Inter-CESTI:

Methodological and Technical Feedback on Hardware Devices Evaluations

Symposium sur la Sécurité des Technologies
de l'Information et des Communications

ANSSI, Amossys, EDSI, LETI, Lexfo, Oppida, Quarkslab,
SERMA, Synacktiv, Thales, Trusted Labs

5 June 2020

Agenda

- Introduction
- Focus on the WooKey platform
- Project start-up
- Attacks
- Conclusion

Introduction: *certification*

About product Certification

Goal: Provide assurance that the product is secured enough

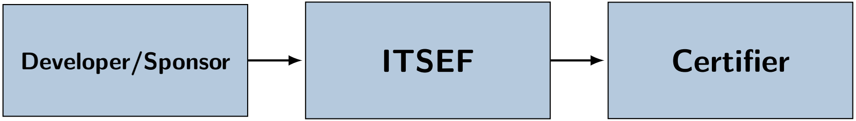
- Verify that the product does what is intended
- Pentest the product to assess the robustness of security functions
- Use evaluation criteria and methodology

COMMON CRITERIA CERTIFIED

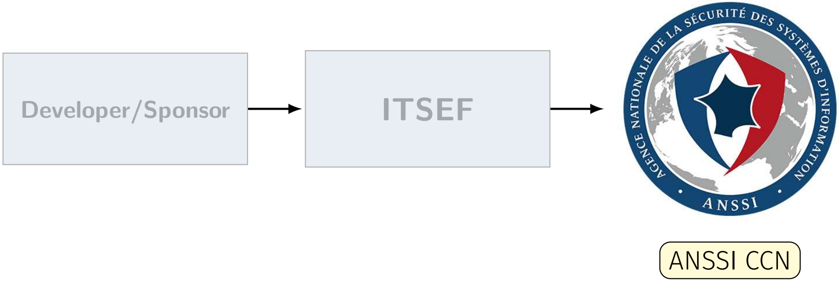
CSPN

CSPN: scope of this presentation

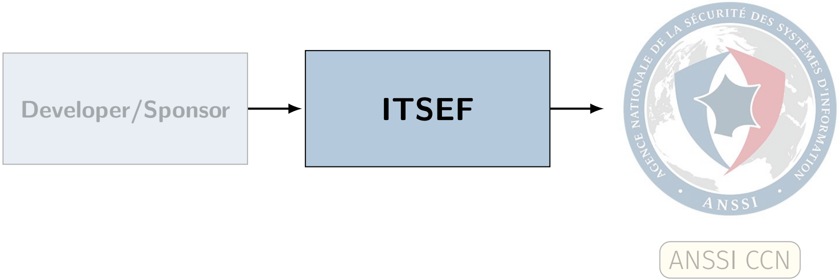
Actors involved in product certification



Who am I?


Developer/Sponsor
ITSEF
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
ANSSI CCN

WHO ARE THEY?


Developer/Sponsor
ITSEF
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
ANSSI CCN

ITSEFs: WHO ARE THEY?

eshi
The Smartcard OS Company

leti
cea tech
TECHNOLOGY RESEARCH INSTITUTE

SERMA
SAFETY & SECURITY

THALES

AMOSSYS
EXPERT IN CYBERSECURITY

LEXFO

OPPIDA
EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Quarkslab
SECURING EVERY BIT OF YOUR DATA

SYNACKTIV
DIGITAL SECURITY

Trusted labs
Creating trust in a connected world

Hardware ITSEFs

edsi The Smartcard OS Company

leti ceatech TECHNOLOGY RESEARCH INSTITUTE

SERMA SAFETY & SECURITY

THALES

AMOSSYS EXPERT IN CYBERSECURITY

LEXFO

OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Quarkslab SECURING EVERY BIT OF YOUR DATA

SYNACKTIV DIGITAL SECURITY

Trusted labs Creating trust in a connected world

Hardware ITSEFs

edsi The Smartcard OS Company

leti ceatech TECHNOLOGY RESEARCH INSTITUTE

SERMA SAFETY & SECURITY

THALES

Products

Hardware ITSEFs

edsi The Smartcard OS Company

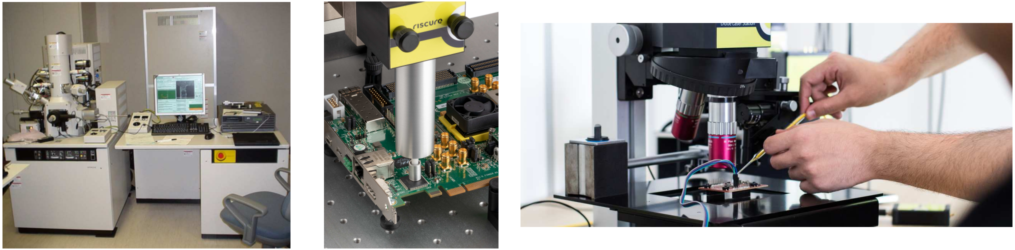
leti cea tech TECHNOLOGY RESEARCH INSTITUTE

