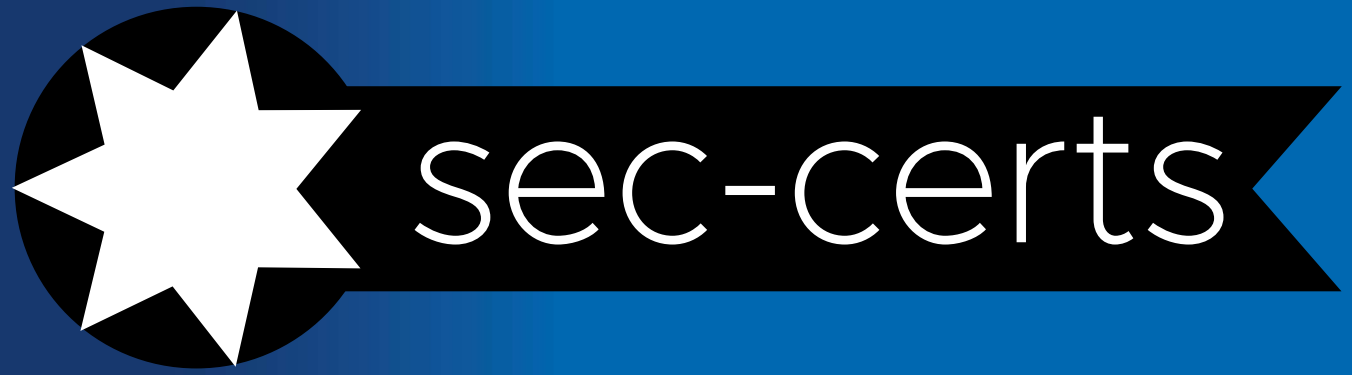


1) Process, Proof, and Practice: Common Criteria Security Certification

2) The Reality of Certified Security: Mining the CC and FIPS Ecosystems with sec-certs

Vashek Matyas *matyas@fi.muni.cz*

Centre for Research on Cryptography and Security, Masaryk University, Czechia

Joint work with Petr Svenda, Jan Jancar, Adam Janovsky, Yakup Y Demircan, Mariia Bakhtina, Martin Ukrop, Milan Broz, Jaroslav Reznik, and many others (thank you all!)

CROCS
Centre for Research on Cryptography and Security

COMMON CRITERIA 101

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

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

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 a TOE meets the SFRs (CC v3.1)
  - 7 levels (EAL1 < EAL7)
  - Hierarchical system – higher or new components

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

Certification of IT products – pros

- **Quality assurance**: Product meets certain industry standards (e.g., security, compatibility, performance).
- **Interoperability**: Guaranteed compatibility with other certified systems.
- **Market trust**: Viewed as more reliable and safer by customers and partners.
- **Compliance**: Meeting legal or regulatory requirements.
- **Competitive edge**: Differentiation from competitors in the market.

Certification of IT products – cons

- **Cost**: Testing fees, labs, paperwork, consultant costs.
- **Time-consuming**: Often extensive testing and review periods.
- **Maintenance overhead**: Re-certification when products or standards change.
- **Limited innovation**: Some products may have to sacrifice experimental features or design flexibility.
- **Fragmentation**: Different markets/regions with different certifications, creating complexity (e.g., CE in Europe vs. FCC in the US).

ChatGPT dialogue I

`Few real-world examples of famous product certifications in IT`

1. Wi-Fi CERTIFIED™ (Wi-Fi Alliance)
2. FCC certification (US Federal Communications Commission)
3. **Common Criteria certification (ISO standard for IT security)**
4. UL (Underwriters Laboratories) certification
5. **PCI DSS compliance certification (for payment systems)**

ChatGPT dialogue II

Examples of worst failures in the IT industry despite certifications

1. Intel Pentium FDIV Bug (1994)
2. Samsung Galaxy Note 7 Battery Explosions (2016)
3. **Heartbleed Bug in OpenSSL (2014)**
4. **Healthcare.gov Launch (2013)**
5. Therac-25 Radiation Machine (1985-87)

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 a TOE meets the SFRs (CC v3.1)
  - 7 levels (EAL1 < EAL7)
  - Hierarchical system – higher or new components

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

- The following slides present 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	4	4	0	0	0	0	0	0	0	0	0	0	0	25	0	33
Canada	0	0	0	0	19	0	1	0	8	0	0	0	0	0	0	0	105	0	133
Germany	7	0	3	11	11	7	42	5	83	2	17	0	51	0	1	0	1	0	241
Spain	4	2	0	11	12	0	4	2	19	1	10	0	1	0	0	0	9	0	75
France	0	0	0	0	23	0	4	1	83	4	238	2	67	4	0	0	0	0	426
India	1	0	0	7	1	1	0	0	0	0	0	0	0	0	0	0	0	0	10
Italy	0	1	1	1	13	0	3	0	27	0	2	0	0	0	0	0	19	0	67
Japan	7	0	0	16	10	0	0	0	0	0	0	0	0	0	0	0	76	0	109
Republic of Korea	0	6	1	4	0	0	0	0	2	0	4	0	0	0	0	0	34	1	52
Malaysia	0	5	0	9	5	0	0	0	0	0	0	0	0	0	0	0	0	0	19
Netherlands	7	0	0	1	16	0	11	5	116	7	89	0	52	0	1	0	0	0	305
Norway	0	0	0	0	0	0	0	1	4	0	4	0	0	0	0	0	0	0	9
Poland	0	0	0	1	0	1	0	1	2	0	0	0	0	0	0	0	0	0	5
Qatar	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Sweden	24	1	2	12	15	3	10	2	9	0	0	0	0	0	0	0	1	0	79
Singapore	0	0	0	2	7	0	0	0	9	0	0	0	0	0	0	0	0	0	18
Turkey	0	0	0	2	0	0	0	0	9	0	1	0	0	0	0	0	0	0	12
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	182	0	182
Totals:	**50**	**16**	**7**	**82**	**136**	**12**	**75**	**17**	**371**	**14**	**365**	**2**	**171**	**4**	**2**	**0**	**452**	**1**	**1777**

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	**B**	**EAL1**	**EAL1+**	**EAL2**	**EAL2+**	**EAL3**	**EAL3+**	**EAL4**	**EAL4+**	**EAL5**	**EAL5+**	**EAL6**	**EAL6+**	**EAL7**	**EAL7+**	**M**	**N**	**S**	**Total**
Australia	0	0	0	4	4	0	0	0	0	0	0	0	0	0	0	0	25	0	33
Canada	0	0	0	0	19	0	1	0	8	0	0	0	0	0	0	0	105	0	133
Germany	7	0	3	11	11	7	42	5	83	2	17	0	51	0	1	0	1	0	241
Spain	4	2	0	11	12	0	4	2	19	1	10	0	1	0	0	0	9	0	75
France	0	0	0	0	23	0	4	1	83	4	238	2	67	4	0	0	0	0	426
India	1	0	0	7	1	1	0	0	0	0	0	0	0	0	0	0	0	0	10
Italy	0	1	1	1	13	0	3	0	27	0	2	0	0	0	0	0	19	0	67
Japan	7	0	0	16	10	0	0	0	0	0	0	0	0	0	0	0	76	0	109
Republic of Korea	0	6	1	4	0	0	0	0	2	0	4	0	0	0	0	0	34	1	52
Malaysia	0	5	0	9	5	0	0	0	0	0	0	0	0	0	0	0	0	0	19
Netherlands	7	0	0	1	16	0	11	5	116	7	89	0	52	0	1	0	0	0	305
Norway	0	0	0	0	0	0	0	1	4	0	4	0	0	0	0	0	0	0	9
Poland	0	0	0	1	0	1	0	1	2	0	0	0	0	0	0	0	0	0	5
Qatar	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Sweden	24	1	2	12	15	3	10	2	9	0	0	0	0	0	0	0	1	0	79
Singapore	0	0	0	2	7	0	0	0	9	0	0	0	0	0	0	0	0	0	18
Turkey	0	0	0	2	0	0	0	0	9	0	1	0	0	0	0	0	0	0	12
United States	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	182	0	182
Totals:	**50**	**16**	**7**	**82**	**136**	**12**	**75**	**17**	**371**	**14**	**365**	**2**	**171**	**4**	**2**	**0**	**452**	**1**	**1777**

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)

FIPS 140-2 / 140-3

- Cryptographic modules validation
  - Algorithm, modules and entropy certificates
- Limited set of approved algorithms and parameters (AES…)
- NIST/CCCS CAVP and CMVP
- Validation scenarios
- FIPS 140-2 certificates to expire this September!

Challenges of security certifications

- Lack of transparency
- Expensive
- Sloooow

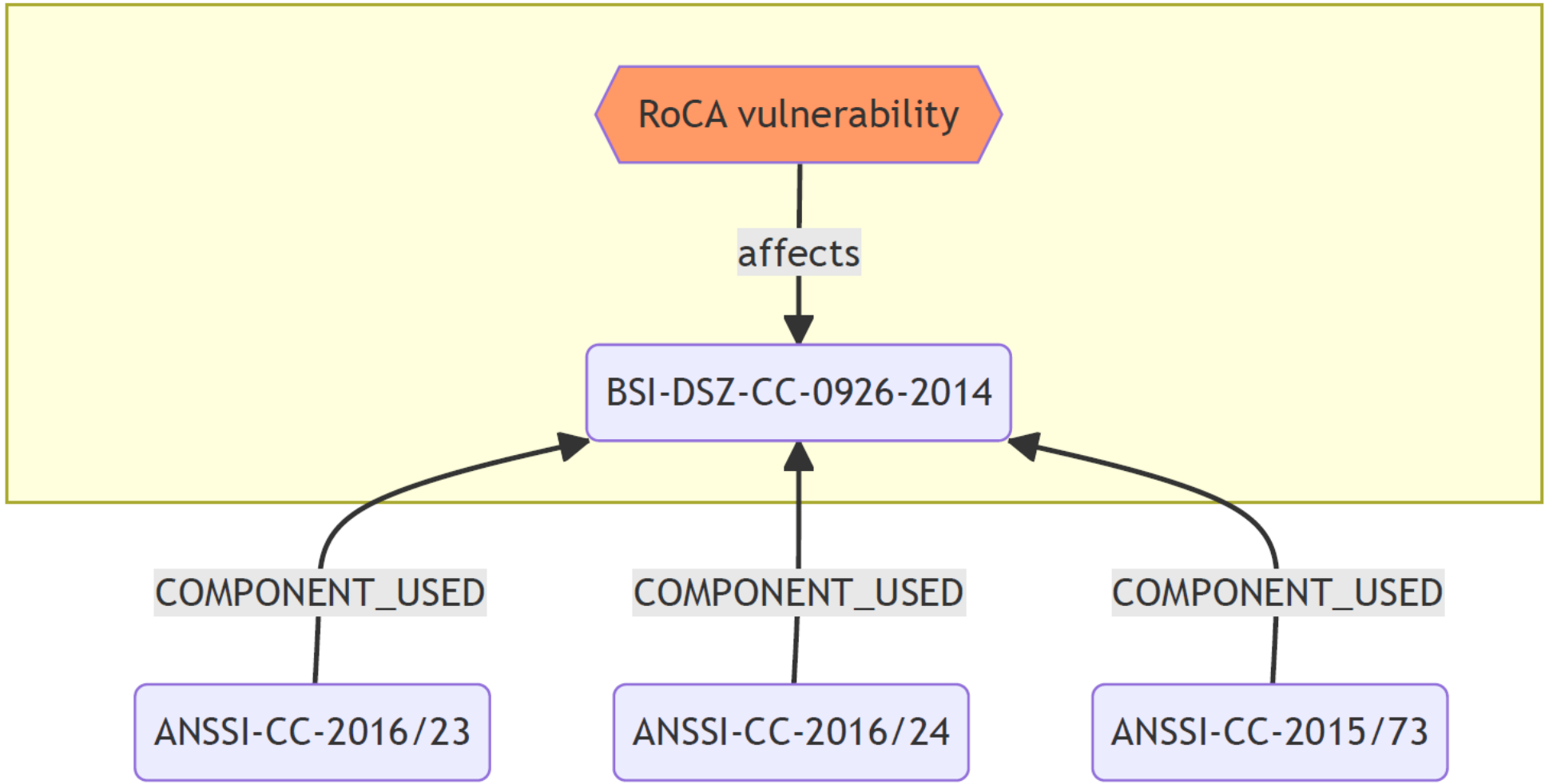
WHY DID WE CARE (AGAIN) ABOUT CC?

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?

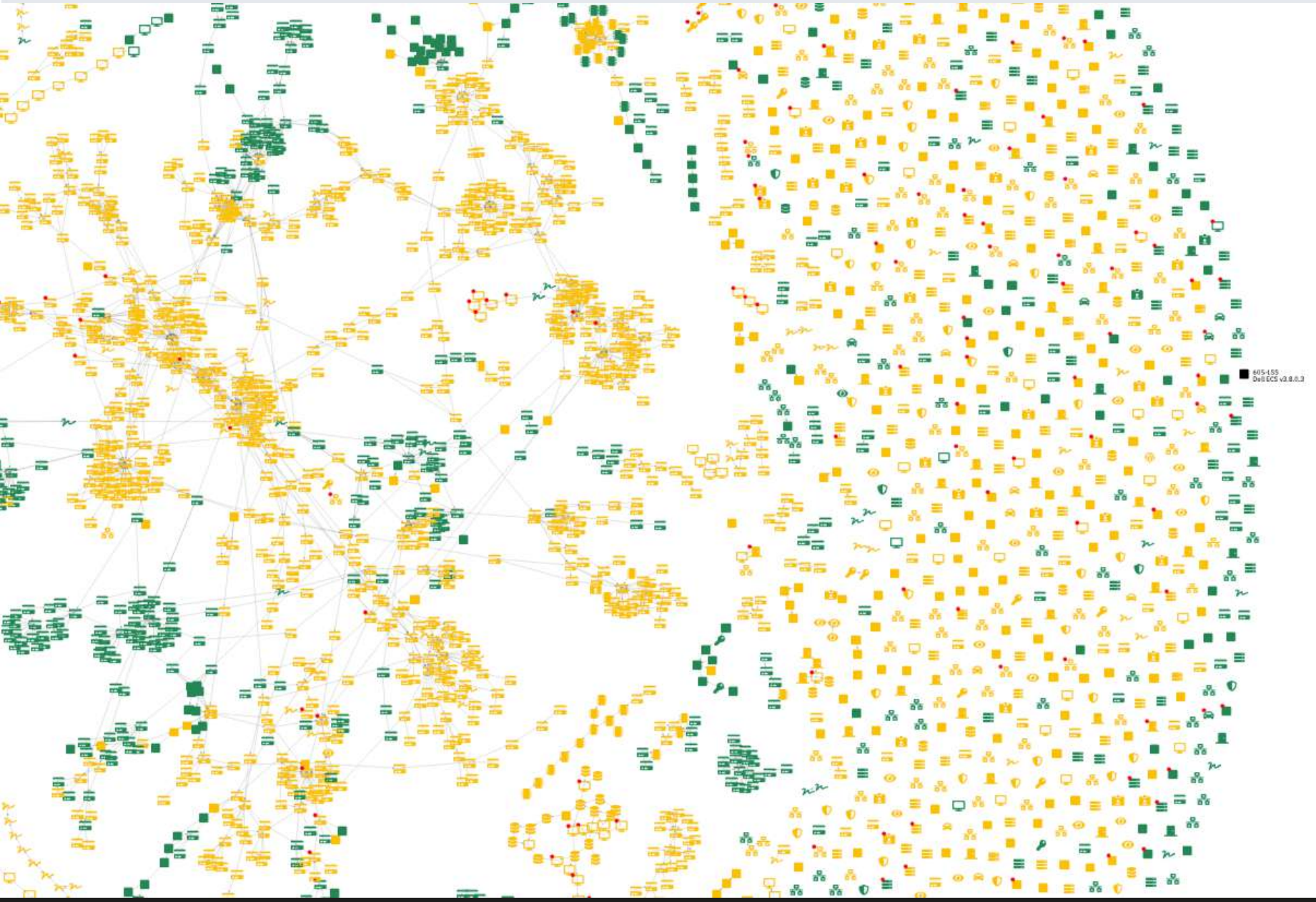
CVE-2017-15361



Common Criteria – certified products/systems

- FIPS 140
  - 5000 (Aug ‘26)
    - 1100 valid

1777 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems	21	139
Biometric Systems and Devices	2	3
Boundary Protection Devices and Systems	38	228
Data Protection	47	209
Databases	9	89
Detection Devices and Systems	6	75
ICs, Smart Cards and Smart Card-Related Devices and Systems	749	1494
Key Management Systems	5	53
Mobility	42	96
Multi-Function Devices	220	531
Network and Network-Related Devices and Systems	227	730
Operating Systems	43	213
Other Devices and Systems	304	869
Products for Digital Signatures	50	137
Trusted Computing	14	57
Totals:	**1777**	**4923**
	Grand Total:	**6700**



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.

Common Criteria

NIST FIPS 140-2/3

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

Base Score: 8.8 HIGH

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

Main functionality of *sec-certs.org* project

- Fulltext search over all CC and FIPS 140 certificates
- Continuous insight into certification ecosystem
- Extracted graph of references between certificates
- Mapping to NIST National Vulnerability Database (CVEs)
- Automatic notification of events for observed certificates (RSS feed)
- Correlation of certification requirements and vulnerability occurrence
- Python API for custom queries, preprocessed datasets for downloads
- Connecting additional metadata about certified items (tests, information)
- Local processing with inclusion of non-public documents

Users of the sec-certs.org tool

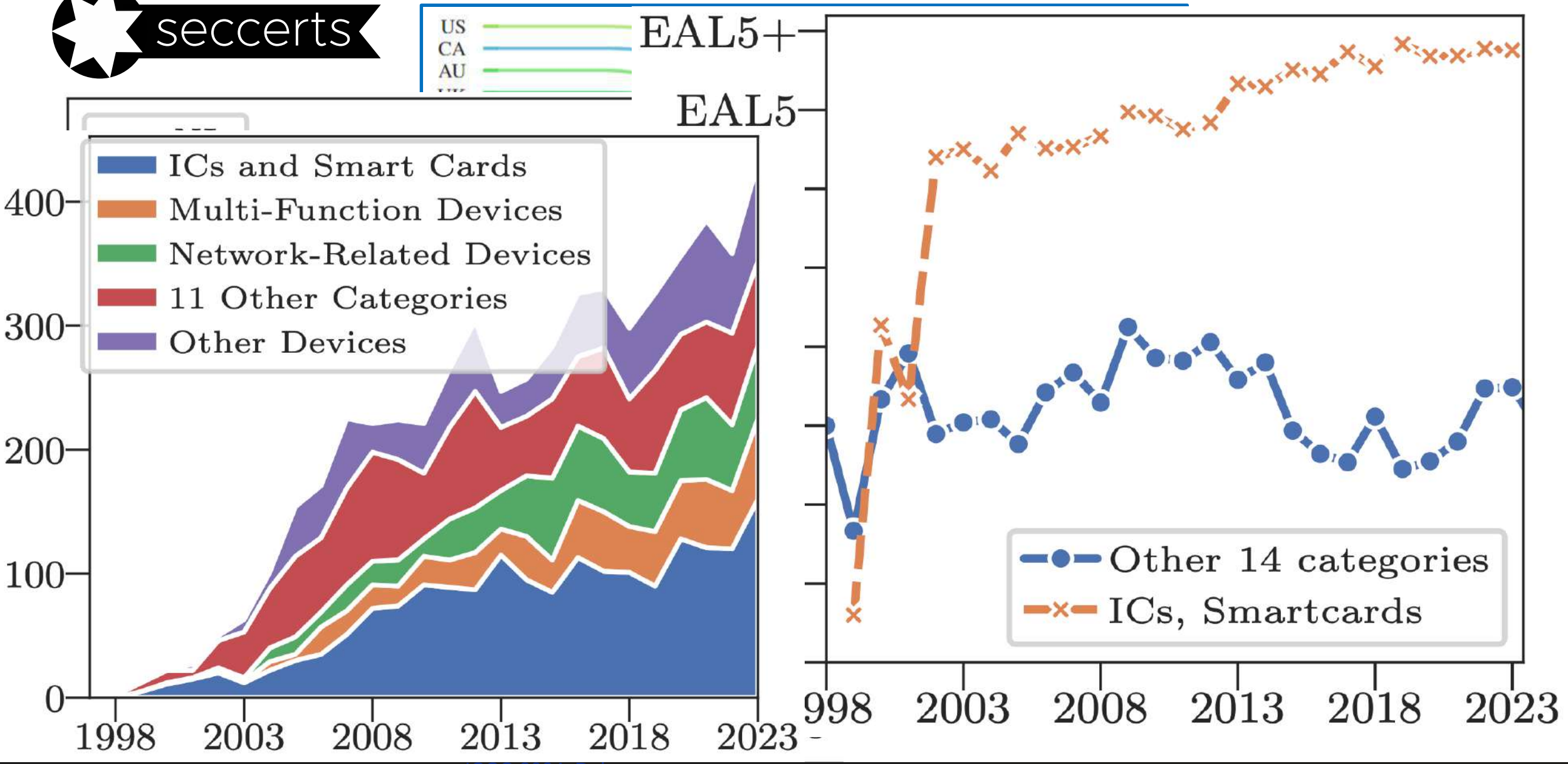
- Owners/users of certified devices / security researchers
  - What security claims are made?
  - What certificates to additionally monitor?
  - Notification after new (possibly relevant) vulnerability is found
  - Analyze impact of vulnerability (e.g., RoCA case)
- Vendors of certified products
  - Are we under/over certifying with respect to competition?
  - Who is certifying products of our type and what were requirements in past?
- Certification bodies
  - Performance of labs, suspiciously short validity, non-standard cert. claims…
  - Impact of certification requirements (SARs) on the actual security

Users of the sec-certs.org tool

- Certification laboratories
  - Are we comparable with other laboratories? What are the trends?
- Government agencies & corporations
  - Processing additional non-public documents
  - Attaching additional metadata (test results, powertrace…) and its governance
    - Generate sec-certs “web” locally with additional information
- General public
  - Easy access to information (interactive webpage, info from multiple sources…)
  - Ecosystem insights: What is standardized? Change in time?

VARIOUS ECOSYSTEM INSIGHTS

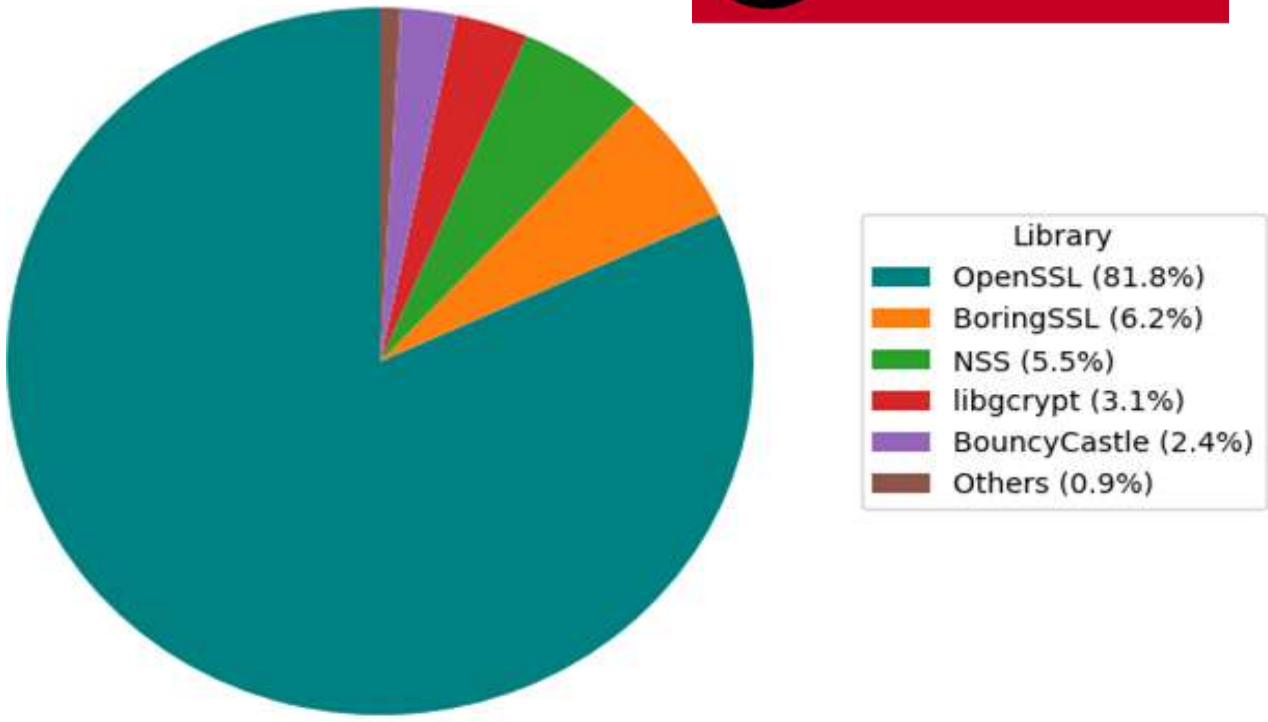
seccerts


US
CA
AU
EAL5+
EAL5
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
Other 14 categories
ICs, Smartcards

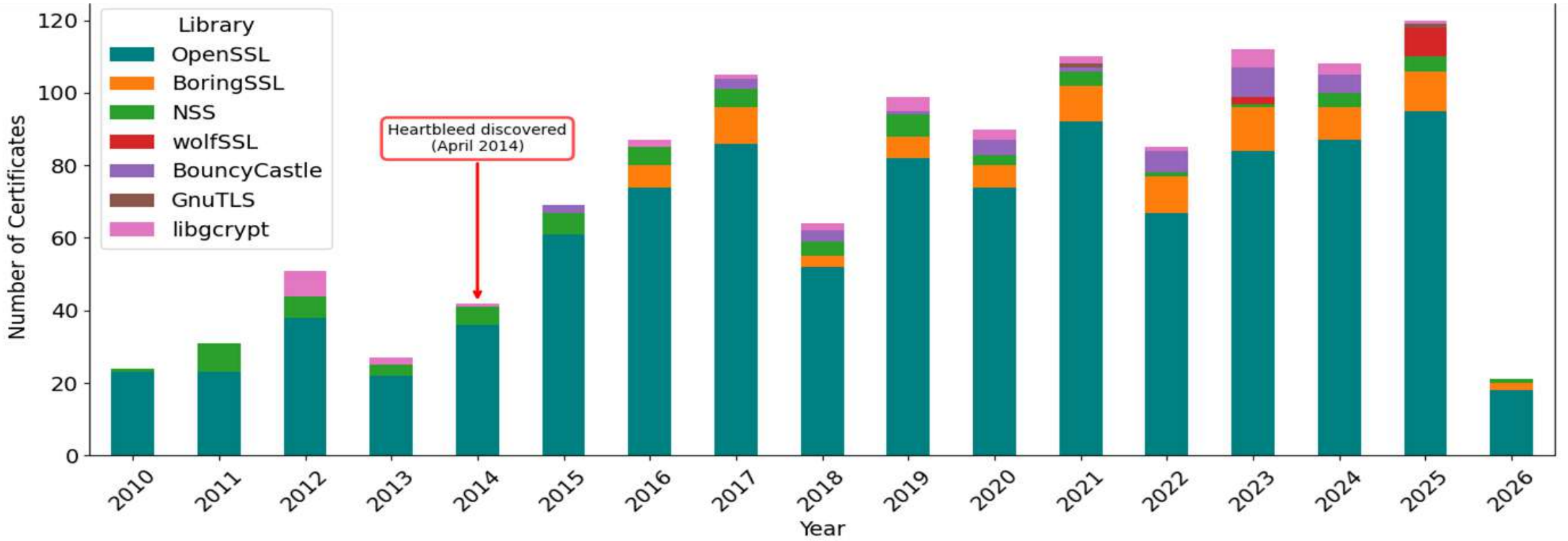
OpenSSL dominance

OpenSSL dominance in security certifications

- 17% Common Criteria
- 16% FIPS 140



Appearance of OpenSSL alternatives

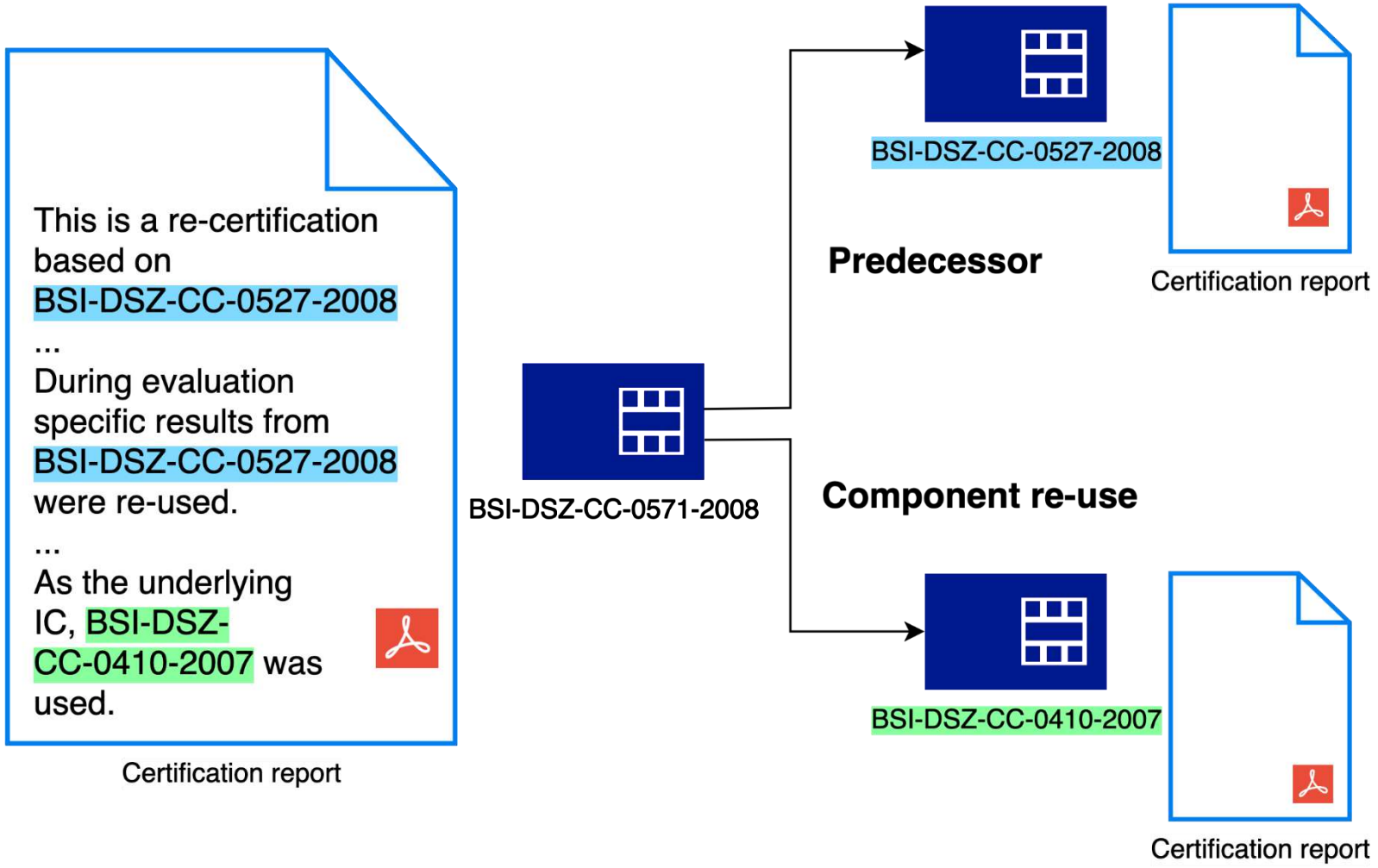


REFERENCES, REFERENCES, REFER…

Building the reference graph

- Each device is a **vertex**.
- A reference from device A to device B is a **directed edge**.
  - The reference is indicated by the presence of a foreign certificate ID within the artifacts.
- The categorical context of the reference, e.g. `COMPONENT_USED`, is an **edge label**.
- We worked with 5780 vertices and 3007 edges.

Building the reference graph

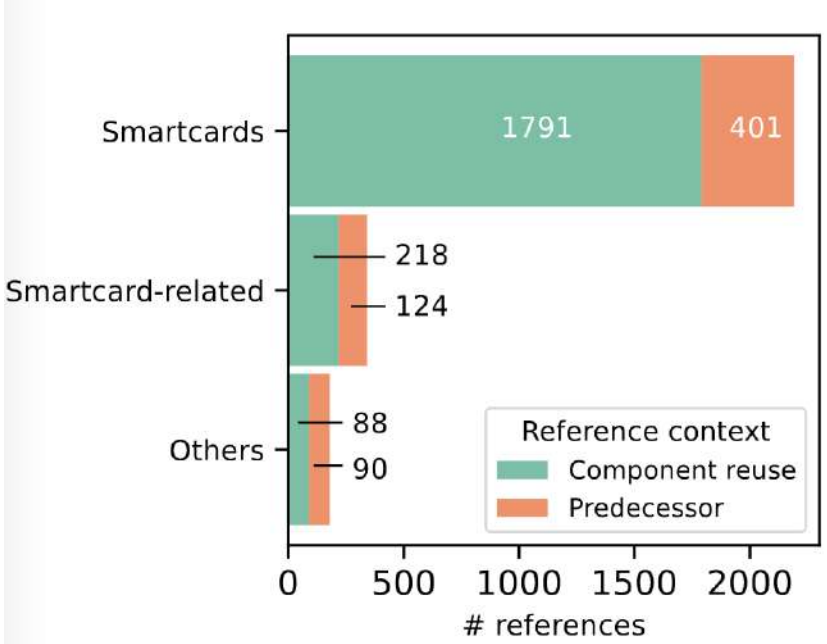


Inferring reference contexts

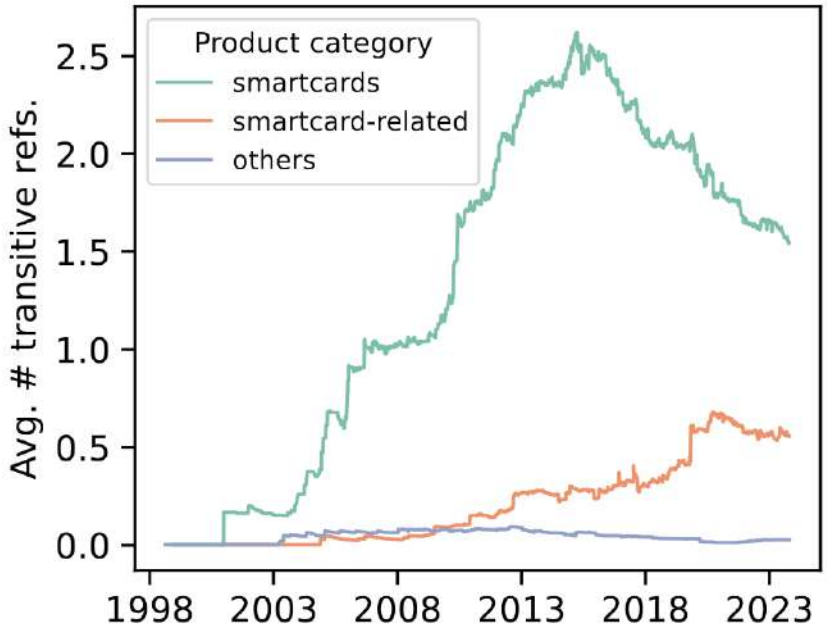
- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`
  - Component used (C)
  - Component shared (C)
  - Evaluation reused (C)
  - Re-evaluation (P)
  - Previous version (P)

- *75% of references constitute real dependencies, 25% are predecessor references.*

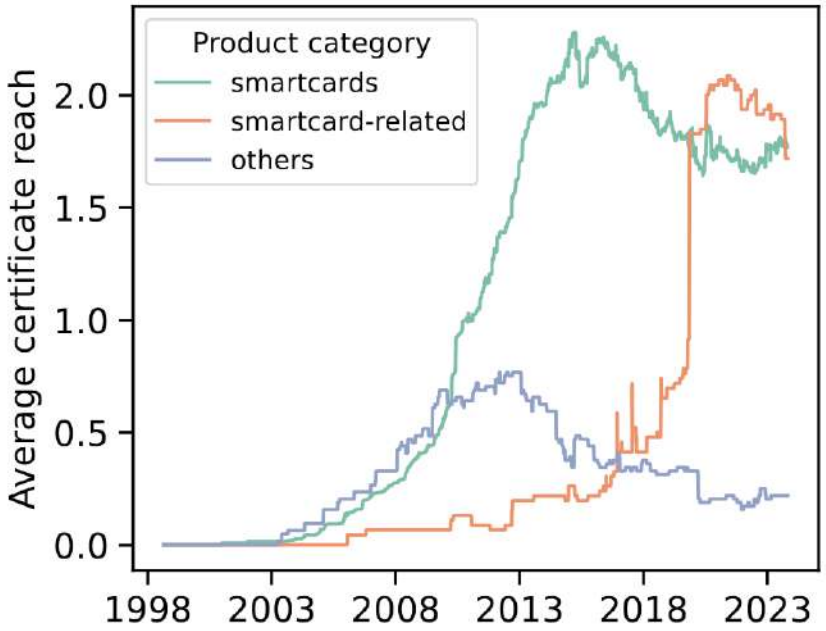
Ecosystem trends



(a) Reference context freq.



(b) Avg. # trans. refs



(c) Average product reach

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.

In a nutshell

- We have developed a pipeline for automated processing of Common Criteria artifacts.
  - We also cover FIPS 140, EUCC and NVD vulnerability DB.
  - Mapping of dependencies among certificates
  - Continuous insights into certification ecosystem
  - Support for more transparency in security certifications

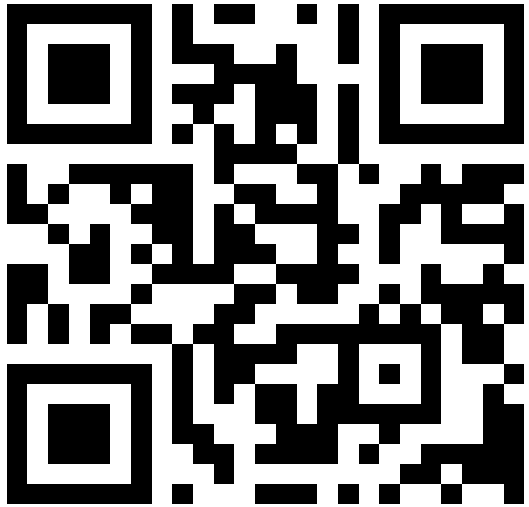
- The analysis is tedious due to artefacts *produced by humans and meant to be consumed by humans*.

Come and play – with sec-certs!

CAT
CYBERSECURITY CERTIFICATION AND ASSESSMENT TOOLS

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Cyber Security for Europe



https://sec-certs.org/

sec-certs: Examining the security certification practice for better vulnerability mitigation (article)

Revisiting the analysis of references among Common Criteria certified products