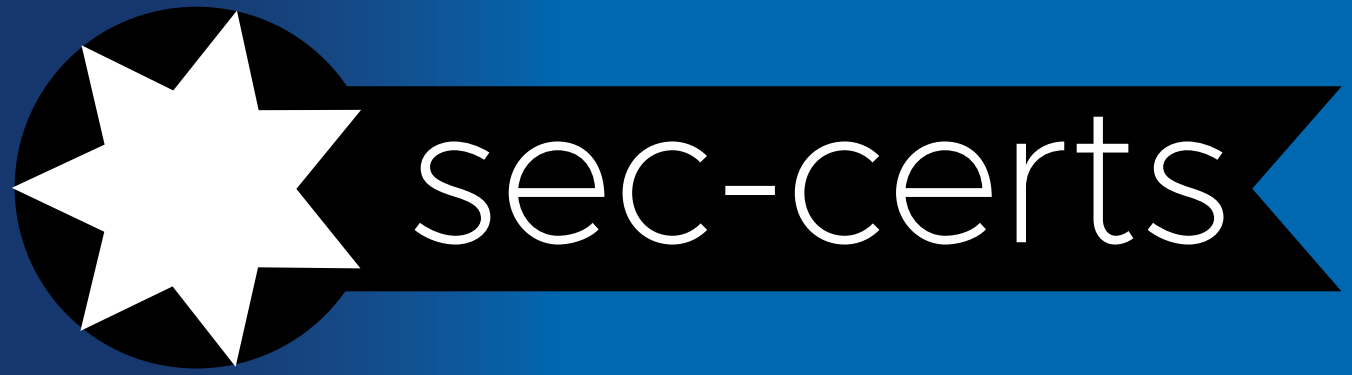


sec-certs: Insights from the world of certified computer security products and systems

Vashek Matyas & Petr Svenda ***matyas | svenda @fi.muni.cz***
Centre for Research on Cryptography and Security, Masaryk University, Czechia
Joint work with Jan Jancar, Adam Janovsky, Martin Ukrop, Stanislav Bobon, Martin Fryan, Milan Broz, Jaroslav Reznik, and many others (thank you all!)

CROCS
Centre for Research on Cryptography and Security

COMMON CRITERIA 101

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

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

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 – certified products/systems

- FIPS 140
  - 5000+
    - 950–1000 active today

1851 Certified Products by Category *		
Category	**Products**	**Archived**
Access Control Devices and Systems	22	138
Biometric Systems and Devices	2	3
Boundary Protection Devices and Systems	39	225
Data Protection	46	206
Databases	10	88
Detection Devices and Systems	6	74
ICs, Smart Cards and Smart Card-Related Devices and Systems	755	1437
Key Management Systems	7	51
Mobility	44	90
Multi-Function Devices	240	502
Network and Network-Related Devices and Systems	234	707
Operating Systems	41	208
Other Devices and Systems	327	827
Products for Digital Signatures	51	134
Trusted Computing	27	56
Totals:	**1851**	**4746**
	Grand Total:	**6597**