SERMA SAFETY & SECURITY

THALES

Products

Tools



Software ITSEFs

esi The Smartcard OS Company

leti ceatech TECHNOLOGY RESEARCH INSTITUTE

SERMA SAFETY & SECURITY

THALES

AMOSSYS EXPERT IN CYBERSECURITY

LEXFO

OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Quarkslab SECURING EVERY BIT OF YOUR DATA

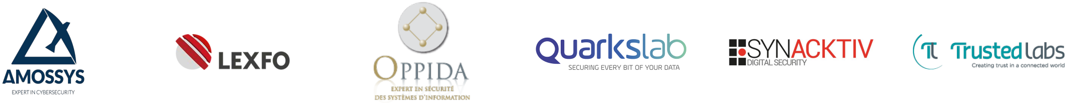
SYNACKTIV DIGITAL SECURITY

Trusted labs Creating trust in a connected world

Software ITSEFs

Products

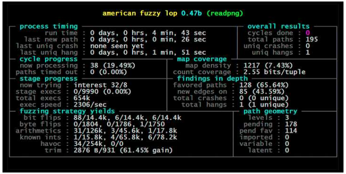
VPN
GEMALTO MOBILE PROTECTOR
SSL Secure Connection


AMOSSYS
EXPERT IN CYBERSECURITY
LEXFO
OPPIDA
EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION
Quarkslab
SECURING EVERY BIT OF YOUR DATA
SYNACKTIV
DIGITAL SECURITY
Trusted labs
Creating trust in a connected world

Software ITSEFs

Products

Tools



```
                american fuzzy lop 0.47b (readpng)

  process timing                                       overall results
        run time : 0 days, 0 hrs, 4 min, 43 sec        cycles done : 0
   last new path : 0 days, 0 hrs, 0 min, 26 sec        total paths : 195
 last uniq crash : none seen yet                      uniq crashes : 0
  last uniq hang : 0 days, 0 hrs, 1 min, 51 sec         uniq hangs : 1
  cycle progress                         map coverage
  now processing : 38 (19.49%)              map density : 1217 (7.43%)
 paths timed out : 0 (0.00%)             count coverage : 2.55 bits/tuple
  stage progress                         findings in depth
  now trying : interest 32/8             favored paths : 128 (65.64%)
 stage execs : 0/9990 (0.00%)             new edges on : 85 (43.59%)
 total execs : 654k                      total crashes : 0 (0 unique)
  exec speed : 2306/sec                    total hangs : 1 (1 unique)
  fuzzing strategy yields                               path geometry
   bit flips : 88/14.4k, 6/14.4k, 6/14.4k                  levels : 3
  byte flips : 0/1804, 0/1786, 1/1750                     pending : 178
 arithmetics : 31/126k, 3/45.6k, 1/17.8k                 pend fav : 114
  known ints : 1/15.8k, 4/65.8k, 6/78.2k                 imported : 0
       havoc : 34/254k, 0/0                              variable : 0
        trim : 2876 B/931 (61.45% gain)                    latent : 0
```

AMOSSYS EXPERT IN CYBERSECURITY

LEXFO

OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Quarkslab SECURING EVERY BIT OF YOUR DATA

SYNACKTIV DIGITAL SECURITY

Trusted labs Creating trust in a connected world

ITSEFs: what about these?

esi The Smartcard OS Company

leti ceatech TECHNOLOGY RESEARCH INSTITUTE

SERMA SAFETY & SECURITY

THALES

“Hardware devices”

AMOSSYS EXPERT IN CYBERSECURITY

LEXFO

OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Quarkslab SECURING EVERY BIT OF YOUR DATA

SYNACKTIV DIGITAL SECURITY

Trusted labs Creating trust in a connected world

Introducing the Inter-CESTI

edsi The Smartcard OS Company

leti ceatech TECHNOLOGY RESEARCH INSTITUTE

SERMA SAFETY & SECURITY

THALES

"Hardware devices"

