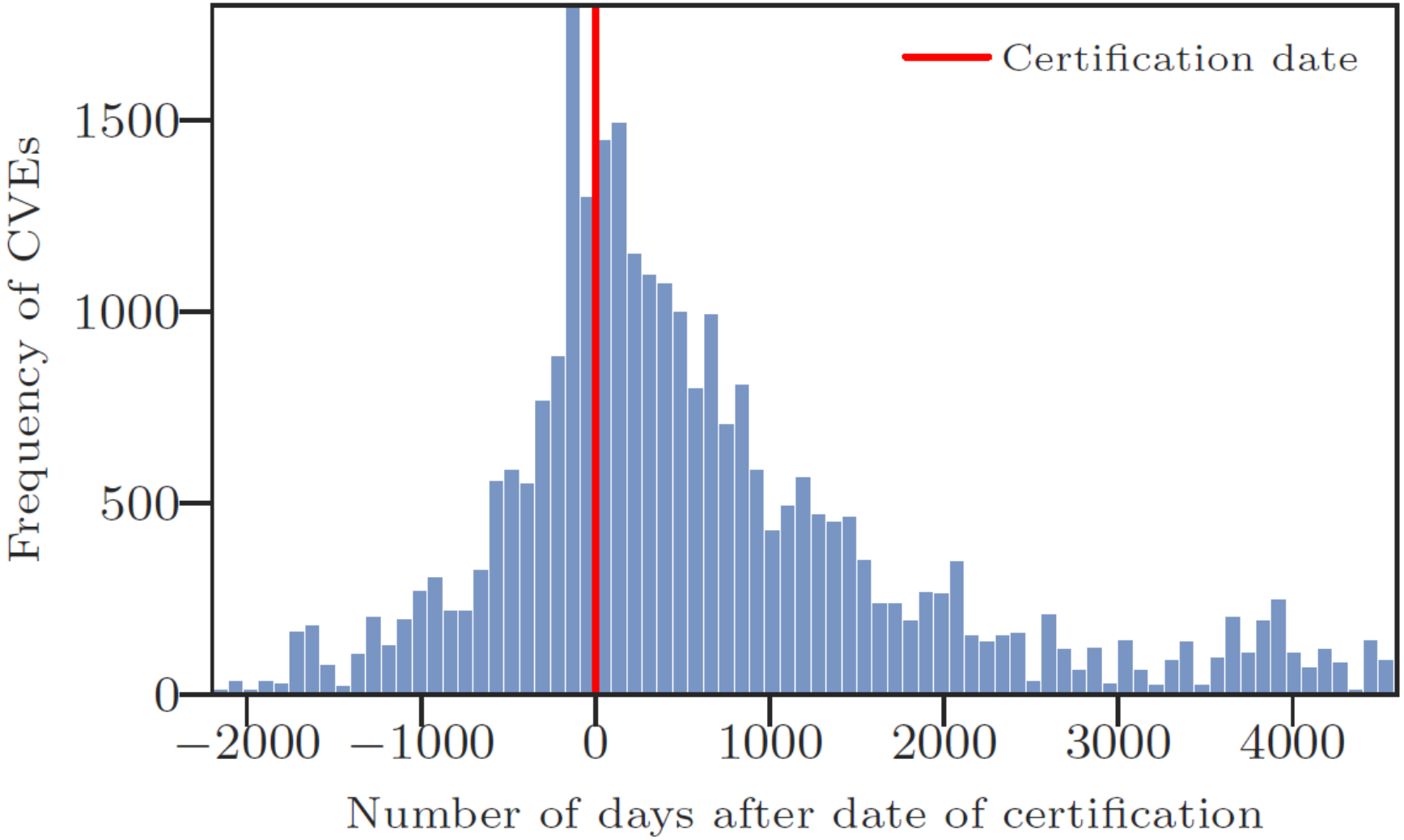
Windows 2000 EAL-4 certification

- 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)

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- 7 úrovní záruky (EAL) – Společná kritéria
- Zajímavý příklad s Win2K
- Závěr

Vztah data certifikace a data CVE



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?

