This work is distributed under the CC BY-SA license, unless stated otherwise.

Hardware Security

15. Certifications and Recap

Ján Jančár

Summer 2026

Today

- Assignment 3
- Course evaluation
- Security certifications
- Recap

Assignment 3

Congratulations everyone!

- Level 1: Many possible faults
- Level 2: Many possible faults
- Level 3: Many possible faults

Course evaluation

Please fill in the course evaluation.

Security certifications

Trust me bro, it is secure

Security certifications

Why?

- How do you get assurances of security?
  - Without trusting vendors
- Independent evaluation of security
- Certificate that a given product passed a given certification
- Certifications necessary in some sectors
  - Government use
  - Healthcare
  - Payments
  - Military

Security certifications

What?

- Globally: Common Criteria standard (CC)
- Globally (payments): EMVCo
- US: FIPS 140 standard
- EU: EUCC standard

Common Criteria

Process

- Certification that product adheres to some *Security Target*
  - Vendor pays and provides materials
  - Independent lab (ITSEF) evaluates
  - Certification body issues *Certificate* and *Certification Report*
  - Certificates released and internationally recognized
- Security target might point to a *Protection Profile* instead
  - Common set of requirements for a product class (e.g. a firewall PP)

What is not in the Security Target is not certified!

Common Criteria

Documents & Terms

Public documents

- **Security Target**: Vendor-authored, contains description of the product's security claims: functions (SFRs) and assurances (SARs)
  - Defines the **Target of Evaluation** (ToE)
- **Protection Profile**: Standardized, contains baseline requirements for a product class
- **Certification Report**: Certification body-authored, contains the results of the certification

Private documents

- Implementation docs
- User guidance
- Security target details

Common Criteria

Security claims

- **SFRs** (Security Functional Requirements)
  - What the product must do
  - Have a strong RNG, access control, RSA encryption, …
  - `FCS_RBG`, `FDP_ACC`, `FCS_COP`, …
- **SARs** (Security Assurance Requirements)
  - The measures taken to verify the SFRs
  - Independent testing, functional specification, vulnerability analysis, …
  - `ATE_IND`, `ADV_FSP`, `AVA_VAN`, …
- **EAL** (Evaluation Assurance Level)
  - Set of SARs
  - A scale of increasing assurance
  - EAL1 to EAL7

EAL1	Functionally tested
EAL2	Structurally tested
EAL3	Methodically tested and checked
EAL4	Methodically designed, tested, and reviewed
EAL5	Semiformally designed and tested
EAL6	Semiformally verified design and tested
EAL7	Formally verified design and tested

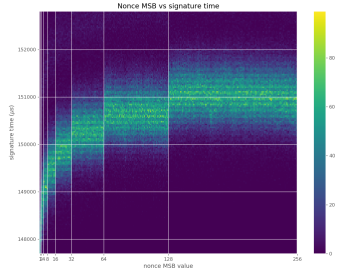
Common Criteria

Common pitfalls

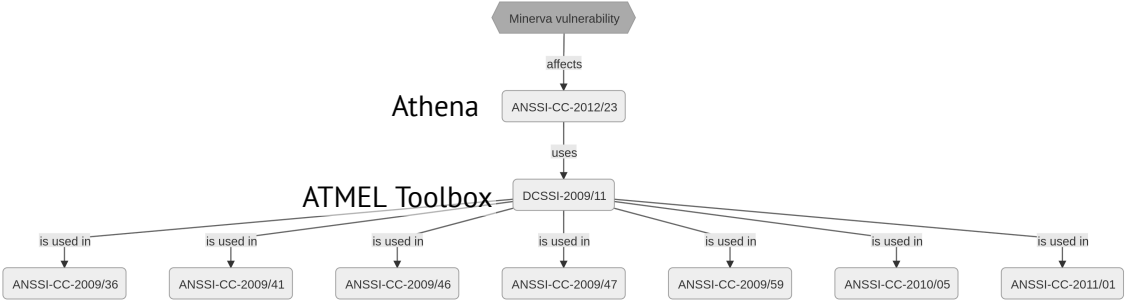
- Certification is costly
  - Only large vendors can afford it
- Certification takes time
  - Product becomes obsolete by the time it is certified
- Certification is complex
  - Knowing what to certify
  - Knowing how to use certified products
- Certification rewards secrecy (of design/implementation)
  - Goes against Kerckhoffs' principle