Inter-CESTI:
- common target
- use cheap material
- hardware + software attacks

open source

open hardware

AMOSSYS EXPERT IN CYBERSECURITY

LEXFO

OPPIDA EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

Quarkslab SECURING EVERY BIT OF YOUR DATA

SYNACKTIV DIGITAL SECURITY

Trusted labs Creating trust in a connected world

WooKey: the *test vehicle*

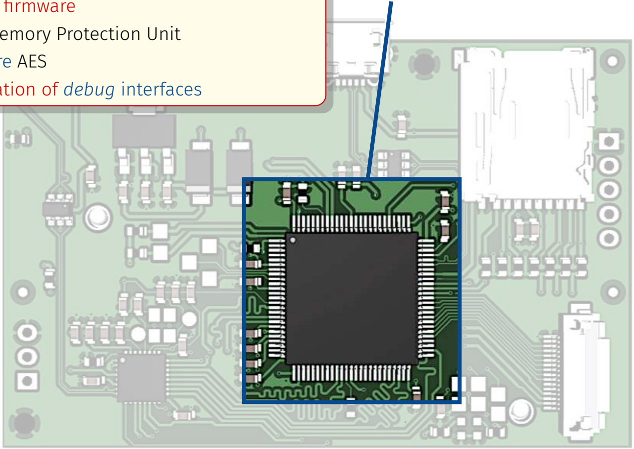
WHY WOOKEY?

- WooKey platform (presented at SSTIC 2018) fitted perfectly:
  - Open source software and hardware
  - A lot of security features
  - Numerous external interfaces
  - Knowlegde of the product

Hardware Architecture

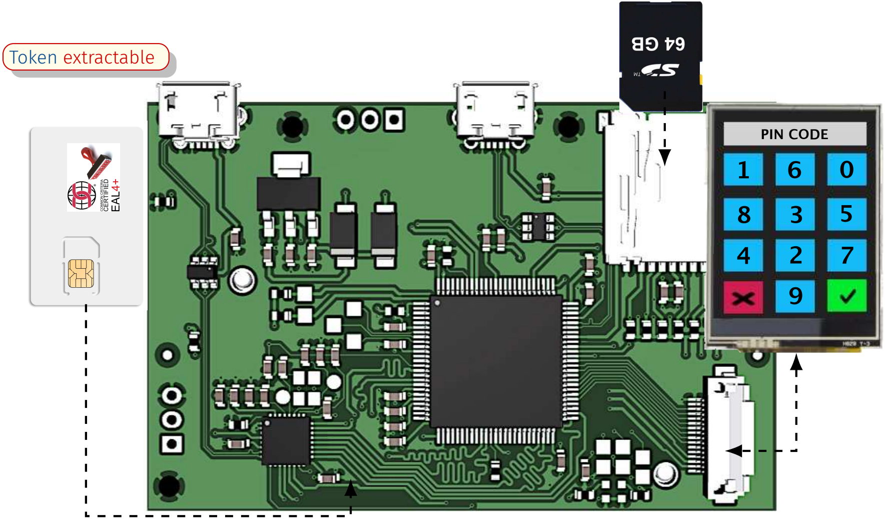
- 2 MB of flash, 192 kB of SRAM
- Internal firmware
- MPU : Memory Protection Unit
- Hardware AES
- Deactivation of *debug* interfaces