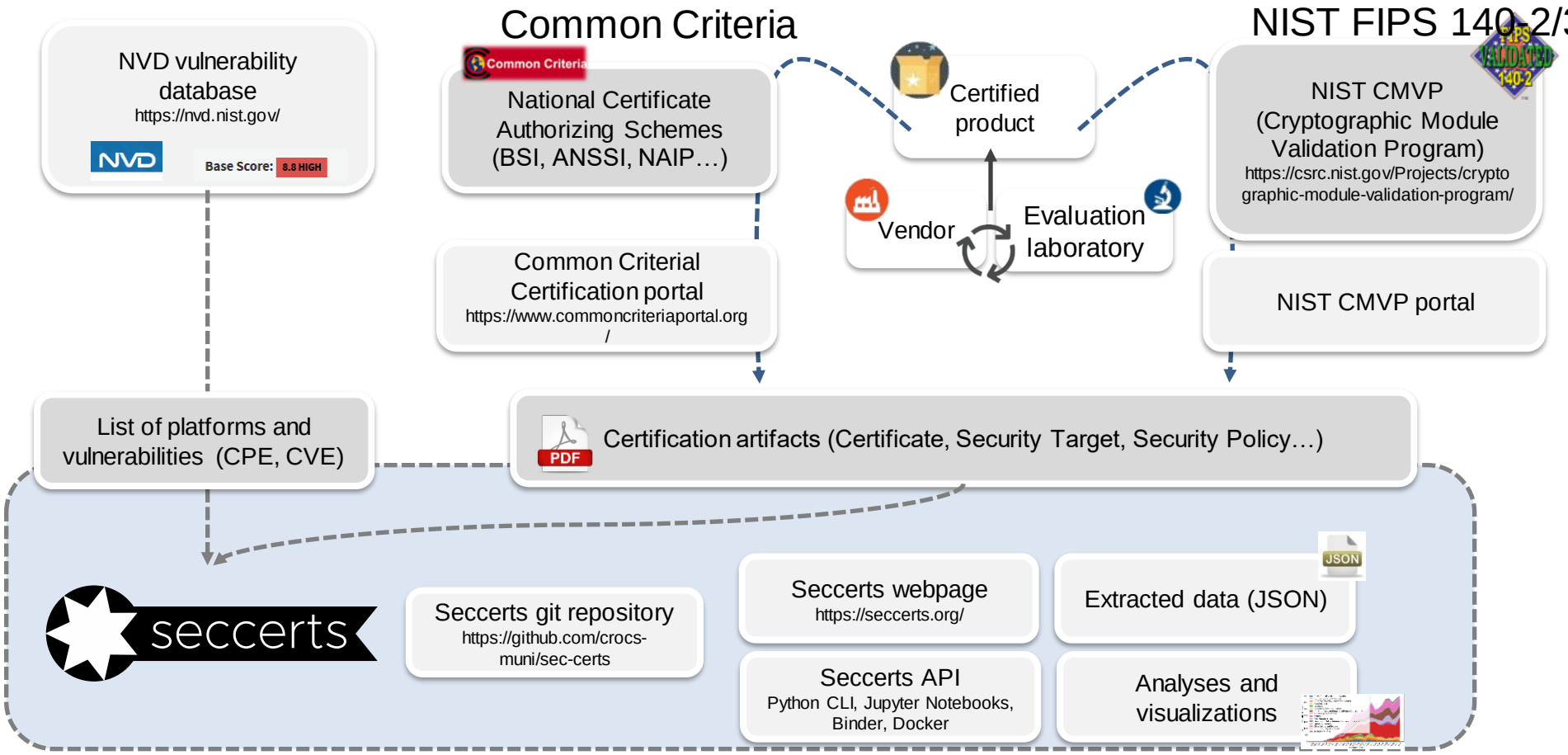
Význam a výhody kritérií

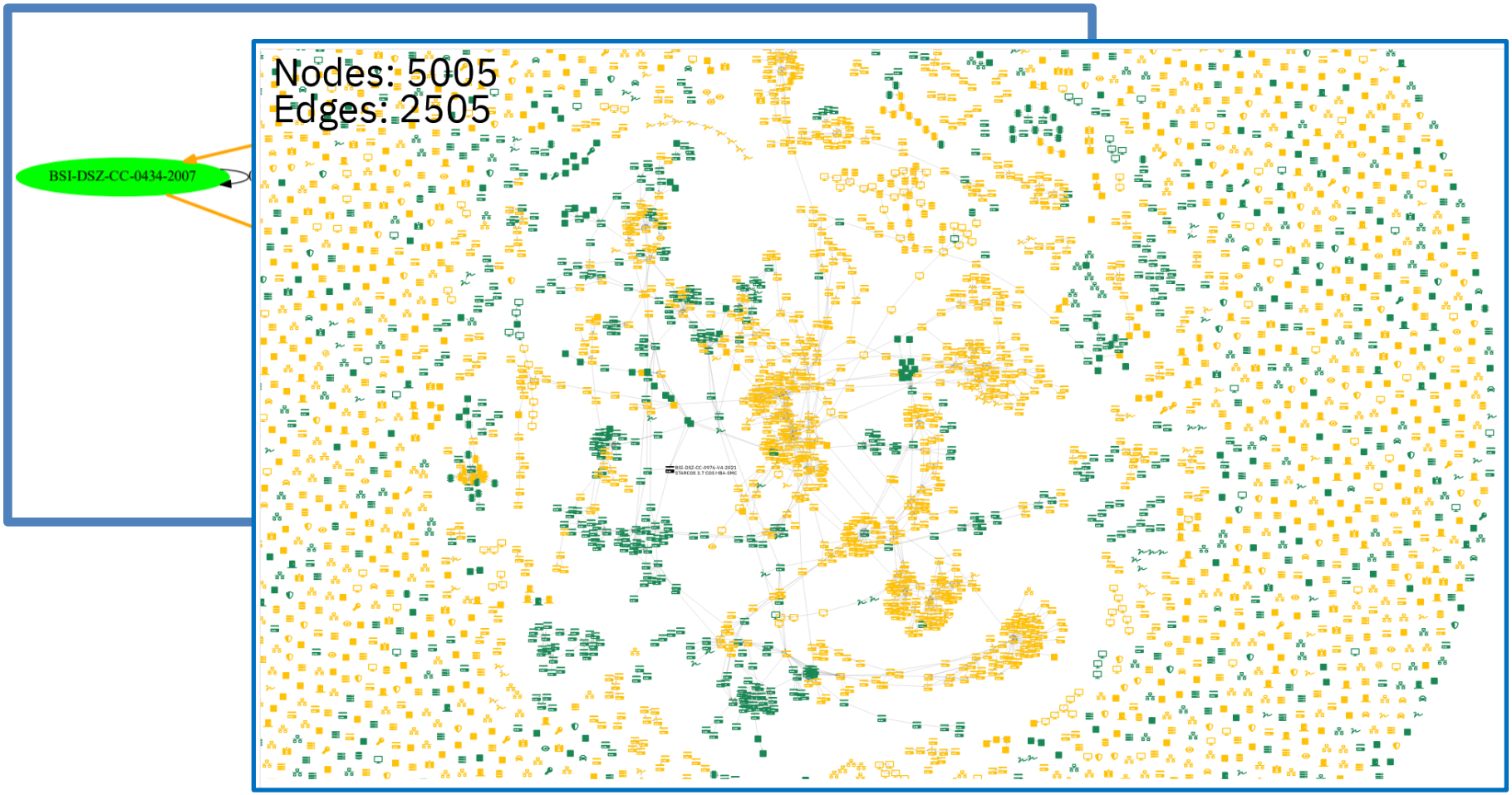
- Usnadňují nasazení a používání bezpečných systémů – jednodušší srovnávání a výběr podle skutečných potřeb
- Usnadňují specifikaci požadavků
- Ujasňují požadavky na návrh a vývoj

Problémy kritérií (CC)

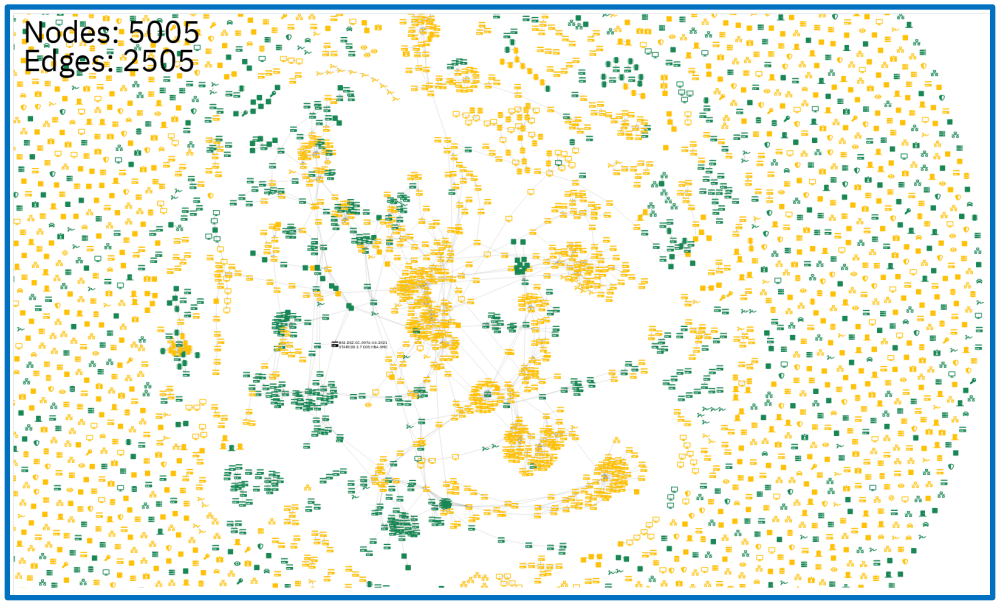
- Hodnocení není levné ani rychlé (>$100k, >3 měs)
- Certifikace platí jen pro přesně danou konfiguraci (HW i SW!!)
- Marketingové označení “Common Criteria certified” (ToE details, achieved EAL, PP conformance, laboratory used…) není to stejné jako “Common Criteria ready”
- Řada detailů hodnocení není veřejně dostupná

