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)
- Zajímavý příklad s Win2K
- Nástroj sec-certs
- 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

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)

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- Zajímavý příklad s Win2K
- Nástroj sec-certs
- 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)
- Zajímavý příklad s Win2K
- Nástroj sec-certs
- 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 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?

7 evaluation assurance levels (EALs)

- Hierarchical system – higher or new components

Agenda

- Kritéria hodnocení (bezpečnosti) – úvod
- Příklad profilu bezpečnosti
- Funkčnost (functionality) a záruka (assurance)
- Zajímavý příklad s Win2K
- Nástroj sec-certs
- 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)
- Zajímavý příklad s Win2K
- Nástroj sec-certs
- Závěr

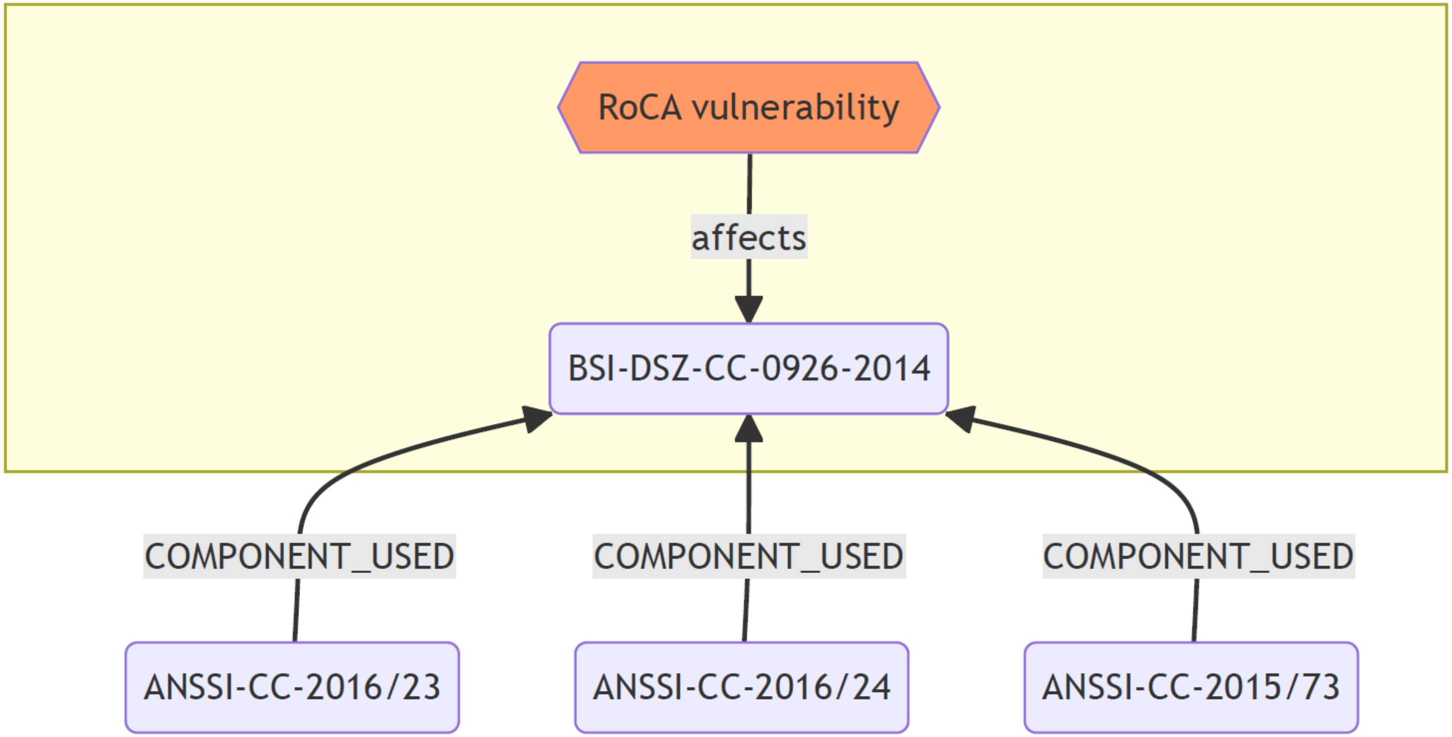
seccerts

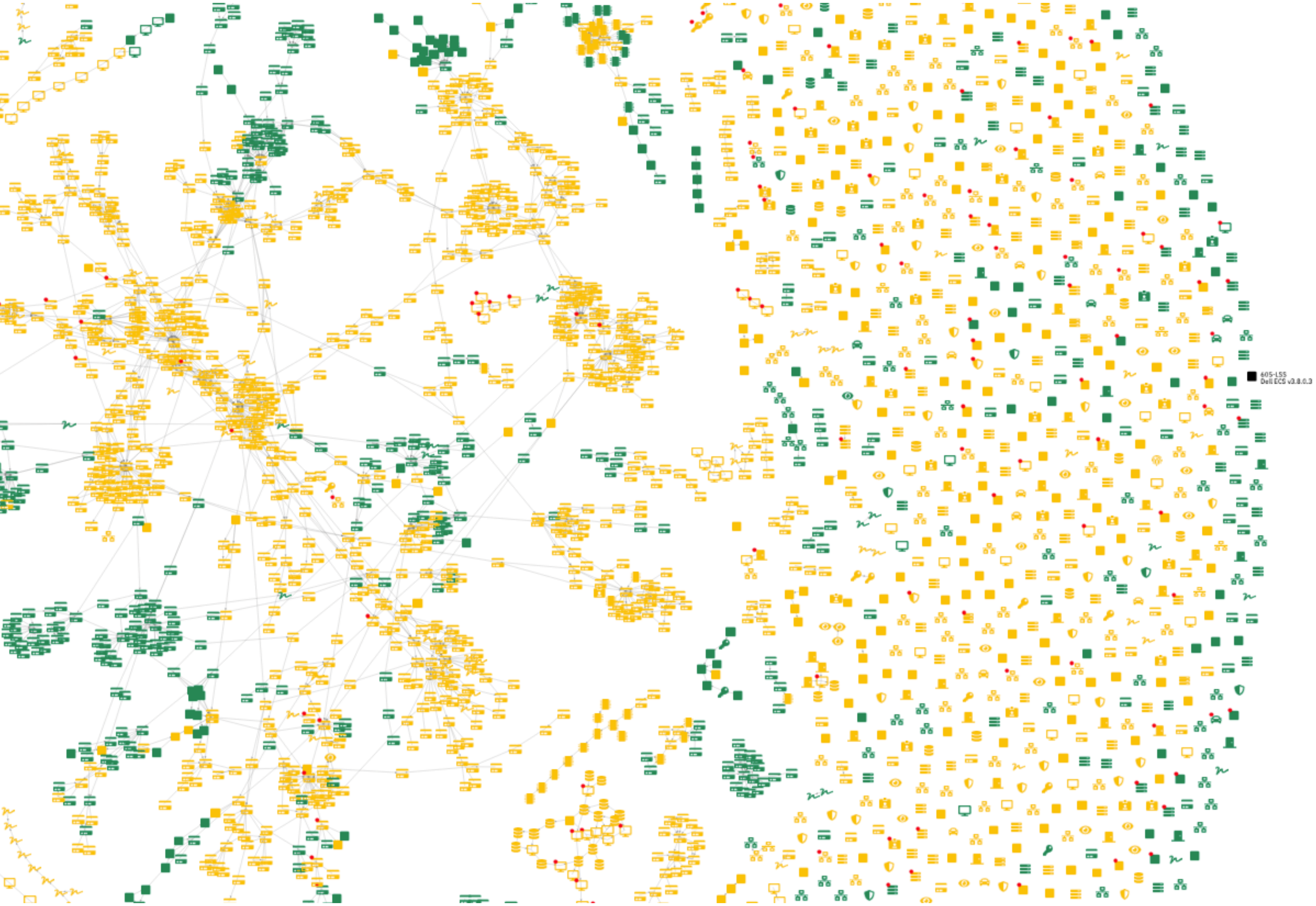
CVE-2017-15361 (RoCA)

- [CVE-2017-15361]: practical factorization of certain RSA keys.
- Billion+ devices affected.

- ⚠ How many products certified under Common Criteria are impacted?