MCU = Cortex-M4 STM32F439

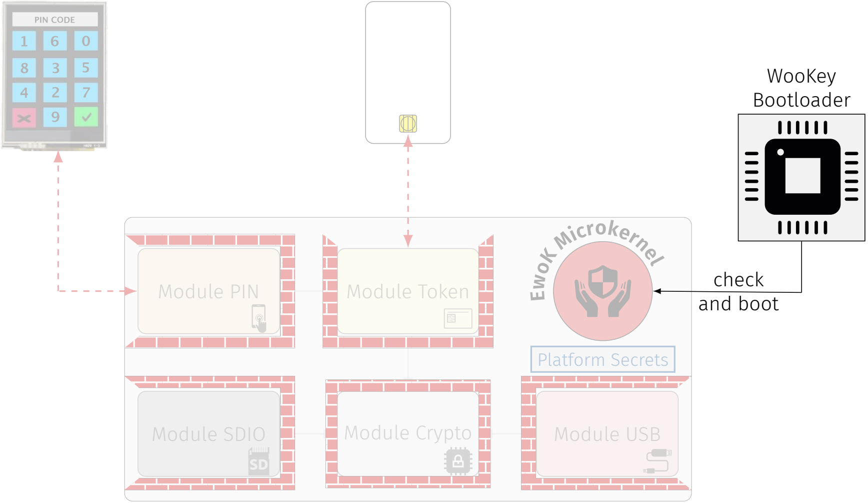


Hardware Architecture

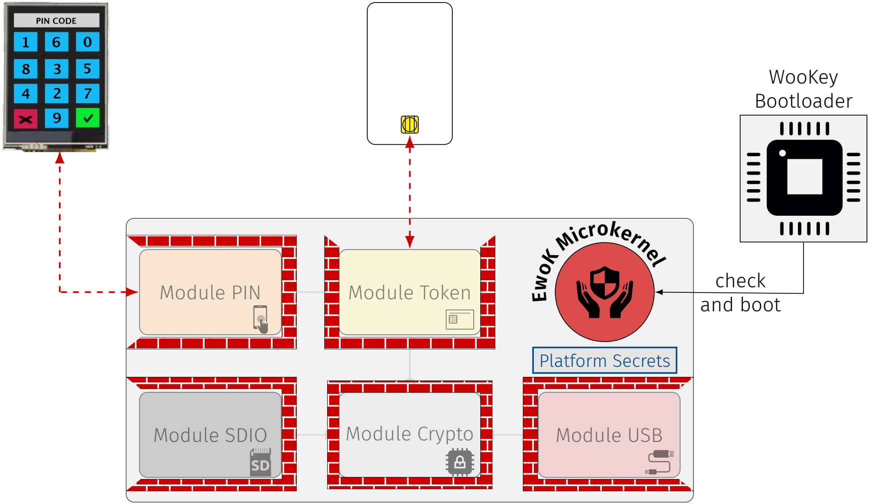
Token extractable



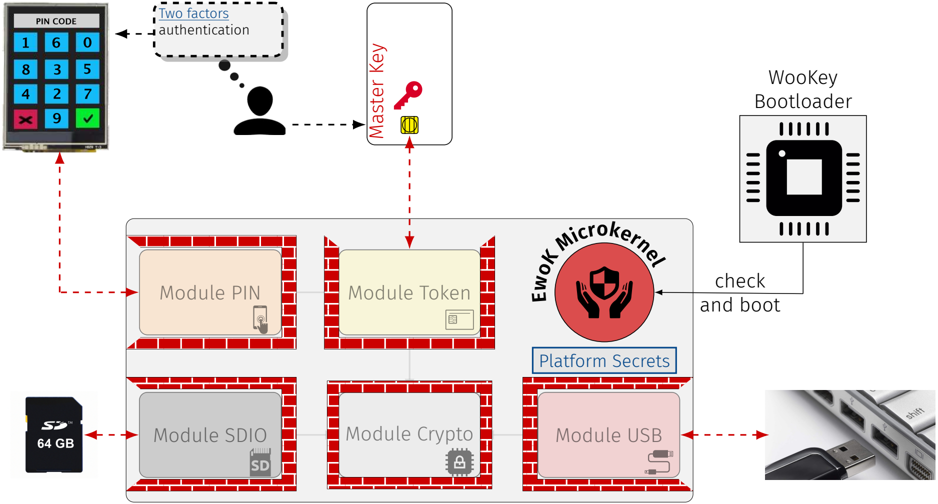
Modules and services of WooKey



MODULES AND SERVICES OF WOOKEY



Modules and services of WooKey



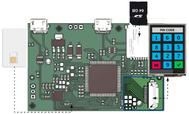
Methodology details

Inter-CESTI timeline

T0

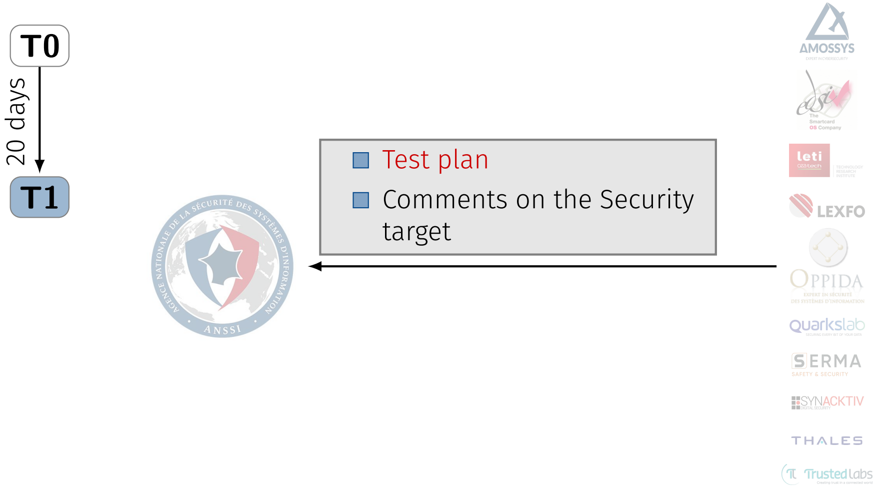
- Security target
- Cryptographic supplies
- WooKey platforms samples

Closed



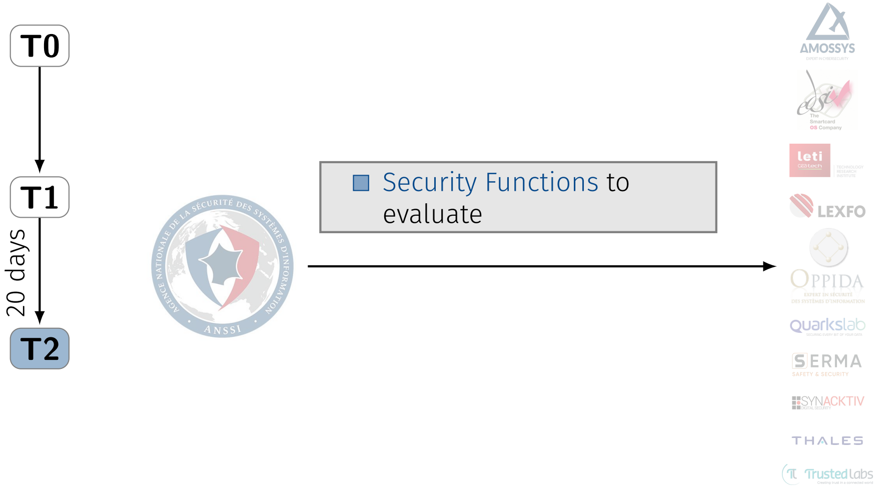