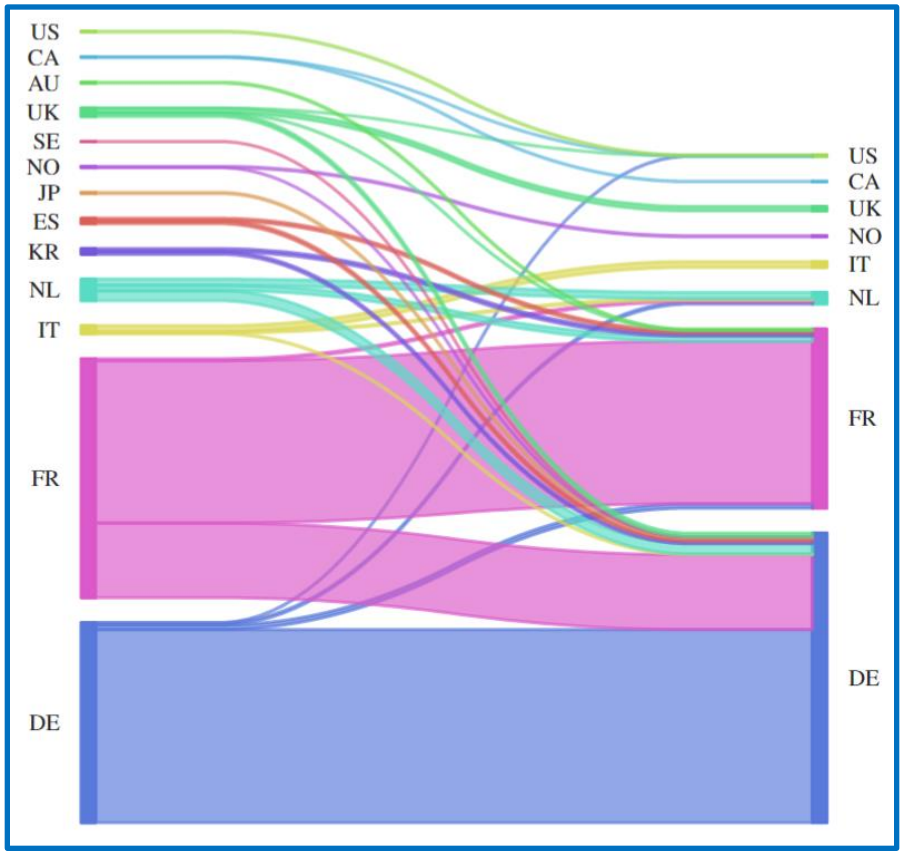

seccerts


Common Criteria
NIST FIPS 140-2/3
NVD vulnerability database
https://nvd.nist.gov/
NVD
Base Score: 8.8 HIGH
Common Criteria
National Certificate Authorizing Schemes (BSI, ANSSI, NAIP…)
Certified product
NIST CMVP (Cryptographic Module Validation Program)
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/
FIPS VALIDATED 140-2
Vendor
Evaluation laboratory
Common Criterial Certification portal
https://www.commoncriteriaportal.org/
NIST CMVP portal
List of platforms and vulnerabilities (CPE, CVE)
PDF
Certification artifacts (Certificate, Security Target, Security Policy…)
seccerts
Seccerts git repository
https://github.com/crocs-muni/sec-certs
Seccerts webpage
https://seccerts.org/
JSON
Extracted data (JSON)
Seccerts API
Python CLI, Jupyter Notebooks, Binder, Docker
Analyses and visualizations


Nodes: 5005
Edges: 2505
BSI-DSZ-CC-0434-2007

Vhledy…


Nodes: 5005
Edges: 2505


US
CA
AU
UK
SE
NO
JP
ES
KR
NL
IT
FR
DE
US
CA
UK
NO
IT
NL
FR
DE

DĚKUJI ZA POZORNOST!

Použité zdroje

- *Common Criteria for Information Technology Security Evaluation*, v 3.1, release 5, April 2017
  - https://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
- https://seccerts.org