Minerva

- Vulnerability in Athena IDProtect smartcard
  - ECDSA leaked bit-length of nonce k via timing
  - Common Criteria EAL4+ certified
  - ANSSI-CC-2012/23: report, target
- Uses Atmel AT90 chip with Atmel Crypto Toolbox
  - ANSSI-CC-2009/11: report, target



Minerva



Note

* The **Fast** functions of M10.3, M10.4, M10.5, M10.7, M10.8, M10.9, do not offer any DPA/SPA protection and **must** not be used for secure data.

FIPS 140

- Originally for assessing tamper-resistance of HSMs
  - Focus remains to this day
- Focuses heavily on *cryptographic modules*
- FIPS 140-3 (latest version)
- Four levels
  - **Level 1**: "*production-grade*" components
  - **Level 2**: tamper-evidence and role-based authentication
  - **Level 3**: tamper-resistance and identity-based authentication
  - **Level 4**: …more of everything
- Did not include non-invasive side-channel attacks!
  - Only FIPS 140-3 (2019) added requirements

EMVCo

- Formed by **E**uropay, **M**astercard, and **V**isa
  - Global technical body for secure payment transactions
- **Target:** Interoperability and security in the payment ecosystem
  - Smart cards (credit/debit), Point of Sale (POS) terminals, mobile wallets
- **Security approach**
  - Extreme focus on physical security and side-channel resistance
  - Cards are always in the hands of the attacker
  - Evaluated by recognized independent labs (often the same ITSEFs as CC)
  - Shorter certification cycles compared to CC (to match fast payment tech)

EUCC

European Common Criteria-based Scheme

- First scheme under the **EU Cybersecurity Act** (CSA)
- Replaces fragmented national CC schemes (e.g., BSI in DE, ANSSI in FR)
  - One certificate, legally recognized across all EU member states
  - Replaces the older SOG-IS mutual recognition agreement
- Two assurance levels
  - **Substantial**: Protects against basic risks and known incidents
  - **High**: Protects against state-of-the-art attacks (Hardware security and smart cards sit here)
- Introduces stricter rules for continuous vulnerability handling and patching

Takeaways

- Certifications have a lot of issues
- ...but are the best we have

Recap

What you (hopefully) learned

Recap

The course

1. ?
2. ?
3. ?
4. ?
5. ?
6. ?
7. ?
8. ?
9. ?
10. ?
11. ?
12. ?
13. ?
14. ?
15. ?

Recap

The course

1. ?Introduction & cryptography
2. ?Smartcards
3. ?Authenticators
4. ?TPMs
5. ?HSMs, TEEs
6. ?Timing and cache attacks
7. ?Microarchitectural attacks
8. ?Physical side-channel attacks 1 (passive)
9. ?Physical side-channel attack defences 1 (passive)
10. ?Physical side-channel attacks 2 (passive)
11. ?Physical side-channel attacks 3 (active)
12. ?Physical side-channel attack defences 2 (active)
13. ?Guest lecture: Thomas Roche
14. ?Guest lecture: Łukasz Chmielewski
15. ?Certifications

Introduction & Cryptography

Smartcards

Authenticators

TPMs

HSMs, TEEs

Timing and cache attacks

Microarchitectural attacks

Physical side-channel attacks 1 (passive)

Physical side-channel attacks defences 1 (passive)

Physical side-channel attacks 2 (passive)

Physical side-channel attacks 3 (active)

Physical side-channel attacks defences 2 (active)

Guest lecture: Thomas Roche

Guest lecture: Łukasz Chmielewski

Certifications

Recommended reading

- For **this** lecture
  - Read Security Engineering – Chapter 28 – Assurance and Sustainability

References

- Common Criteria - Part 1: Introduction and general model
- Common Criteria - Part 2: Security functional requirements
- Common Criteria - Part 3: Security assurance requirements
- Common Criteria - Part 4: Framework for the specification of evaluation methods and activities
- Common Criteria - Part 5: Pre-defined packages of security requirements