Open

Inter-CESTI timeline



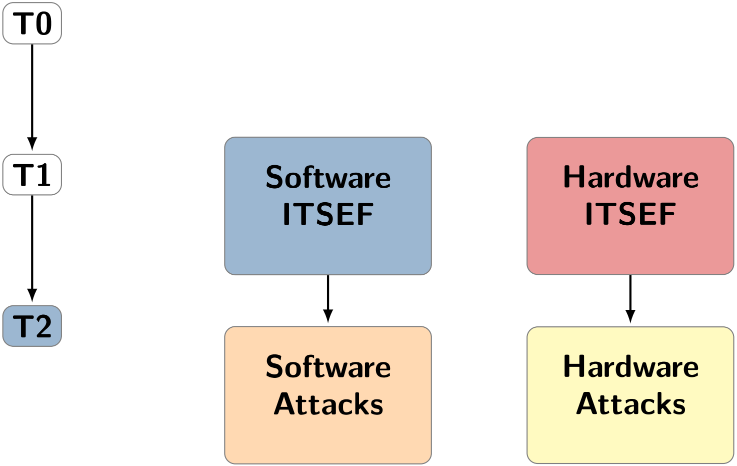
- Test plan
- Comments on the Security target

Inter-CESTI timeline


T0
T1
20 days
T2
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
AMOSSYS
EXPERT IN CYBERSECURITY
The Smartcard OS Company
leti
ceatech
TECHNOLOGY RESEARCH INSTITUTE
LEXFO
OPPIDA
EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION
Quarkslab
SECURING EVERY BIT OF YOUR DATA
SERMA
SAFETY & SECURITY
SYNACKTIV
DIGITAL SECURITY
THALES
Trusted Labs
Creating trust in a connected world

