



Enhancing Transparency: Insights From the Common Criteria Certification Ecosystem

Vashek Matyas  matyas@fi.muni.cz

Centre for Research on Cryptography and Security, Masaryk University

Joint work with Petr Svenda, Jan Jancar, Adam Janovsky, Martin Ukrop, Stanislav Bobon, Martin Fryan, Milan Broz, Jaroslav Reznik, and many others (thank you all!)

CRCS

Centre for Research on
Cryptography and Security

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




Base Score: **8.8 HIGH**

List of platforms and vulnerabilities (CPE, CVE)




Common Criteria



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


Common Criteria Certification portal
<https://www.commoncriteriaportal.org/>


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

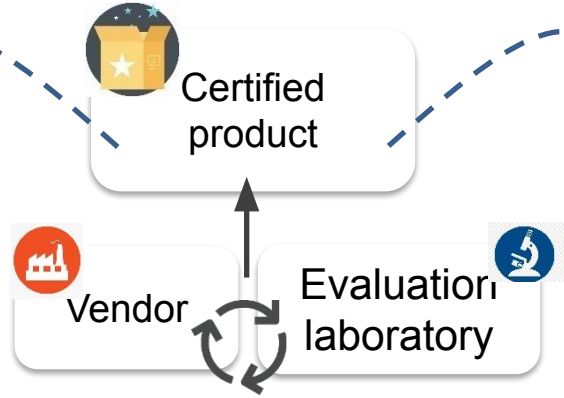
sec-certs git repository
<https://github.com/crocs-muni/sec-certs>

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


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

Extracted data (JSON) 

Analyses and visualizations 



NIST FIPS 140-2/3




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

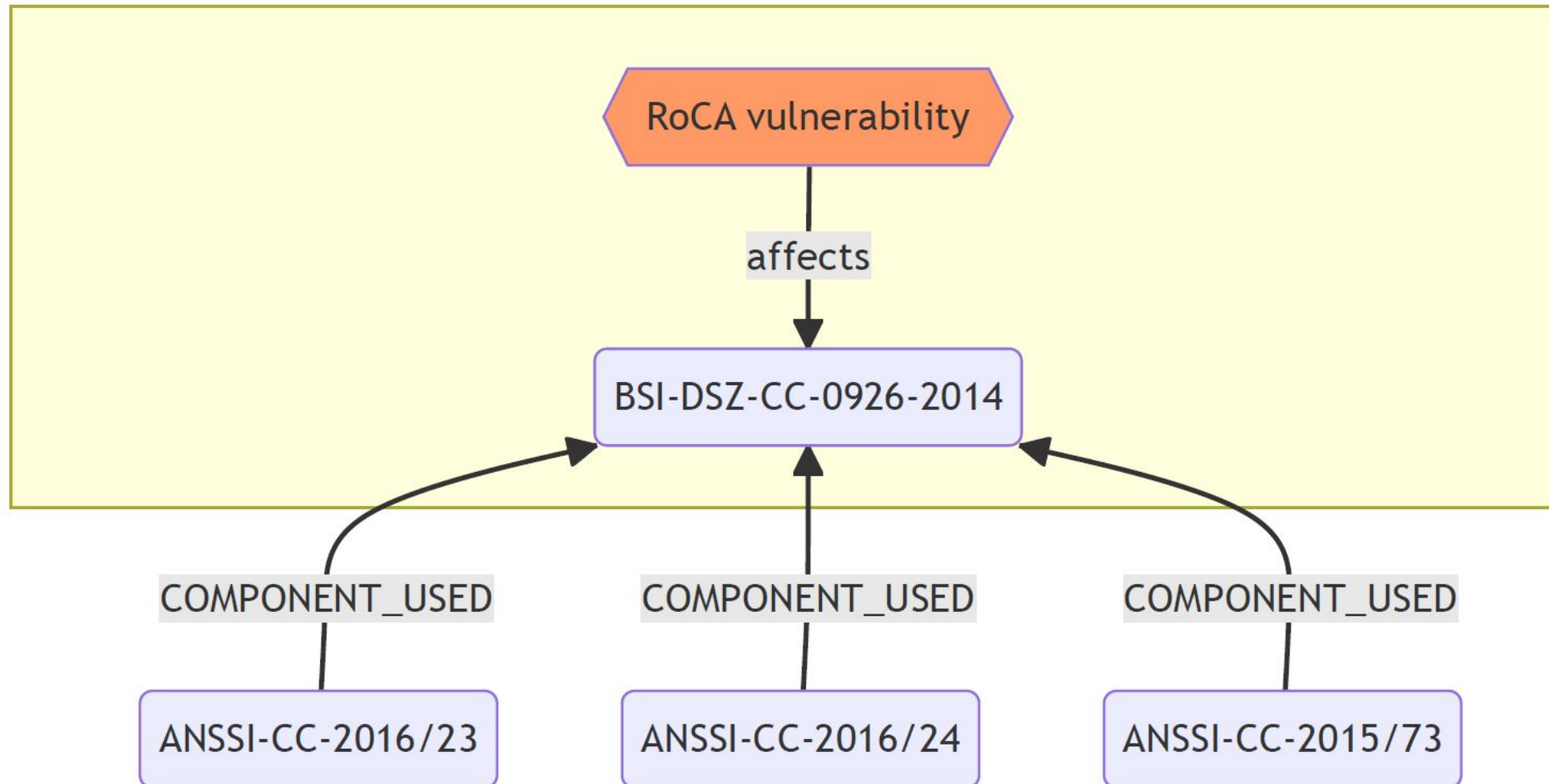
NIST CMVP portal

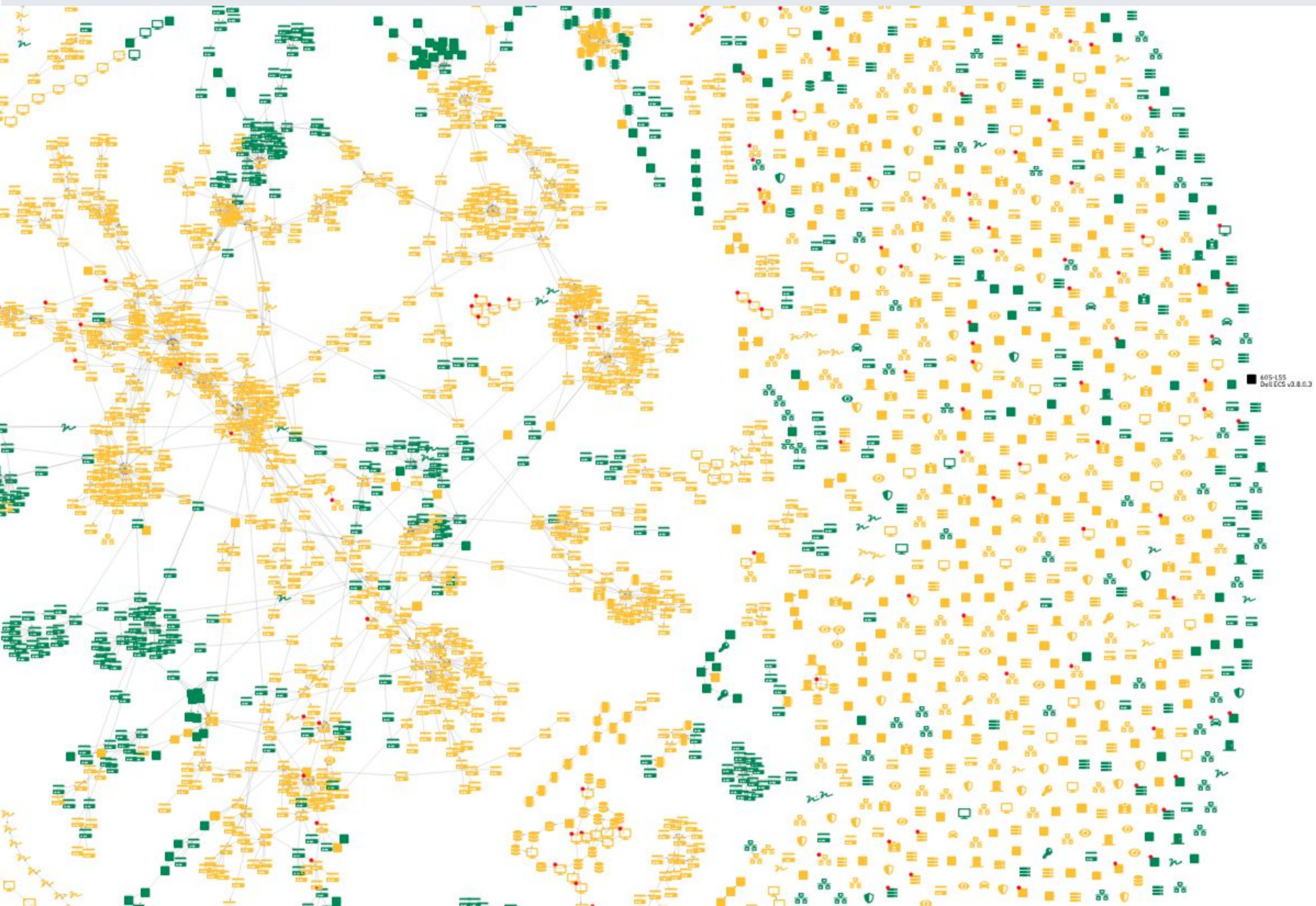
OUR INITIAL INTEREST – DEPENDENCIES

CVE-2017-15361 (RoCA)

- [CVE-2017-15361]: practical factorization of widely used RSA moduli.
- Billion+ devices affected.
-  How many devices certified under Common Criteria are impacted?

CVE-2017-15361

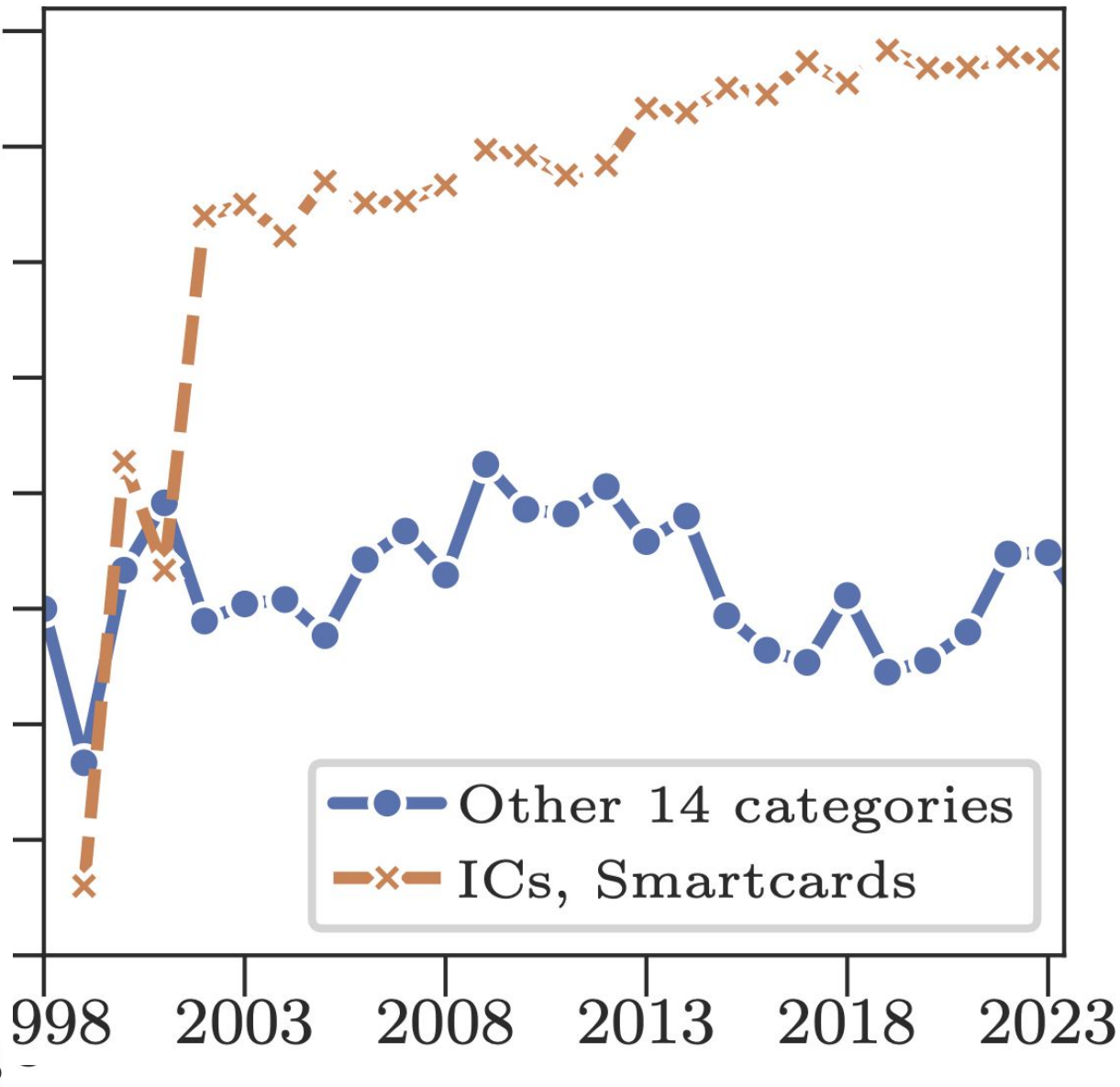
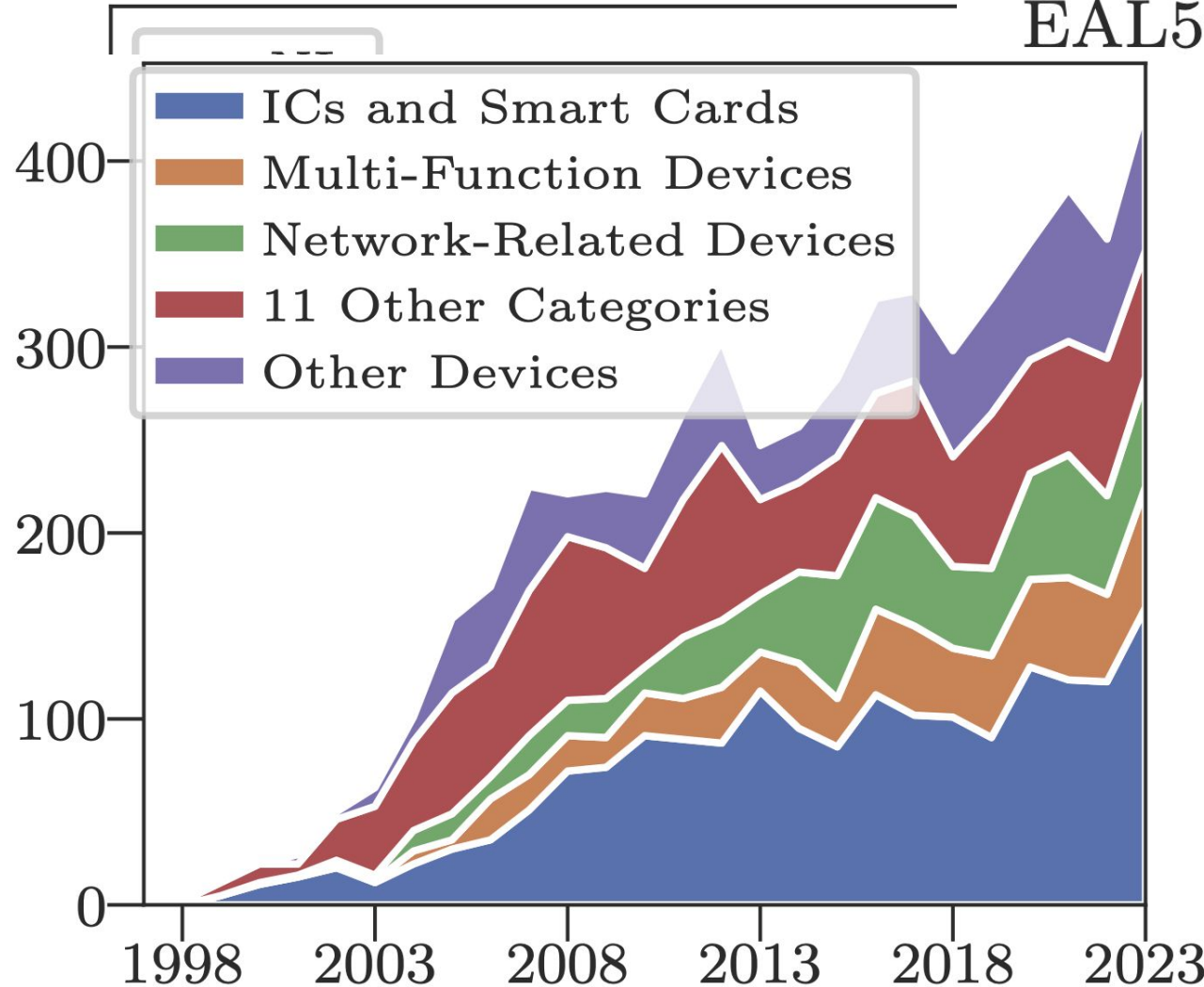




VARIOUS ECOSYSTEM INSIGHTS



US EAL5+
 CA
 AU
 ...

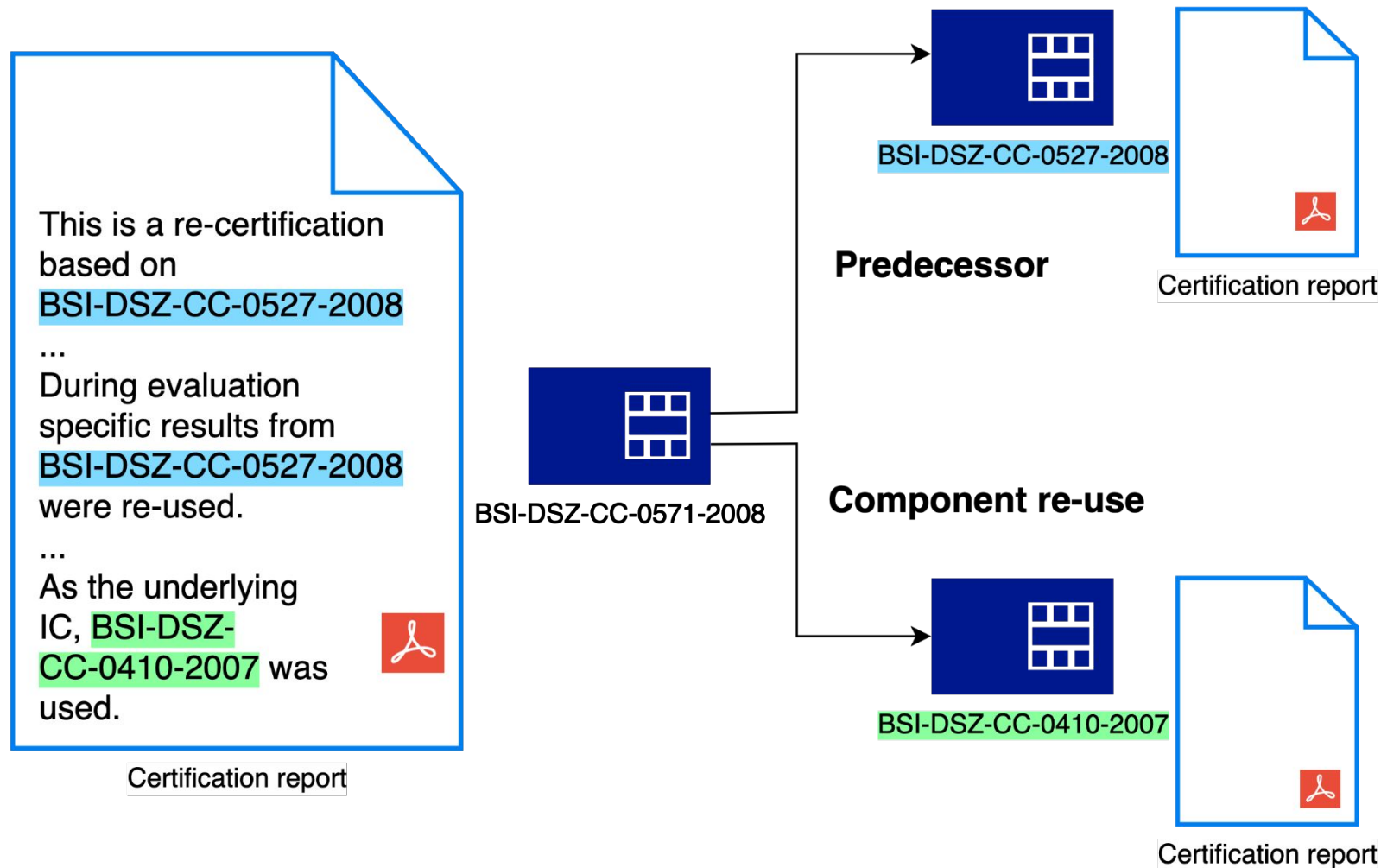


REFERENCES, REFERENCES, REFER...

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 5394 vertices and 2712 edges.

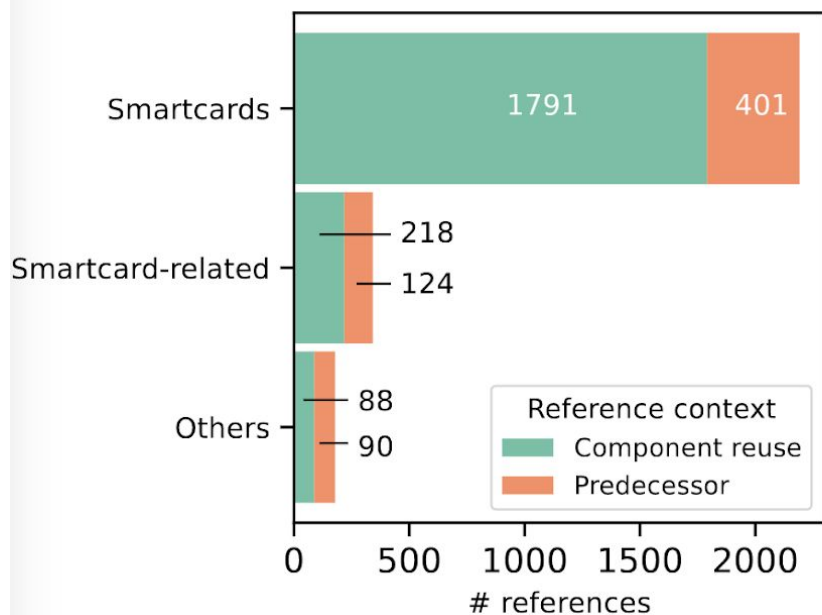
Building the reference graph



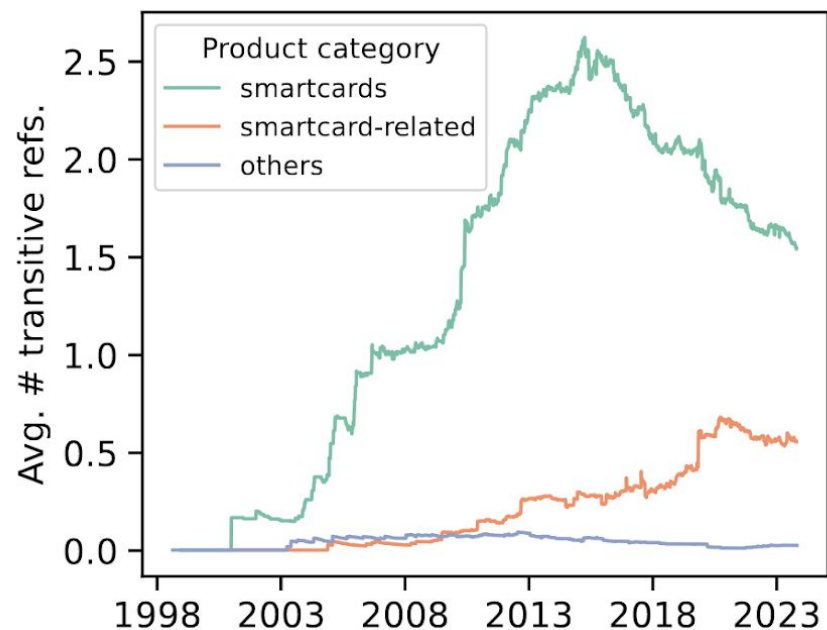
Inferring reference contexts

- Two major contexts: `COMPONENT_REUSE` & `PREDECESSOR`
 - Component used (C)
 - Component shared (C)
 - Evaluation reused (C)
 - Re-evaluation (P)
 - Previous version (P)
- Two co-authors annotated 400 references (15%), agreement 0.94.
- *75% of references constitute real dependencies, 25% are predecessor references.*

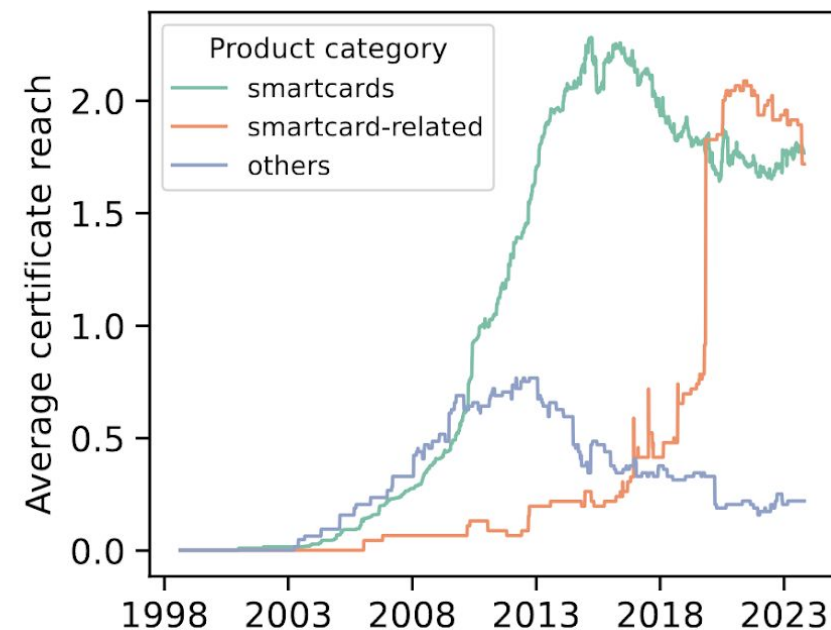
Ecosystem trends



(a) Reference context freq.