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

Let us show you (1) simple search and (2) LLM-based chat

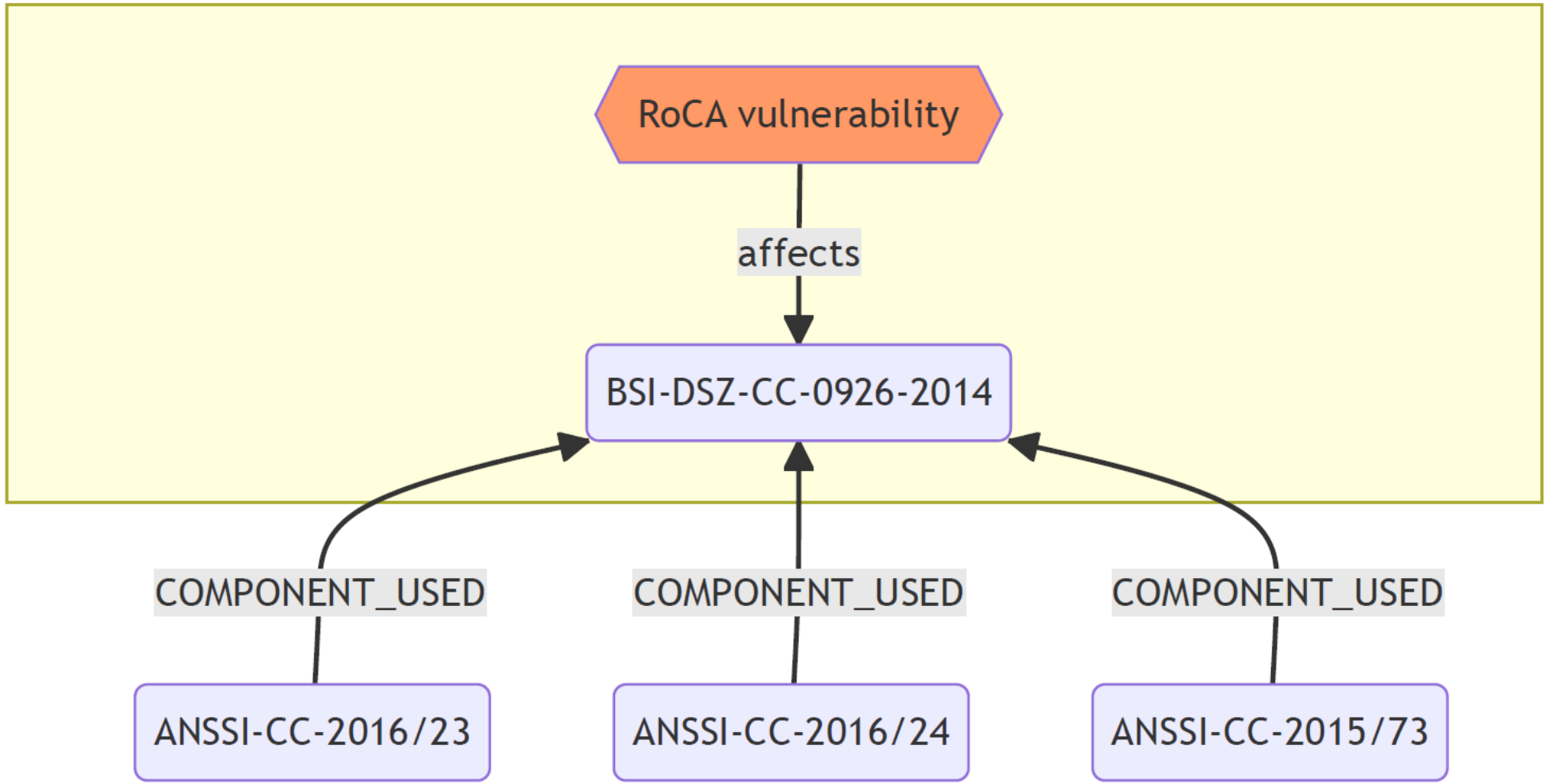
WHY DID WE CARE (AGAIN) ABOUT CC?