CVE-2017-15361

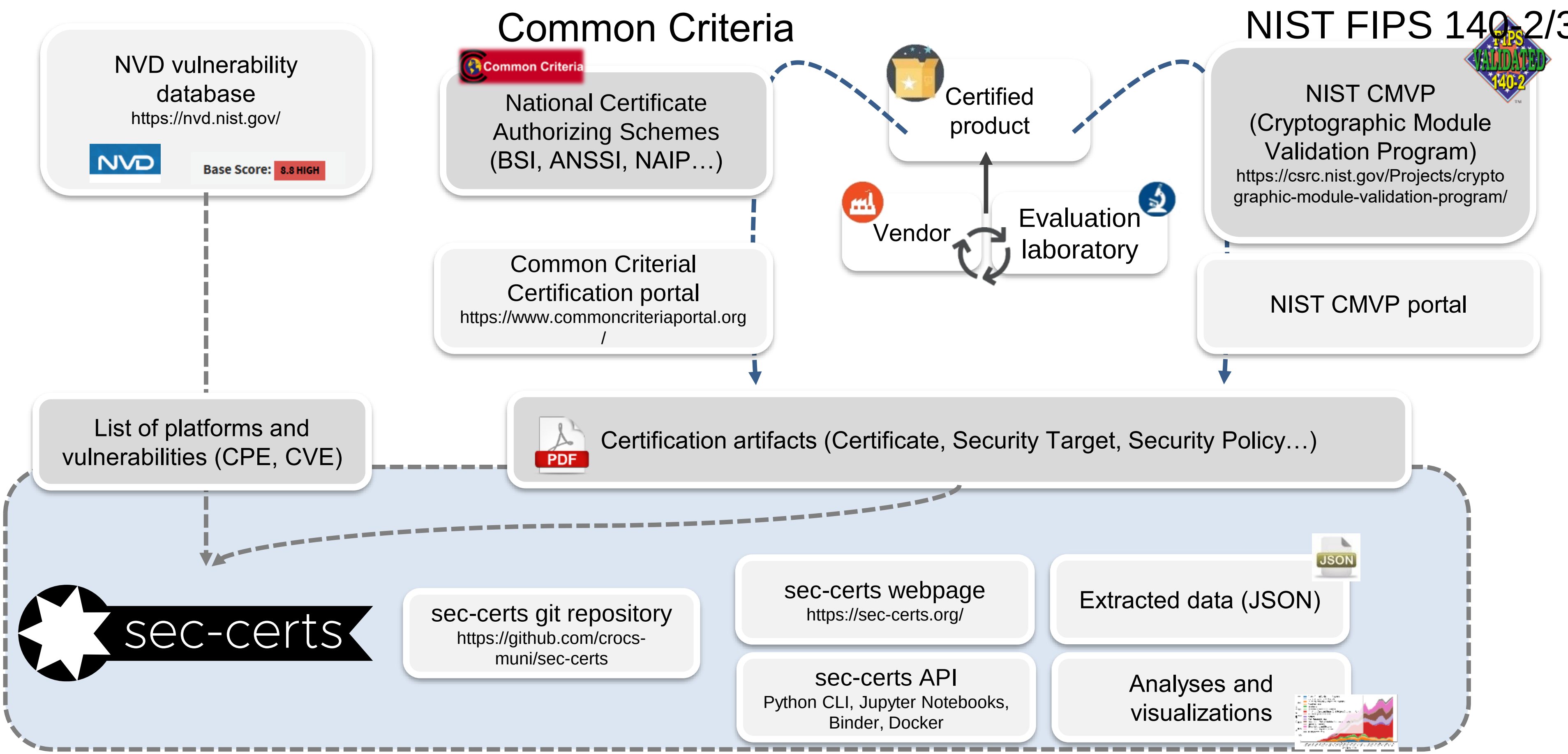



605-LSS
Dell ECS v3.8.0.3

What if you need help answering questions like

- What processor architectures are commonly used in certifications/products of interest?
- How do we compare with our competitors (their certified products)?
- Check how long evaluations take for certain labs, types of products, etc.

SO WHAT DO WE DO?



Common Criteria

NIST FIPS 140-2/3

NVD vulnerability database
https://nvd.nist.gov/

National Certificate Authorizing Schemes (BSI, ANSSI, NAIP…)

Certified product

Vendor

Evaluation laboratory

NIST CMVP (Cryptographic Module Validation Program)
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/

Common Criterial Certification portal
https://www.commoncriteriaportal.org/

NIST CMVP portal

List of platforms and vulnerabilities (CPE, CVE)

Certification artifacts (Certificate, Security Target, Security Policy…)

sec-certs

sec-certs git repository
https://github.com/crocs-muni/sec-certs

sec-certs webpage
https://sec-certs.org/

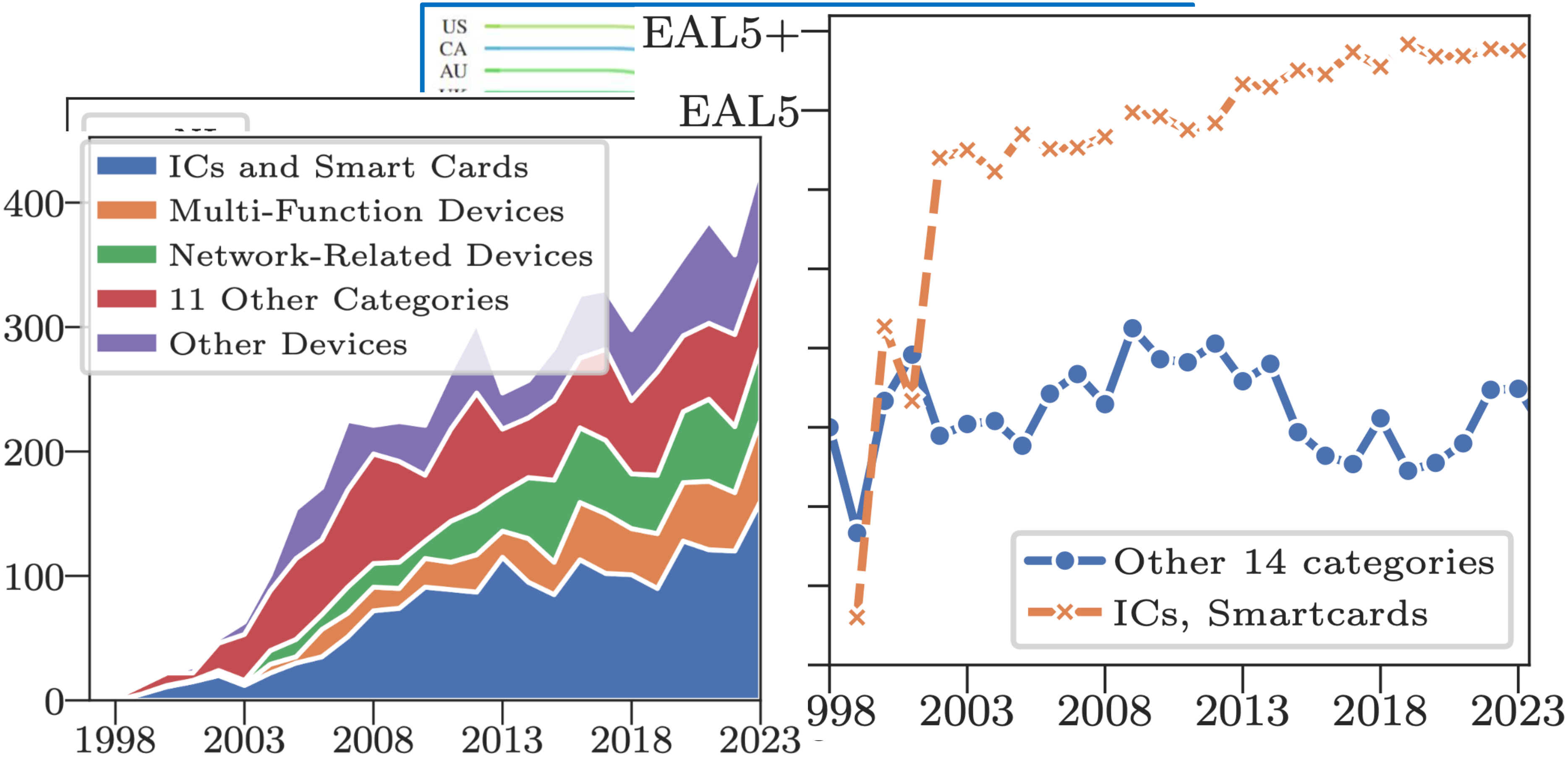
Extracted data (JSON)

sec-certs API
Python CLI, Jupyter Notebooks, Binder, Docker

Analyses and visualizations

VARIOUS ECOSYSTEM INSIGHTS

seccerts


US
CA
AU
ICs and Smart Cards
Multi-Function Devices
Network-Related Devices
11 Other Categories
Other Devices
400
300
200
100
0
1998
2003
2008
2013
2018
2023
EAL5+
EAL5
Other 14 categories
ICs, Smartcards
998
2003
2008
2013
2018
2023

Few major observations from reference analyses

- Top-10 products are used in 16% of all active smartcards.
  - These are microcontrollers, typically with cryptographic functionality.
- Higher reach is positively associated with higher evaluation assurance level.
- A vulnerability in cryptographic functionality would spread from high-reach devices to approx. 70% of their dependants.
  - Affecting 50+ certified products, RoCA was not an outlier.

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
- Dokumenty jsou často nekvalitně zpracované/chybné

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