(b) Avg. # trans. refs

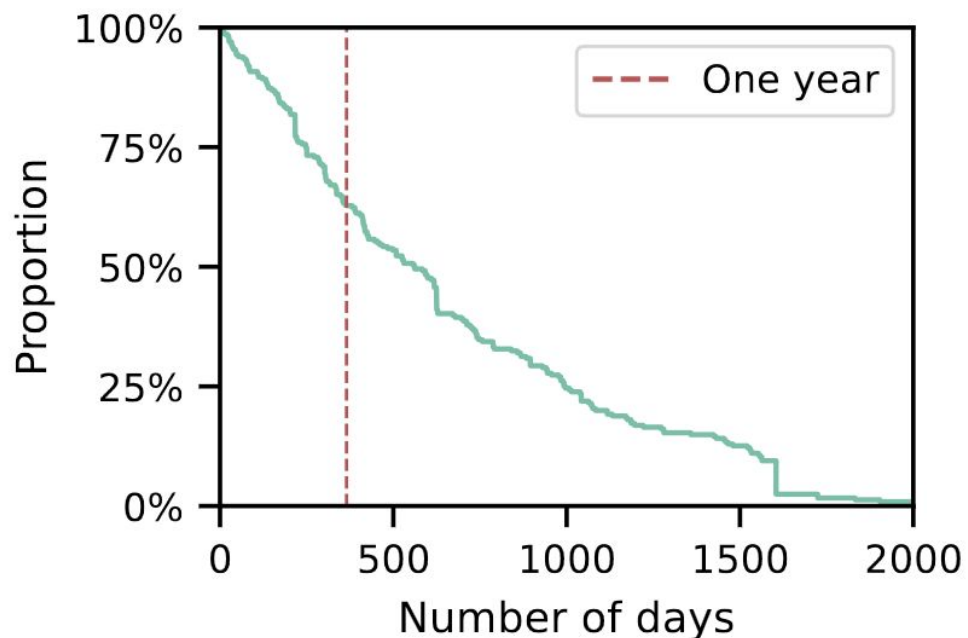


(c) Average product reach

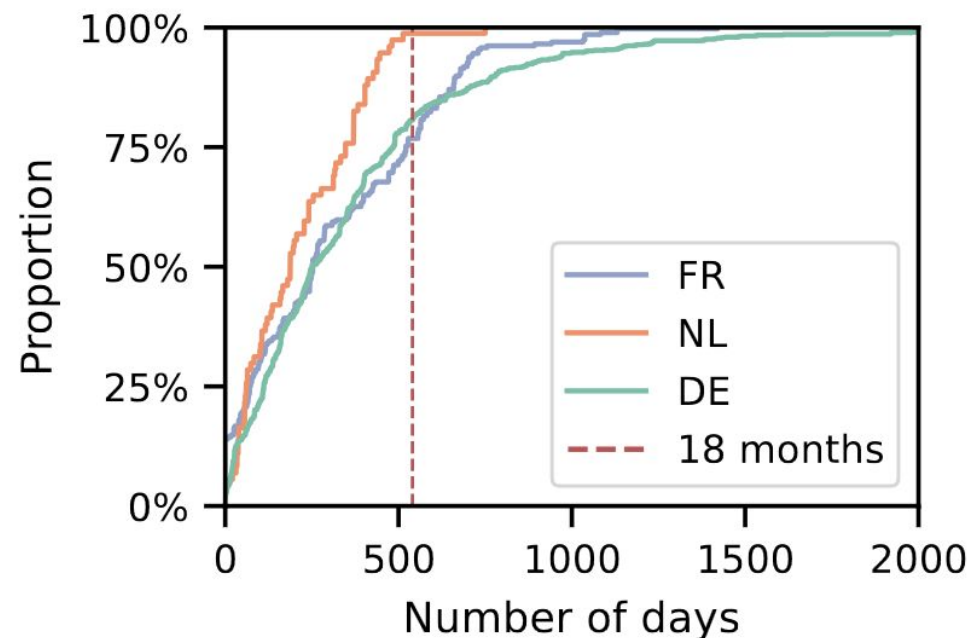
High-reach components

- Top-10 smartcards are used as (transitive) dependencies in 16% of all active smartcards.
 - These are microcontrollers, typically with cryptographic functionality.
- Higher reach is positively associated with higher evaluation assurance level.
- We also measured that a vulnerability in cryptographic functionality would spread from high-reach devices to approx. 70% of their dependants.

Ageing references



(a) Ratio of component-reuse referenced certificates with > 0 reach at n days post-archival (only includes products with positive reach on the date of their archival).



(b) CDF: the age of the referenced certificate on the issuance date of the referencing certificate.

Few major observations from reference analyses

- Certified dependencies popular among smartcards, more than 10% of all smartcards depend on top-10 smartcards.
- Affecting 50+ certified products, RoCA was not an outlier.
- Actual dependencies can be inferred from inter-certificate references.

SEC-CERTS.ORG AS METADATA AGGREGATOR FOR MORE TRANSPARENT CERTIFICATION

sec-certs.org as other metadata aggregator

... any future metadata overlay

RSA/ECC keys analysis

ECTester ecc analysis

Power traces (SCRUTINY)

TPMAIlgTest

JCAIlgTest performance results

TRNG randomness assessment

CVE database

Certified items from Common Criteria,
FIPS140, EUCC, EMVCo...

sec-certs.org – more transparent security certification

- Automatic processing of existing Common Criteria and FIPS140 certs
- Proactive monitoring of security vulnerabilities (NVD/CVE database)
- Mapping of dependencies among certificates
- Continuous insights into certification ecosystem
- Support for more transparency in security certifications

FUNCTIONALITY AND NEXT STEPS

In a nutshell

- We have developed a pipeline for automated processing of Common Criteria artifacts.
 - We also cover FIPS 140 and NVD vulnerability DB.
- The analysis is tedious due to artefacts *produced by humans and meant to be consumed by humans*.

Main functionality of *sec-certs.org* project

- Fulltext search over all CC and FIPS140 certificates
- Visualized information combined from multiple sources (CC/NVD/csv/pdf...)
- 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

- General public
 - Easy access to information (interactive webpage, info from multiple sources...)
 - Ecosystem insights: What is standardized? Change in time?
- Owners/users of certified devices / security researchers
 - What security claims are made?
 - Which certificates to additionally monitor?
 - Notification after new (possibly relevant) vulnerability is found
 - Analyze impact of vulnerability (e.g., ROCA case)
- 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

- Government agencies
 - Processing additional non-public documents
 - Attaching additional metadata (test results, powertrace...) and its governance
 - Generate sec-certs “web” locally with additional information
- Certification laboratories
 - Are we comparable with other laboratories? What are the trends?
- Vendors of certified items
 - Are we under/over certifying with respect to competition?
 - Who is certifying products of our type and what were requirements in past?
- (Someone else?)

sec-certs.org next steps

- Extend metadata aggregator
- Finalize NLP-based references analysis (meaning of references)
- Further NLP-based analysis (ToE boundaries, exceptions...)
- Dashboard software for companies (certificates owned, security and maintenance notifications)
- Analysis of Protection Profiles
- Addition of certificates from more schemes (EMVCo, EUCC...)

Thank you for your attention!



Cyber-security Excellence Hub in
Estonia and South Moravia