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

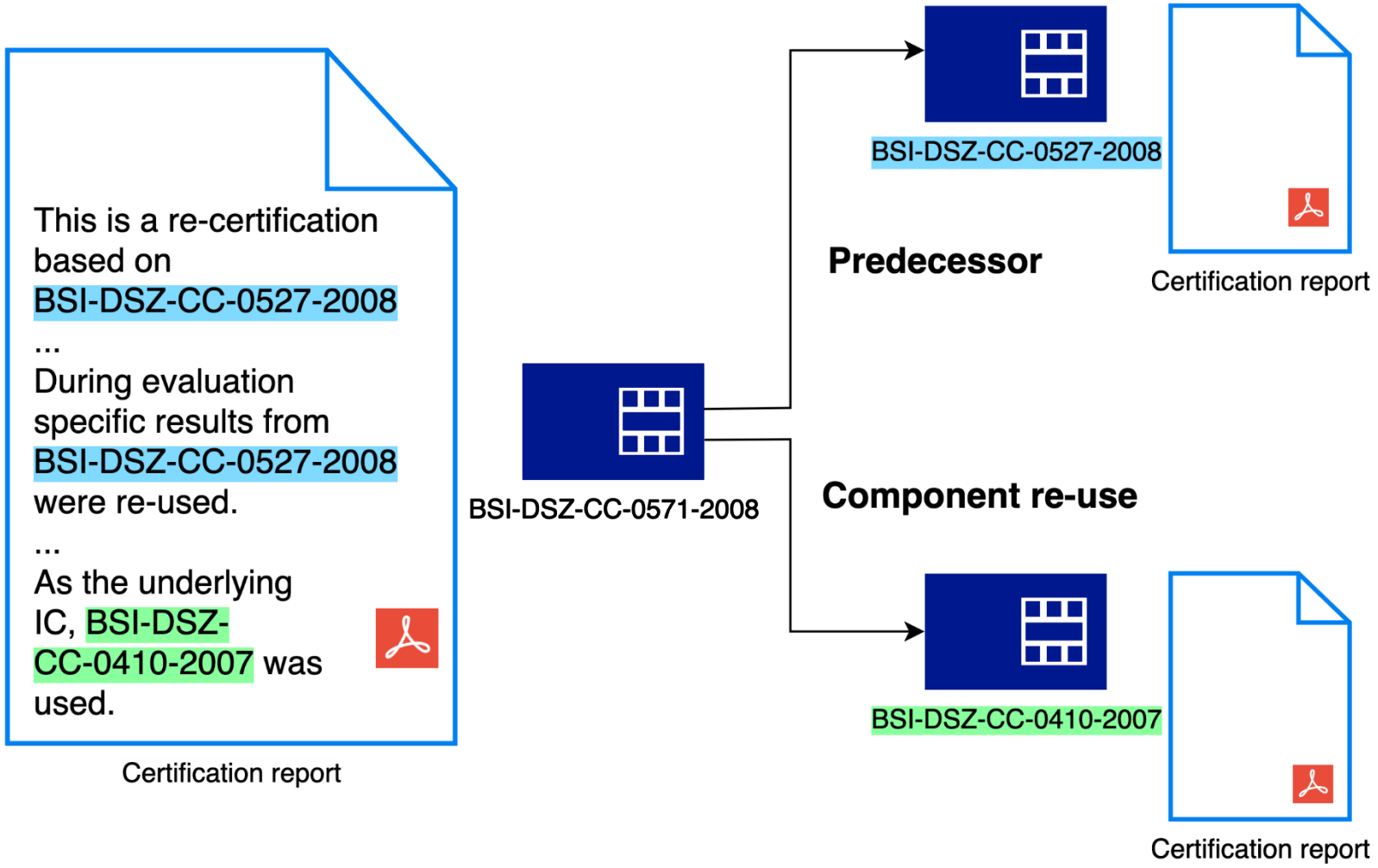


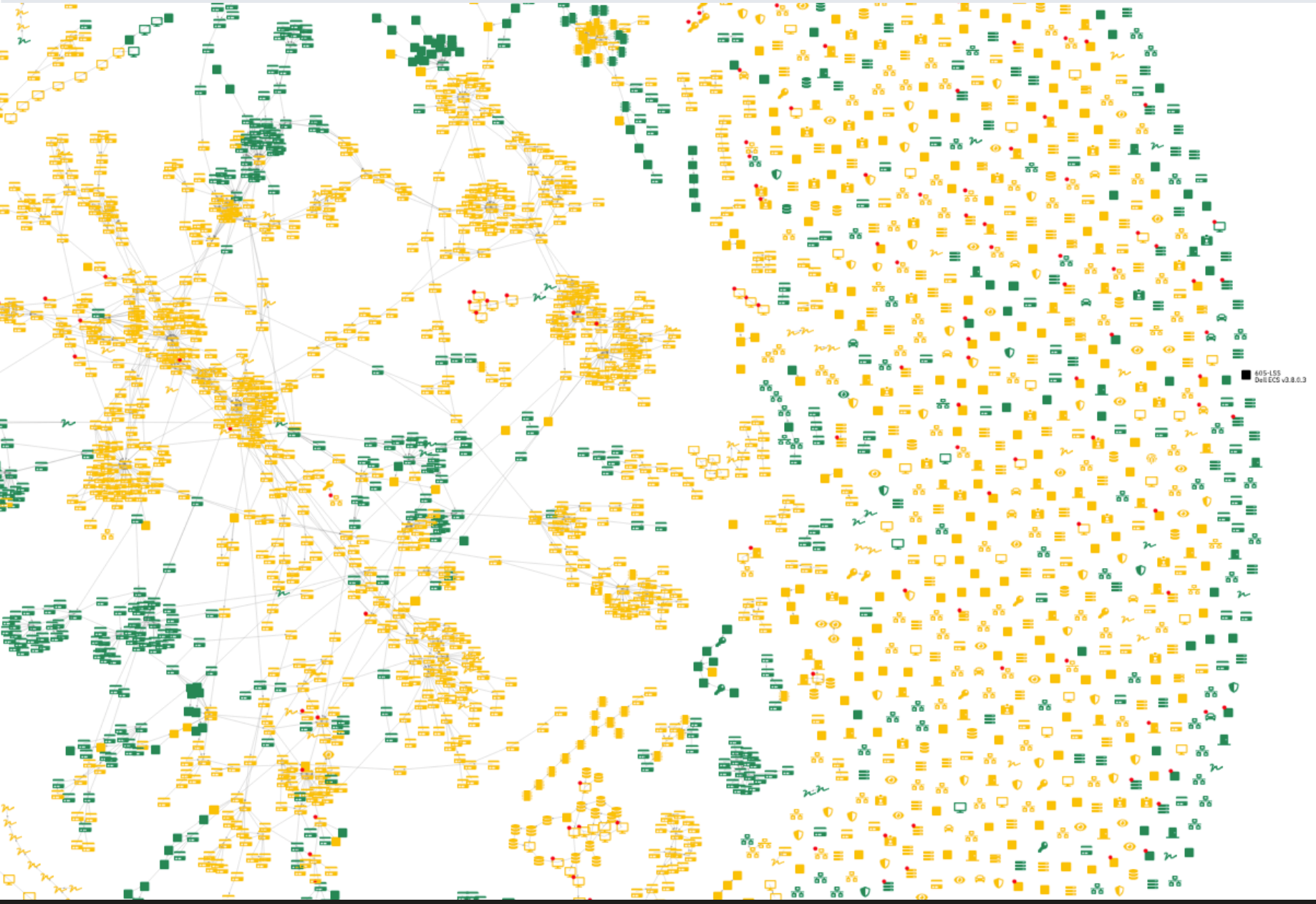
REFERENCES, REFERENCES, REFER…

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




605-LSS
Dell ECS v3.8.0.3

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.

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.

Let us see how (3) how two CC certificates differ.

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?

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

(4) Automatic updates from sec-certs & (5) Dashboarding

In a nutshell

- We have developed a pipeline for automated processing of Common Criteria artifacts.
  - We also cover FIPS 140 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*.

Thank you for your attention!

sec-certs

Cyber Security for Europe

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Red Hat

CAT

CYBERSECURITY CERTIFICATION AND ASSESSMENT TOOLS

Come and play – with sec-certs!

https://sec-certs.org/

Journal articles: