Introduction to Physical Attacks

Ileana Buhan, March 2024
@ileanabuhan

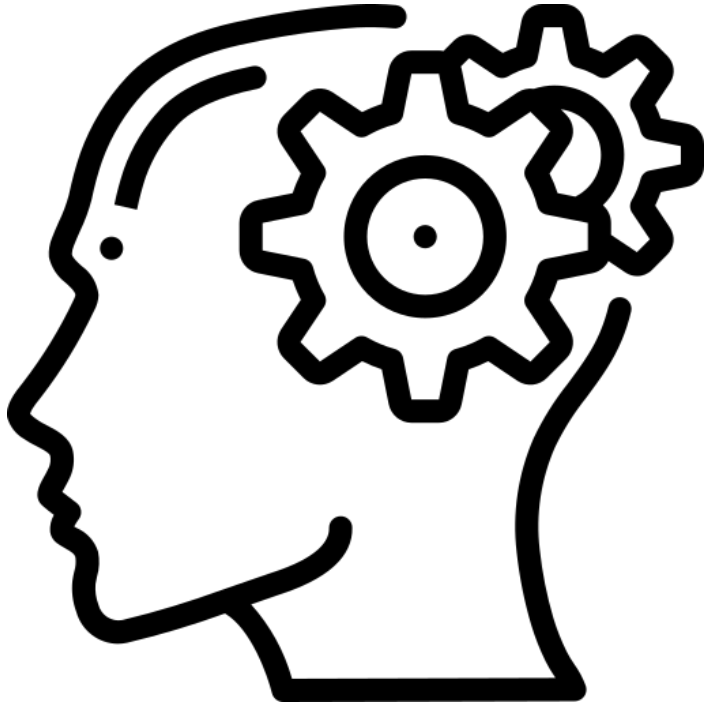
Radboud University

Take a few minutes

Why are physical attacks important?

Who is our adversary?

Do these attacks matter for the industry?



This lecture

1. Why are physical attacks important?
2. Who is our adversary?
3. Lets learn some vocabulary..
4. The industry perspective

Why are physical attacks important?

Why protect against physical attacks?

A Side Channel Attacks

Recover cryptographic keys

Recover NN training data

Reverse engineer code

B Fault Injection

Recover cryptographic keys

Modify memory contents

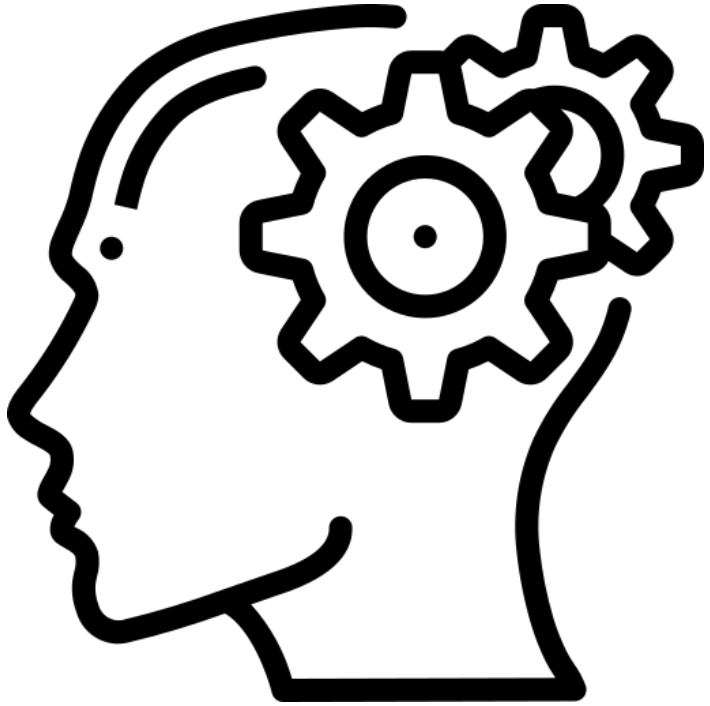
Modify registers contents

Alter the sequence of executed instruction

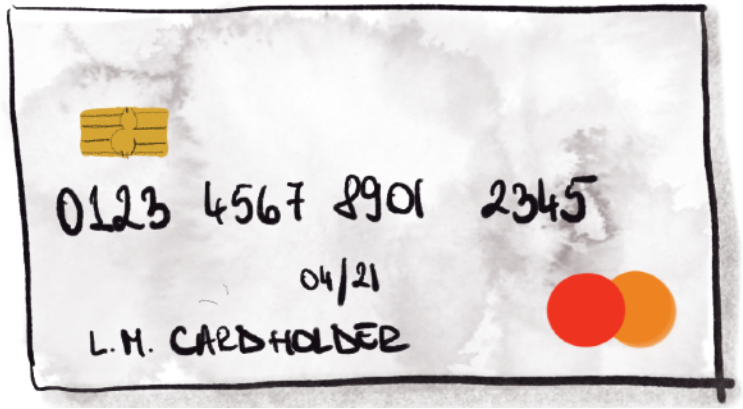
Physical attacks are powerfull !

Take a few minutes

Why protect against physical attacks?



Why protect against physical attacks?



Resilience against physical attacks is mandated in certain industries !

Who is our adversary?

The adversary - TOM

Tamper:

- obtain access to the hardware (evidence, resistant, proof)

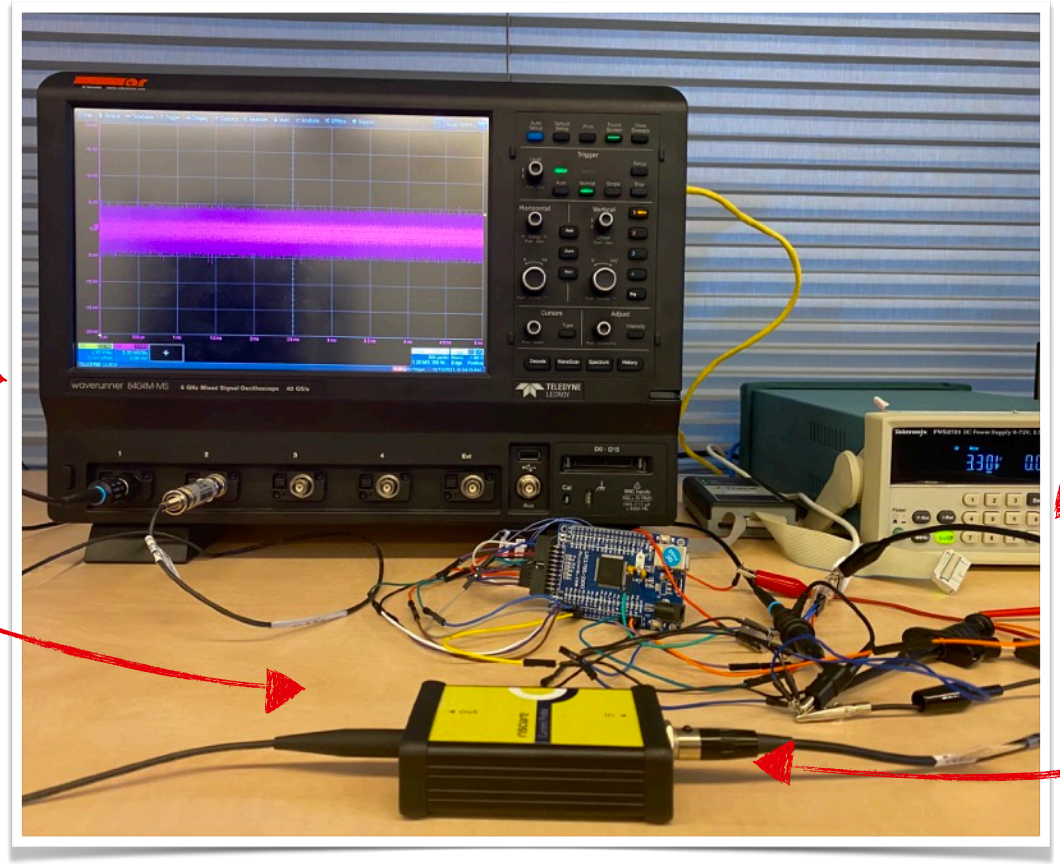
Observe:

- identify components, side channels;

Modify:

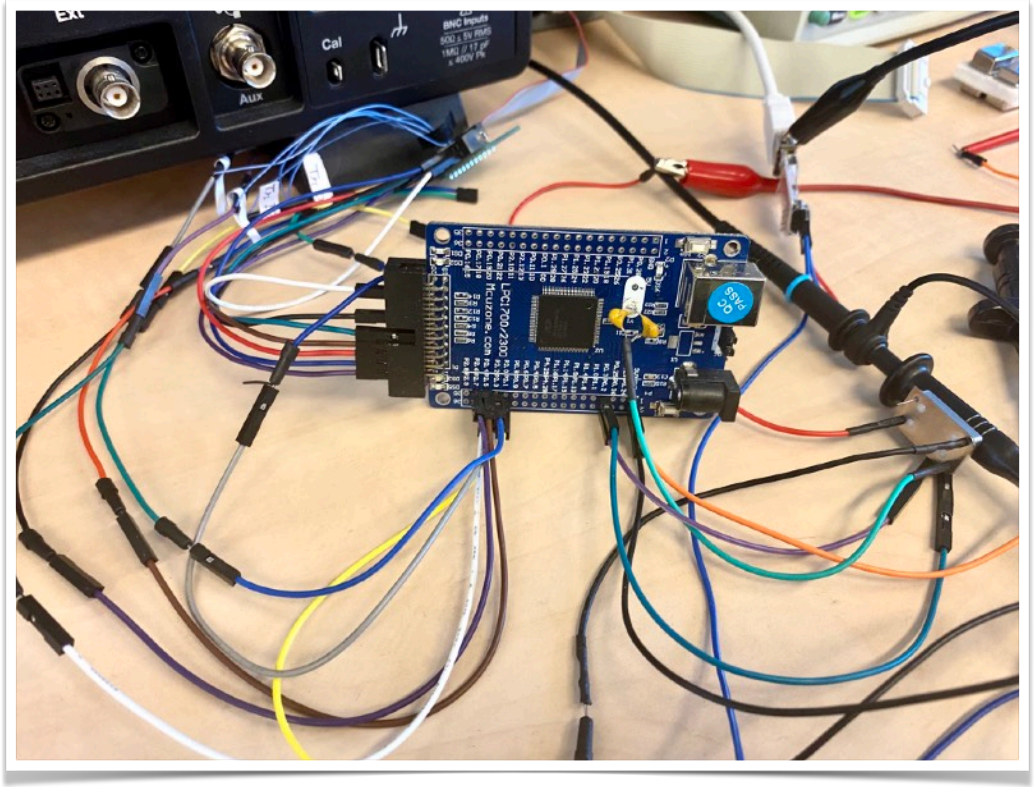
- read restricted data, bypass security checks, etc.

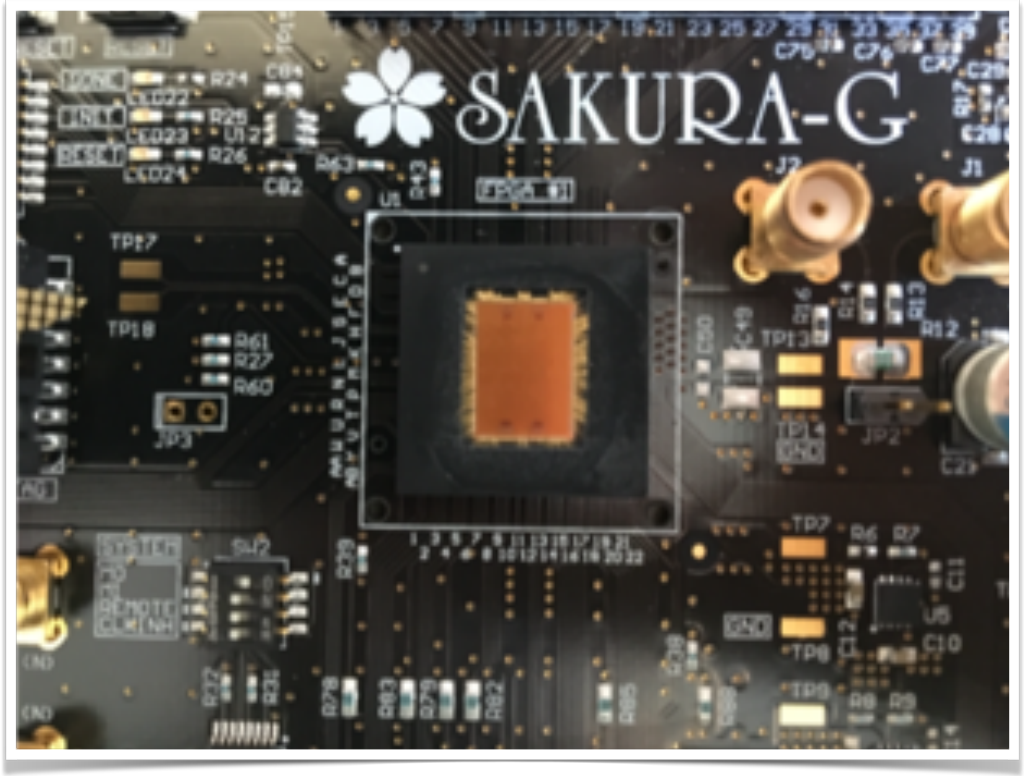
Side-channel typical setup for power analysis



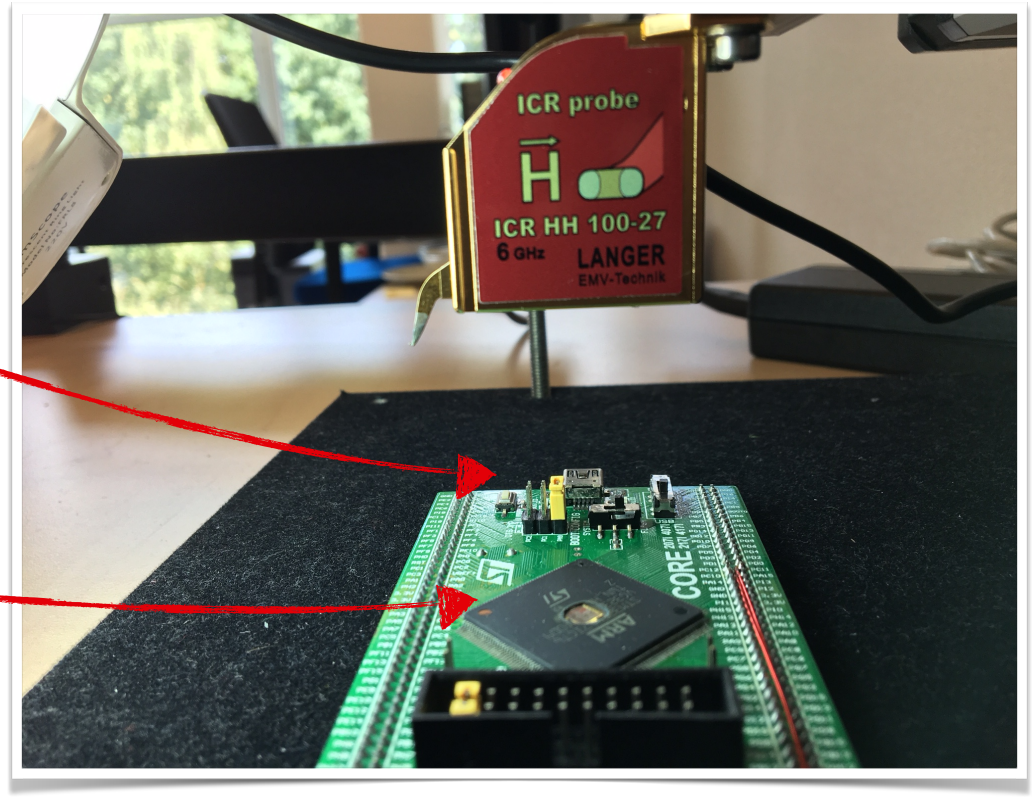
@CESCA, Radboud University

Side-channel typical setup for power analysis



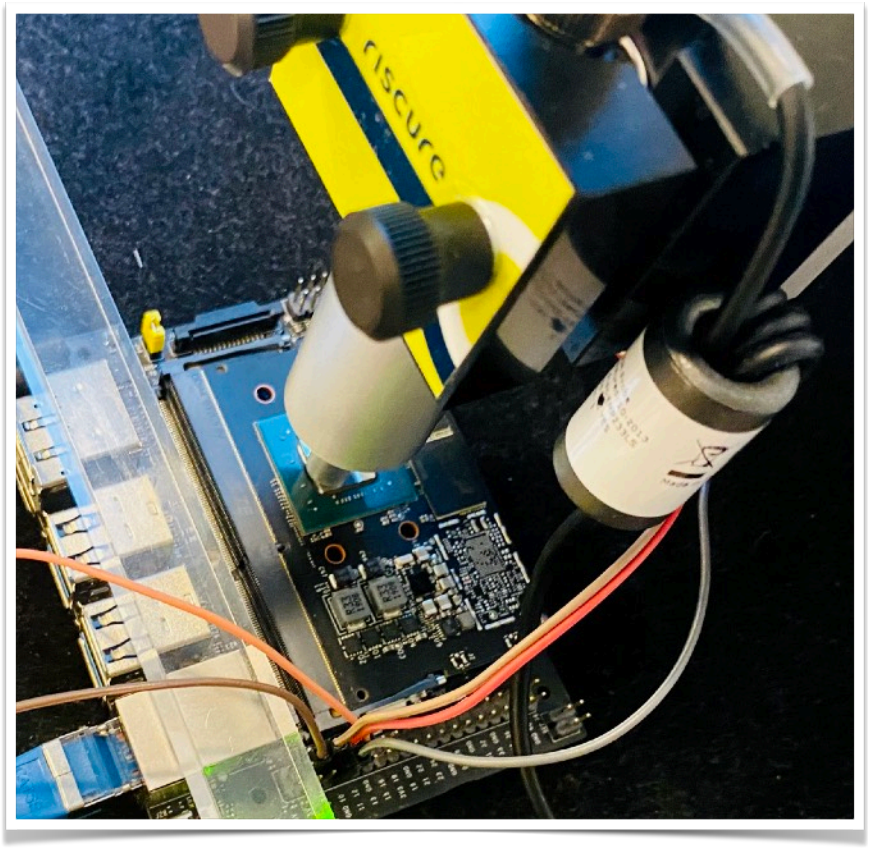


Side-channel typical setup for electromagnetic analysis



Langer EM probe

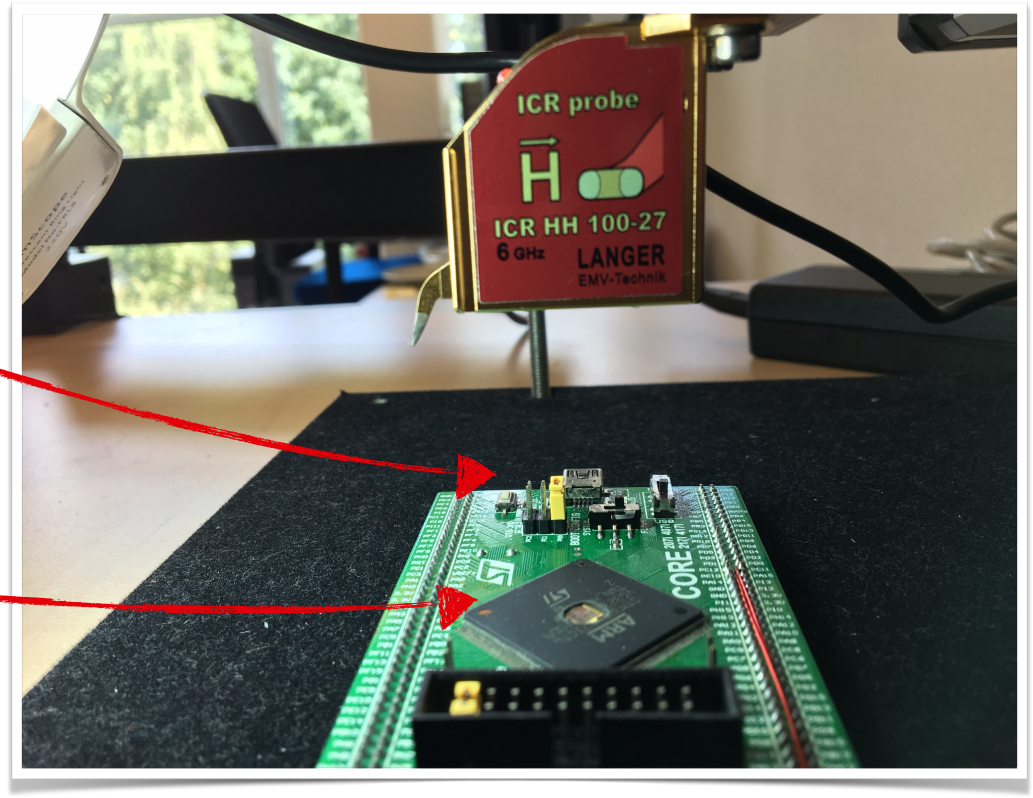
Target Decapped



XYZ station

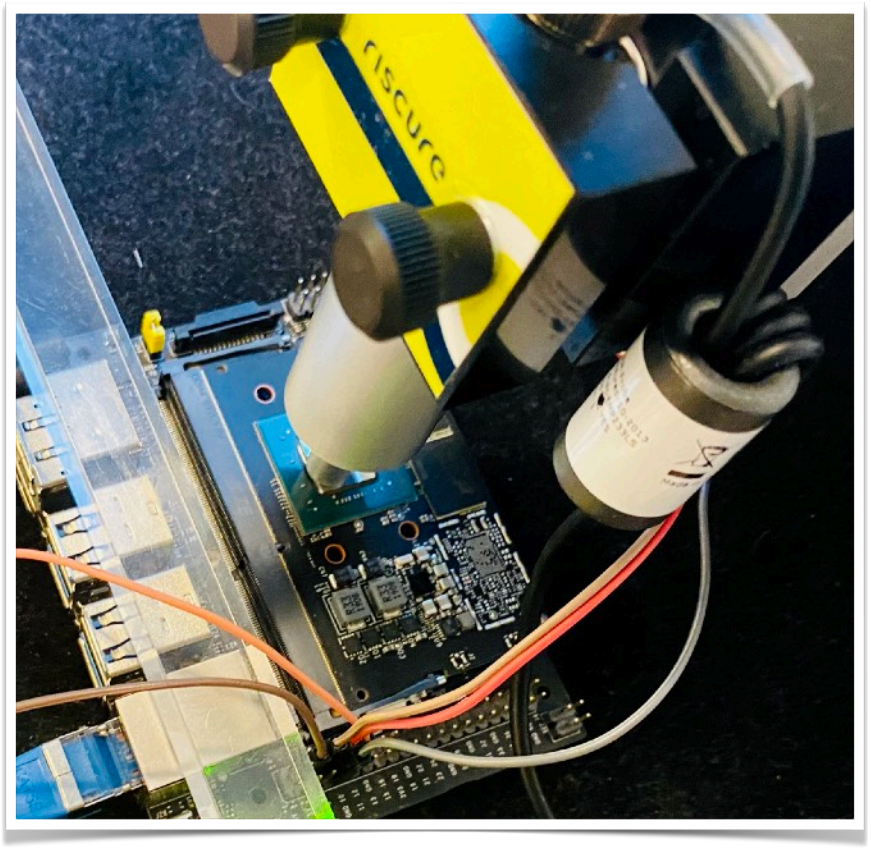
Riscure EM probe

Side-channel typical setup for electromagnetic analysis



Langer EM probe

Target Decapped



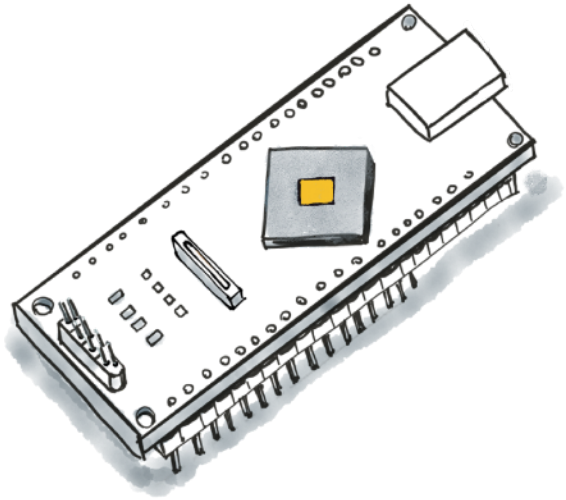
XYZ station

Riscure EM probe

Lets learn some vocabulary

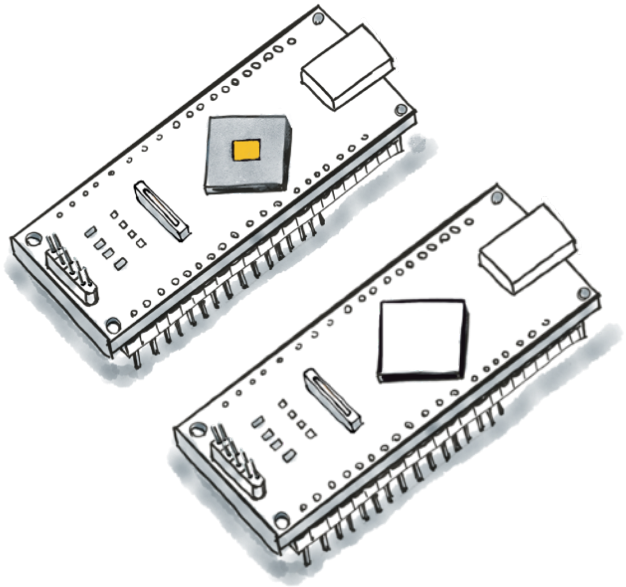
Side channel evaluations

1 Unprofiled attaks



Goal: attack

2 Profiled attacks

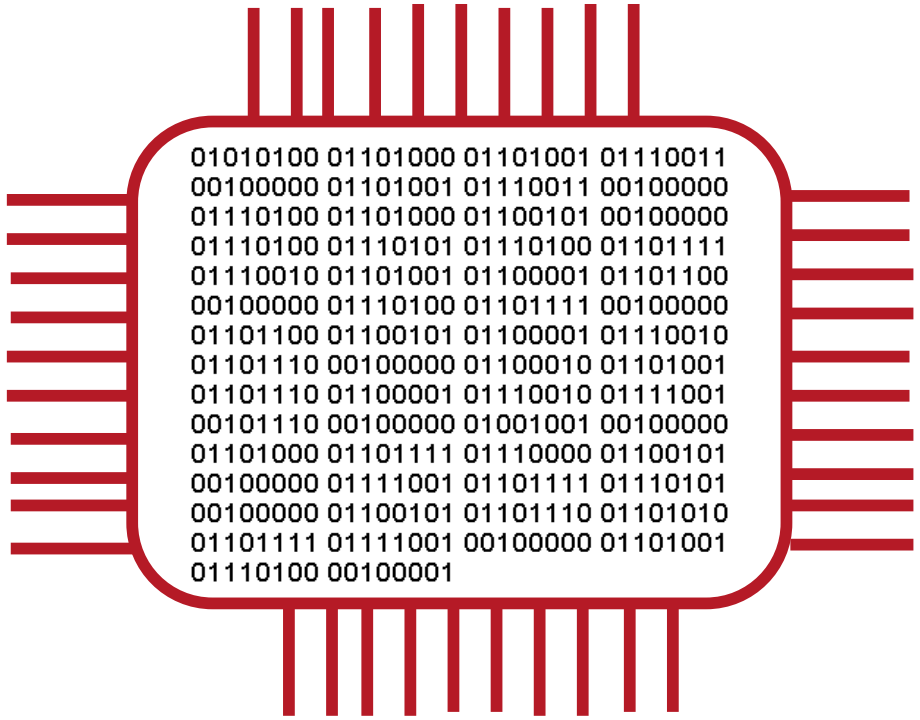


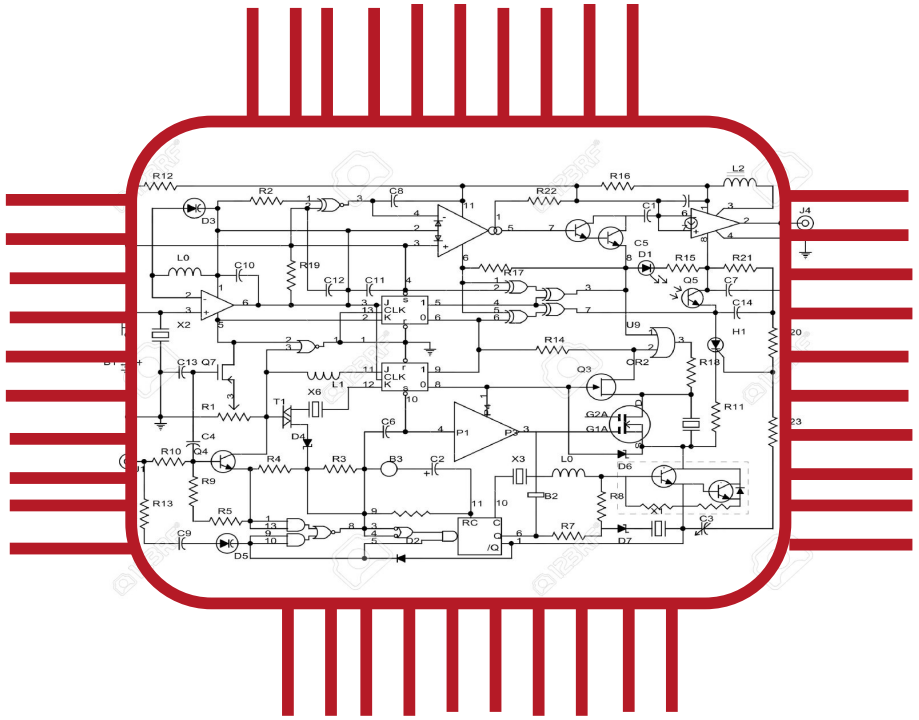
Goal: attack

3 Leakage detection

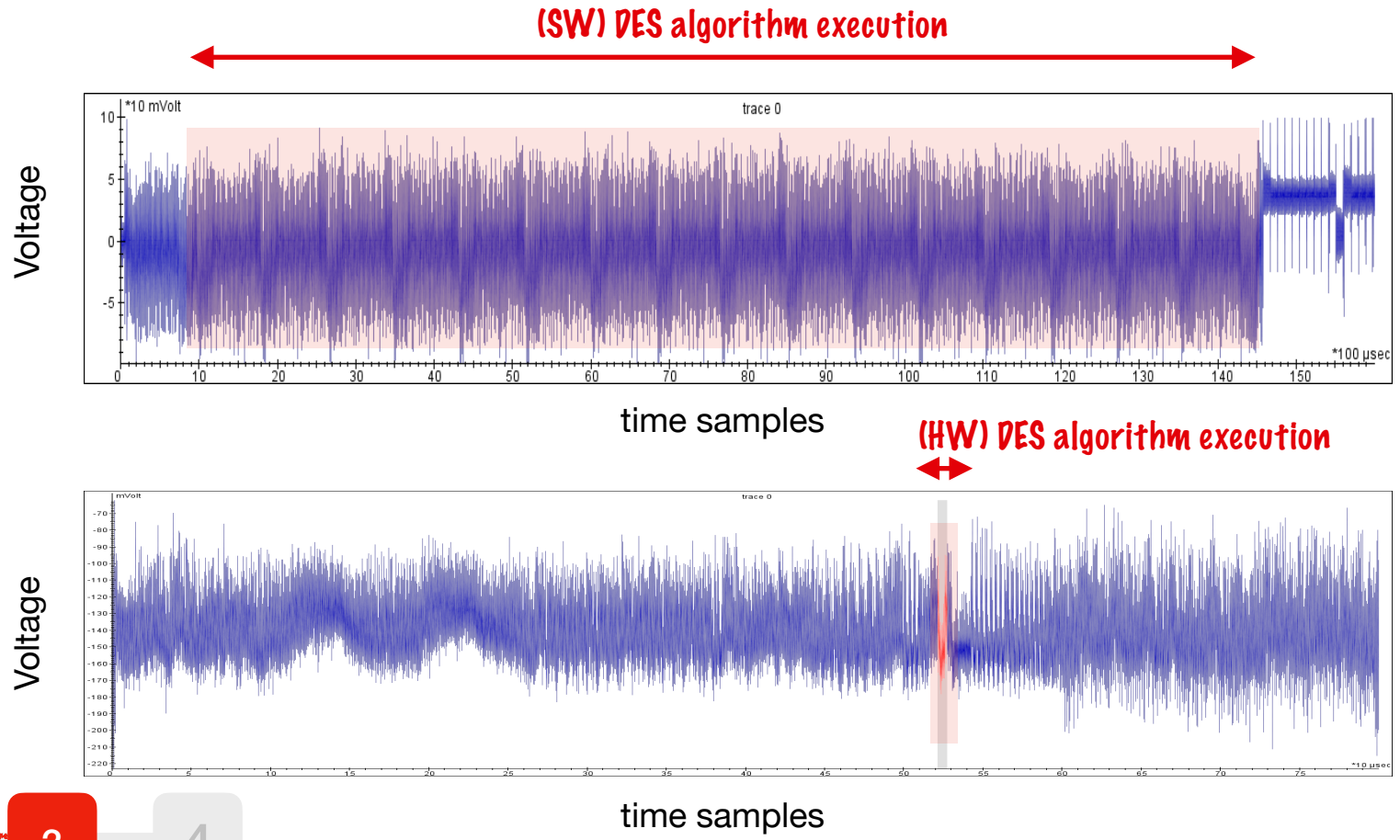
Goal:evaluate

Software vs Hardware implementation

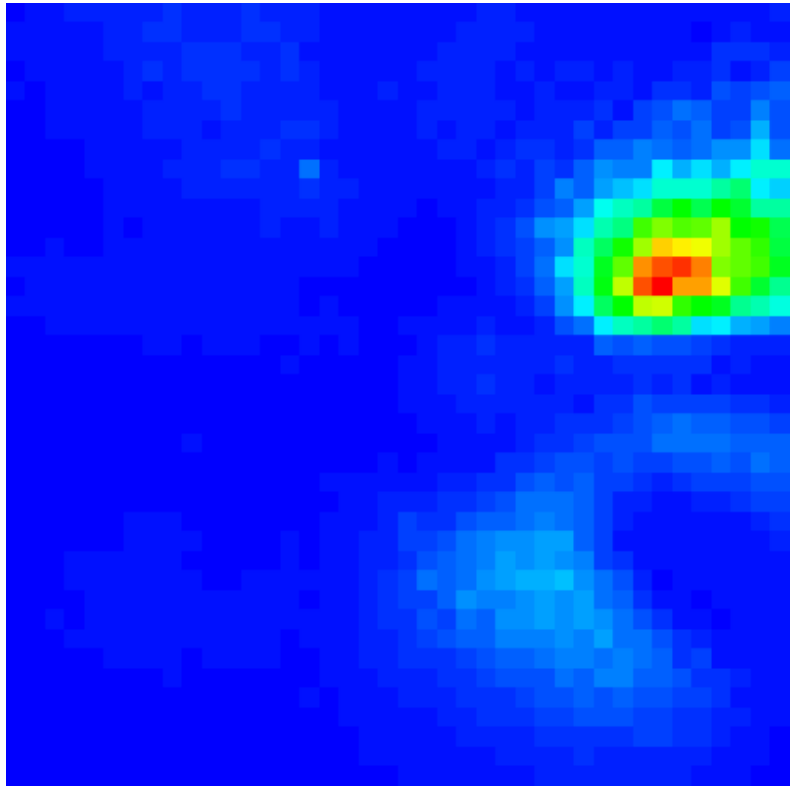


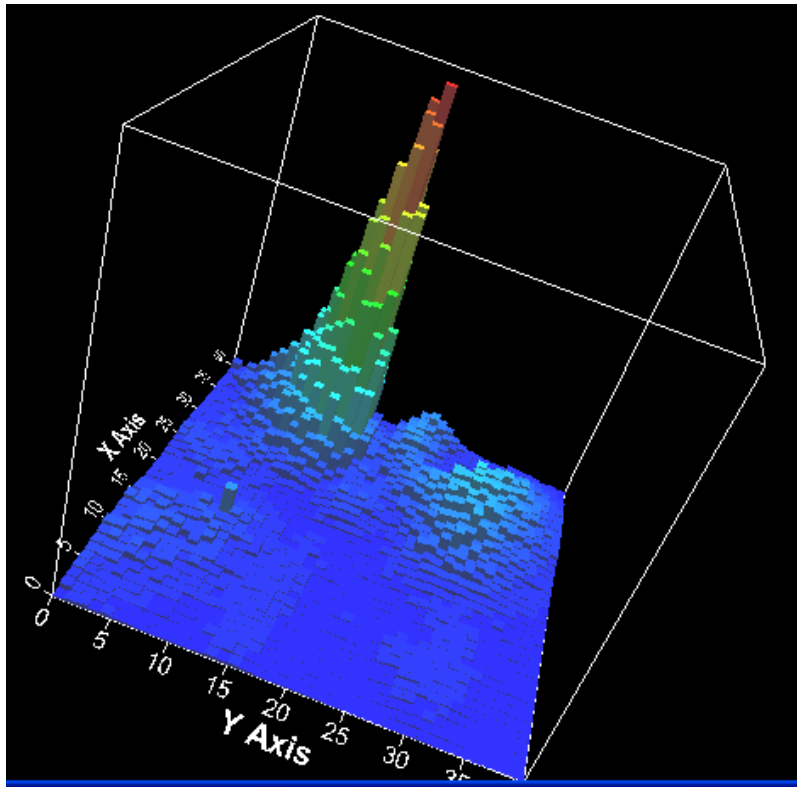


Power signatures of cryptographic implemenations



EM scan of a chip surface





The industry perspective: evaluating device resilience

Radboud University

Why invest in a security evaluation?

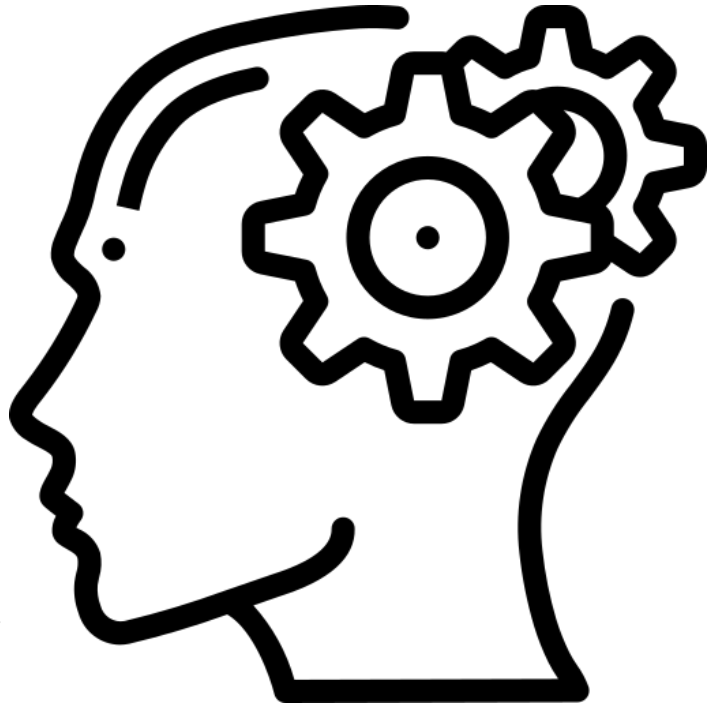
Motivation for purchasing security evaluation services:

(A) Have to, or the product cannot be sold;

(B) Protect against potential future damage;

(C) Competitive advantage

(D) Produce secure devices for the safety of their customers;



Security certification

1. Evidence that a product meets a set of given security requirements;

2. Regulate access to certain markets: payment, content protection, government, etc

3. Different security evaluation standards are available:

4. Cost effective:
   - recognition of certificates
   - pre-defined security requirements
   - pre-defined evaluation methodology

5. Vendor liability

- industry
- product type: IC, OS application
- security requirements
- geographical location

Common Criteria

History & Influence

- (1994) France, Germany, the Netherlands and UK
- (2022)

  Certificate authorizing members: Australia, Canada, France, Germany, India, Italy, Japan, Malasia, Netherlands, New Zeeland, Norway, Korea, Singapore, Spain, Sweden, Turkey, USA

  Certificate consuming members: Austria, Czeck Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Indonesia, Israel, Pakistan, Poland, Qatar, Slovak Republic, UK
- Separation of the role of evaluator (national schemes) and certifier (accredited commercial laboratories)

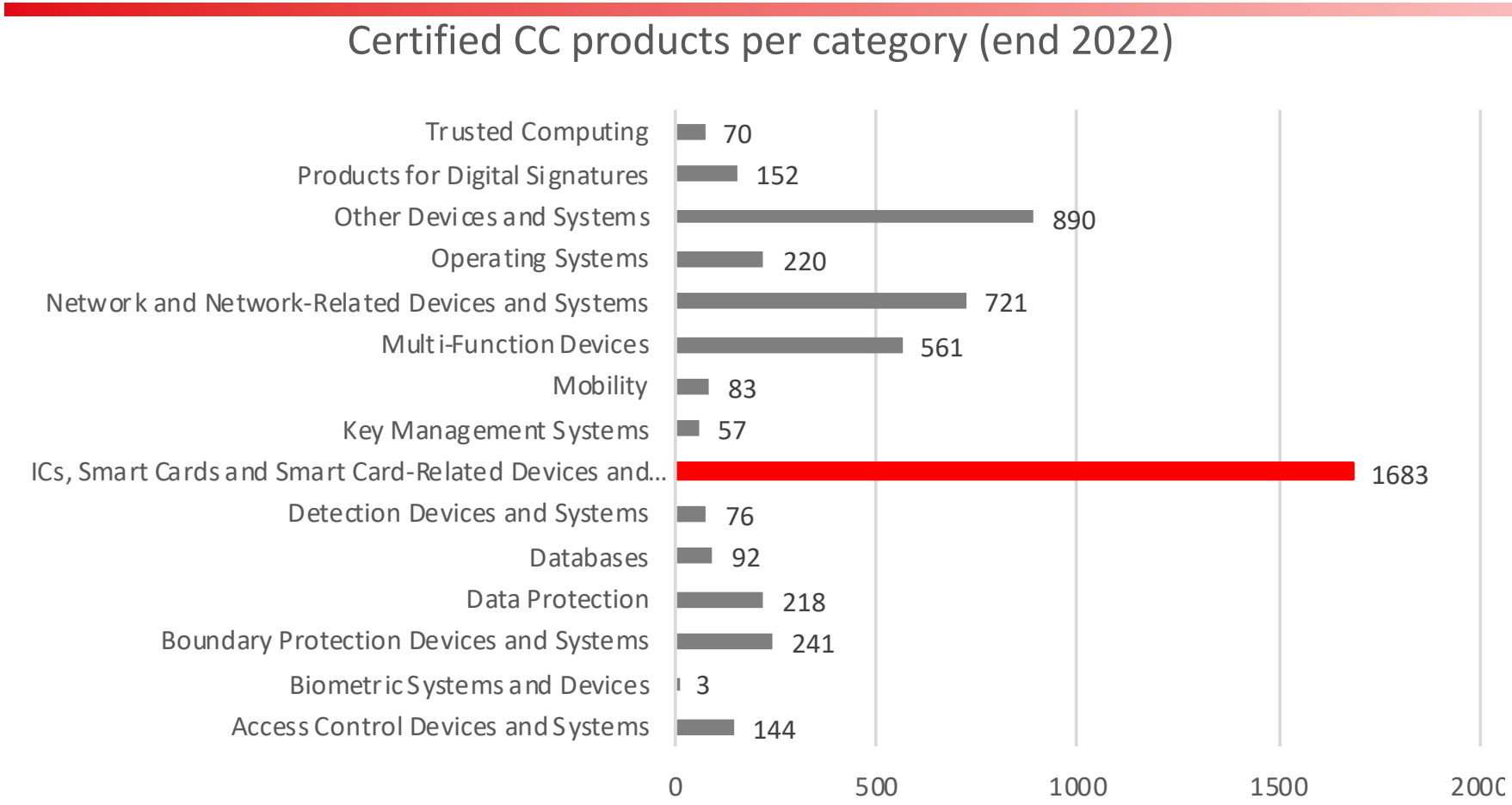
The sponsor for the evaluation is the vendor!

Objectives of CC evalution

- to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards, and are seen to contribute significantly to confidence in the security of those products and profiles;
- to improve the availability of evaluated, security-enhanced IT products and protection profiles;
- to eliminate the burden of duplicating evaluations of IT products and protection profiles;
- to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation1 process for IT products and protection profiles.

Source: Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security, May 2000,
https://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf

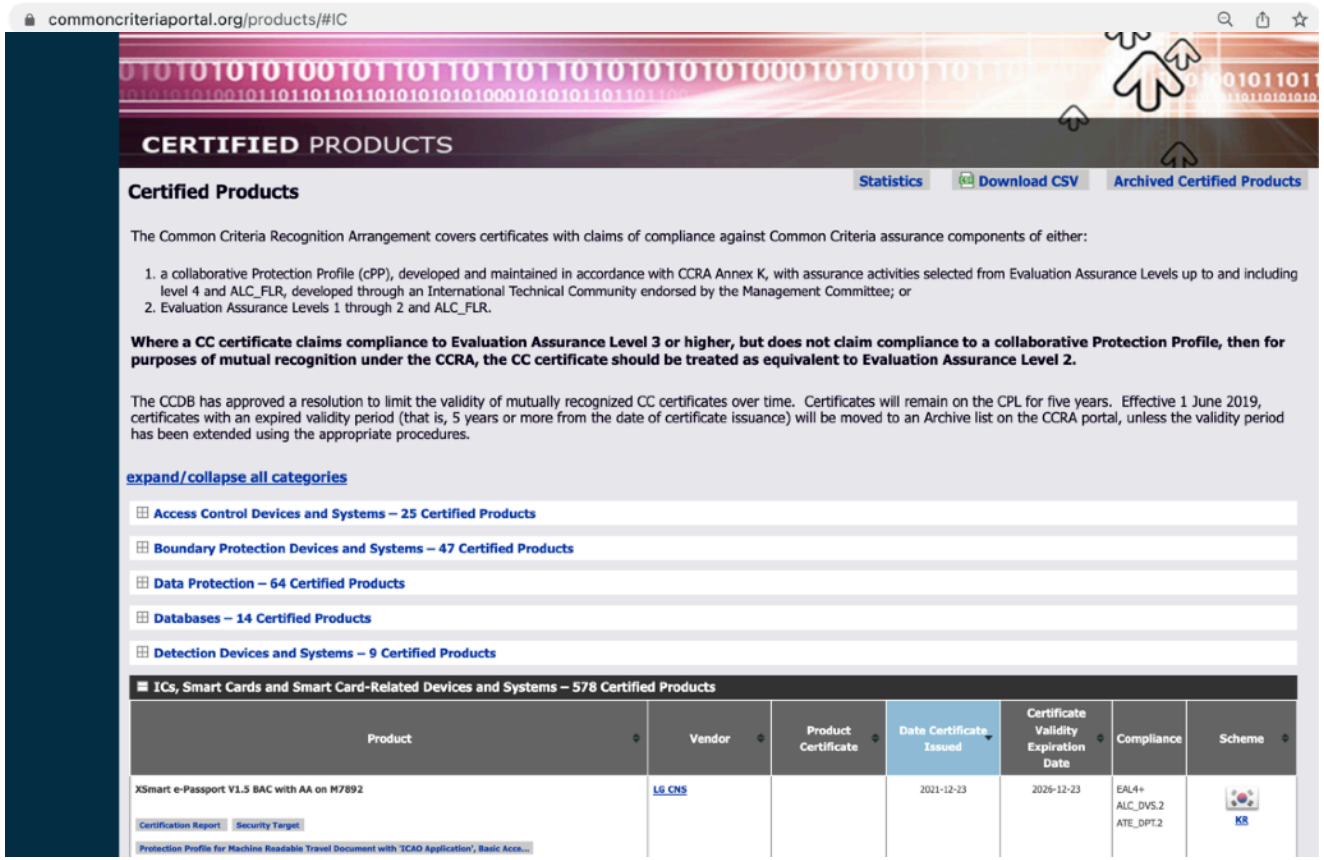
Objectives of CC evaluation



1 2 3 4

Note: the graph includes archived certificates. Data from https://www.commoncriteriaportal.org/products/stats/

CC certificates are public



1 2 3 4

CC certificates are public

ICs, Smart Cards and Smart Card-Related Devices and Systems – 578 Certified Products

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Compliance	Scheme
Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support Certification Report Security Target	Qualcomm Technologies Inc.	CCRA Certificate	2021-12-02	2026-12-02	EAL4+ ALC_DVS.2 AVA_VAN.5	NL
Google H1D3 Secure Microcontroller with Crypto Library v0.1.4 Certification Report Security Target Security IC Platform Protection Profile with Augmentation Packages	Google LLC	CCRA Certificate	2021-11-08	2026-11-08	EAL4+ ALC_DVS.2 ATE_DPT.2 AVA_VAN.5	NL

1 2 3 4

Inside a CC certificate

CC certificate for Qualcomm Secure Processor Unit

Certification Report

Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support

Sponsor and developer: ***Qualcomm Technologies Inc.***
5775 Morehouse Dr
San Diego, CA 92121
USA

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Security features of the target

- Internal Security functions - functionality related to the security of the TOE itself, primarily implemented at the OS level for logical protection mechanisms, e.g.:
  - Access controls for memories,
  - Access controls for keys managed by hardware,
  - Secure boot and root of trust,
  - Protection of user data,
  - Secure loading and updating of software and applications.
  - Domain separation between applications executed by the TOE.
  - Anti-replay island and software freshness protection.
- Cryptographic services (API) - functionality related to the Cryptographic Management Unit, primarily for cryptographic operation security, e.g.:
  - Random number generation,
  - Symmetric and asymmetric cryptographic algorithms (TDES, AES, RSA, Elliptic Curves)
  - Secure key storage in Cryptographic Management Unit,
  - Secure key generation and zeroization,
  - Hashing functions (e.g. SHA-1, SHA-256, SHA-384, SHA-512).
- Physical protection - functionality related to the physical protection of the TOE, primarily related to mechanisms to counter physical attacks at a hardware level, e.g.:

CC certificate for Qualcomm Secure Processor Unit

Certification Report

Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support

Sponsor and developer: ***Qualcomm Technologies Inc.***
5775 Morehouse Dr
San Diego, CA 92121
USA

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support from Qualcomm Technologies Inc. located in San Diego, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SPU 250 Hardware (HW version from RTL (Hardcoded)	4.1
Software	SPU firmware (PBL & Mission ROM) Foundry ID Samsung "S3" Foundry ID Samsung "S5"	55100000 551000F2 551000F6
Software	SPU software (MCP & System application (cryptoapp & asym_cryptoapp))	SPSS.A1.1.4-00108-LAHAINA.0-1

To ensure secure usage a set of guidance documents is provided, together with the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support. For details, see section 2.5 "Documentation" of this report.

1 2 3 4

CC certificate for Qualcomm Secure Processor Unit

Certification Report

Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support

Sponsor and developer: ***Qualcomm Technologies Inc.***
5775 Morehouse Dr
San Diego, CA 92121
USA

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Details about the evalution

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support from Qualcomm Technologies Inc. located in San Diego, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SPU 250 Hardware (HW version from RTL (Hardcoded)	4.1
Software	SPU firmware (PBL & Mission ROM) Foundry ID Samsung "S3"	55100000 551000F2 000F6 SS.A1.1.4- 08- IAINA.0-1

Qualcomm
ragon™ 888) with
ion" of this report.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE focused on the Secure IC and the IC Dedicated Software. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this, analysis will be performed taking into account the attack methods in [JIL-AM] and applicable attack papers with rating according to [JIL-AAPS].
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 36 weeks. During that test campaign, 21,1% of the total time was spent on characterization tests, 5,6% on physical attacks, 12,2% on perturbation attacks, 61,1% on side-channel testing, and 0% on logical tests.

1 2 3 4

CC certificate for Qualcomm Secure Processor Unit

Certification Report

Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support

Sponsor and developer: ***Qualcomm Technologies Inc.***
5775 Morehouse Dr
San Diego, CA 92121
USA

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Details about the evalution

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support from Qualcomm Technologies Inc. located in San Diego, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SPU 250 Hardware (HW version from RTL (Hardcoded)	4.1
Software	SPU firmware (PBL & Mission ROM) Foundry ID Samsung "S3"	55100000 551000F2 000F6 SS.A1.1.4- 08- IAINA.0-1

Qualcomm
ragon™ 888) with
ion" of this report.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE focused on the Secure IC and the IC Dedicated Software. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this, analysis will be performed taking into account the attack methods in [JIL-AM] and applicable attack papers with rating according to [JIL-AAPS].
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 36 weeks. During that test campaign, 21,1% of the total time was spent on characterization tests, 5,6% on physical attacks, 12,2% on perturbation attacks, 61,1% on side-channel testing, and 0% on logical tests.

1 2 3 4

CC certificate for Qualcomm Secure Processor Unit

Certification Report

Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support

Sponsor and developer: ***Qualcomm Technologies Inc.***
5775 Morehouse Dr
San Diego, CA 92121
USA

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Details about the evalution

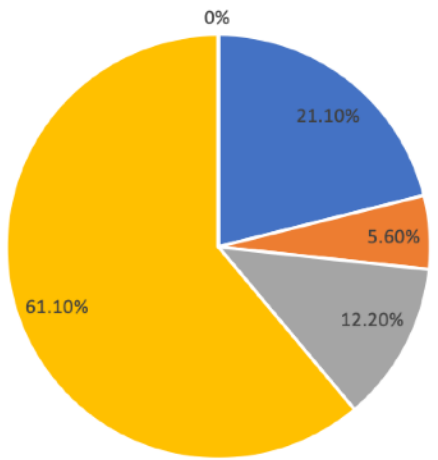
2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support from Qualcomm Technologies Inc. located in San Diego, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
	ded)	4.1
		55100000 551000F2 551000F6
	op &	SPSS.A1.1.4-00108-LAHAINA.0-1

Duration: 36 man/weeks



, together with the Qualcomm ualcomm® Snapdragon™ 888) with n 2.5 "Documentation" of this report.

■ Characterization tests ■ Physical attacks ■ Perturbation attacks ■ Side Channel attacks ■ Logical attacks

1 2 3 4

CC certificate for H1D3 Microcontroller with Crypto Library

Certification Report

H1D3 Secure Microcontroller with Crypto Library v0.1.4

Sponsor and developer: ***Google LLC***
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

Security features of the target

The H1D3 Secure Microcontroller with Crypto Library v0.1.4 basically provides the following hardware features:

- Memory Protection Unit (MPU)
- HMAC- SHA256, SHA256
- AES and TDES hardware engines
- Public Key cryptographic coprocessor
- A True Random Number Generator (TRNG)
- A Deterministic Random Bit Generator (DRGB) based on HMAC
- Environmental sensors.

In addition, the TOE provides the following software features as part of the IC Dedicated Software:

- Bootloader
- Cryptographic library, providing the following services or access to HW co-processors:
  - RSA signature verification
  - EC Key Generation
  - ECDSA
  - ECDH
  - AES (CBC, ECB, CMAC, GCM, and CRT)
  - TDES (CBC, ECB)
  - SHA256
  - HMAC SHA-256

1 2 3 4

CC certificate for H1D3 Microcontroller with Crypto Library

Certification Report

H1D3 Secure Microcontroller with Crypto Library v0.1.4

Sponsor and developer: ***Google LLC***
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the H1D3 Secure Microcontroller with Crypto Library v0.1.4 from Google LLC located in Mountain View, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	H1D3 Secure Microcontroller (packaged as H1D3M, H1D3P or H1D3C)	3
Software	Bootloader (embedded in ROM)	7f4bdb
	Crypto Library	0.1.4

To ensure secure usage a set of guidance documents is provided, together with the H1D3 Secure Microcontroller with Crypto Library v0.1.4. For details, see section 2.5 “Documentation” of this report.

1 2 3 4

CC certificate for H1D3 Microcontroller with Crypto Library

Certification Report

H1D3 Secure Microcontroller with Crypto Library v0.1.4

Sponsor and developer: ***Google LLC***
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

Details about the evalution

1 2 3 4

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the H1D3 Secure Microcontroller with Crypto Library v0.1.4 from Google LLC located in Mountain View, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
	H1D3 Secure Microcontroller (packaged as H1D3M, H1D3P or	
		4bdb
		1.4

…e H1D3 Secure
…tion" of this report.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE focused on the Secure IC, Cryptographic Library and Bootloader. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this, analysis will be performed taking into account the attack methods in *[JIL-AM]* and applicable attack papers with rating according to *[JIL-AAPS]*.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 50 weeks. During that test campaign, 38% of the total time was spent on Perturbation attacks, 60% on side-channel testing, and 2% on logical tests.

CC certificate for H1D3 Microcontroller with Crypto Library

Certification Report

H1D3 Secure Microcontroller with Crypto Library v0.1.4

Sponsor and developer: ***Google LLC***
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

Details about the evalution

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the H1D3 Secure Microcontroller with Crypto Library v0.1.4 from Google LLC located in Mountain View, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
	H1D3 Secure Microcontroller (packaged as H1D3M, H1D3P or	
		4bdb
		1.4

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE focused on the Secure IC, Cryptographic Library and Bootloader. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this, analysis will be performed taking into account the attack methods in *[JIL-AM]* and applicable attack papers with rating according to *[JIL-AAPS]*.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 50 weeks. During that test campaign, 38% of the total time was spent on Perturbation attacks, 60% on side-channel testing, and 2% on logical tests.

ıe H1D3 Secure
ıtion" of this report.

1 2 3 4

CC certificate for H1D3 Microcontroller with Crypto Library

Certification Report

H1D3 Secure Microcontroller with Crypto Library v0.1.4

Sponsor and developer: ***Google LLC***
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

Details about the evalution

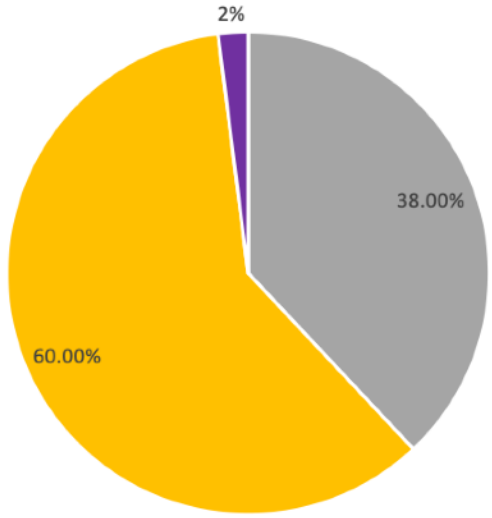
2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the H1D3 Secure Microcontroller with Crypto Library v0.1.4 from Google LLC located in Mountain View, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
	)3M, H1D3P or	3
		7f4bdb
		0.1.4

Duration: 50 man/weeks



ded, together with the H1D3 Secure
tion 2.5 “Documentation” of this report.

1 2 3 4

CC evaluations in a nutshel

A CC certificate cannot guarantee security, but ensures that claims about security are independently verified.

Merits:

White-box evaluations;
Attack based evaluation;
Recognized in multiple markets;
Vetted evaluation labs;

Criticism:

Static, certificate valid for TOE;
Formal, a lot of documentation;
Expensive;

A CC certificate can only be withdrawn when it was issued under misconception, e.g., when it turns out that wrong evidence was submitted, **not** if a vulnerability is found.

EMVco


012345

EMV chip

Europay Mastercard Visa - first published in 1996

EMVchip has three key elements:

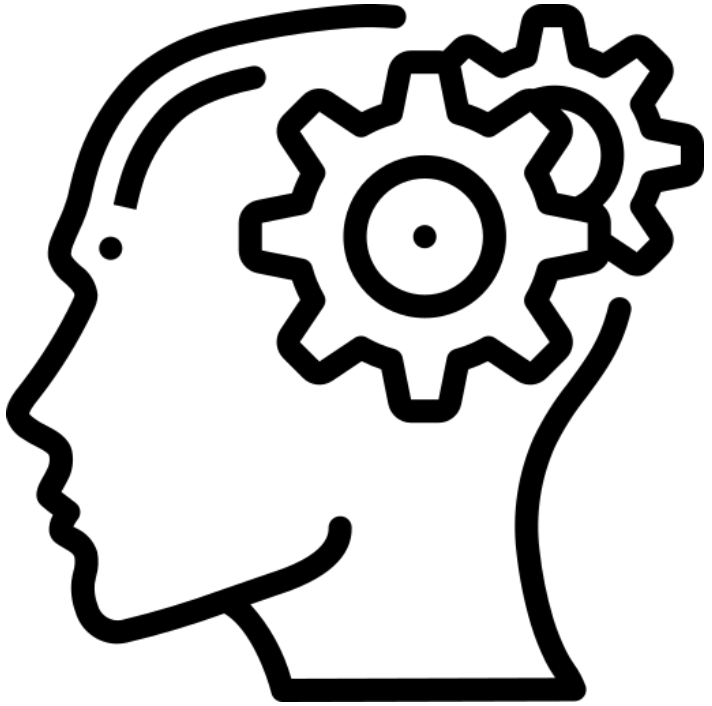
- it can perform processing
- can store confidential information very securely
- can perform cryptographic processing

EMV certification, similar to CC certification

- keyword: secure composability: chip, OS, application
- accredited labs
- manufacturers are sponsors of an evaluation
- certification body are private companies

Take a few minutes

What are some of the challenges for keeping certification up to date?



Beyond EMV chip

- Online payment world, the Chip\&Pin are becoming obsolete
- Support for different integrated payment methods
- Mobile Payment, Payment Tokenization, Wearables, EMV3D
- Technology evolves: HCE, TEE, etc.;
- Secure storage of credentials is hardware related;

Conclusions

Security certification regulate the evaluation and testing in the security industry;

Security certifications exist in a complex eco-systems

Some schemes do not look at the final product but the development process.

Challenges ahead:

technology shifts;
costs;
impact of remote attacks is unclear;
white/grey-box evaluation;
scoring of attacks is subjective to the experts interpretation ;

THANK YOU