- Security Functions to evaluate

Inter-CESTI timeline



T0

T1

T2

Software ITSEF

Hardware ITSEF

Software Attacks

Hardware Attacks

AMOSSYS

The Smartcard OS Company

leti

LEXFO

OPPIDA

Quarkslab

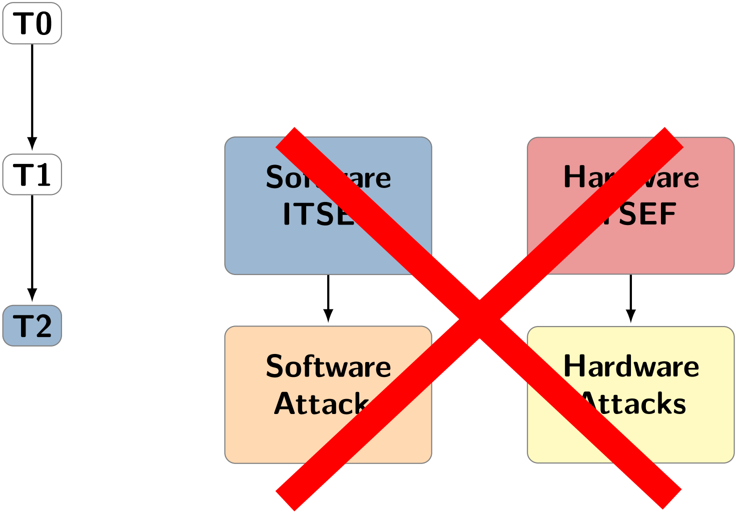
SERMA

SYNACKTIV

THALES

Trusted labs

INTER-CESTI TIMELINE



AMOSSYS

The Smartcard OS Company

leti

LEXFO

OPPIDA

Quarkslab

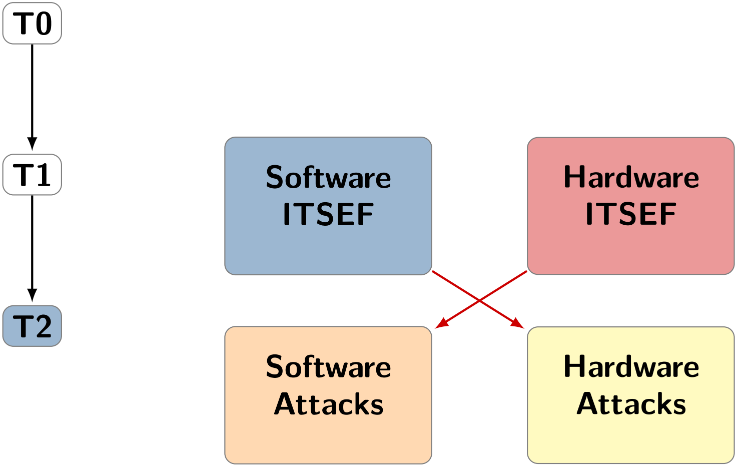
SERMA

SYNACKTIV

THALES

Trusted Labs

Inter-CESTI timeline



AMOSSYS

LEXFO

OPPIDA

Quarkslab

SERMA

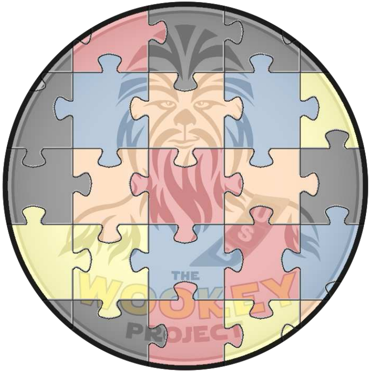
SYNACKTIV

THALES

Trusted labs

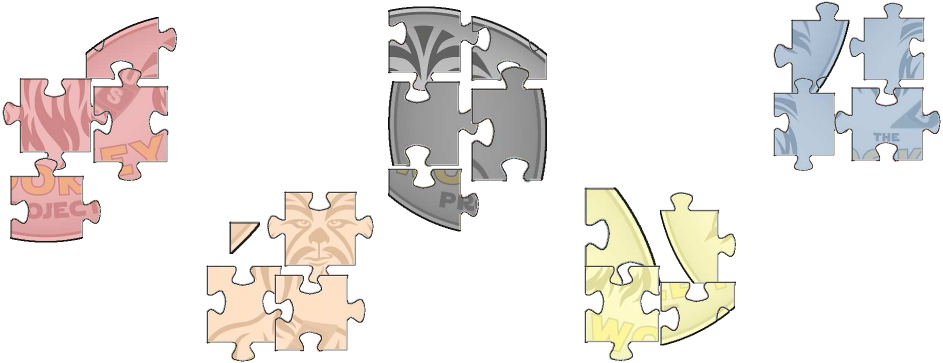
INTER-CESTI TIMELINE

Way too many assets and security functions

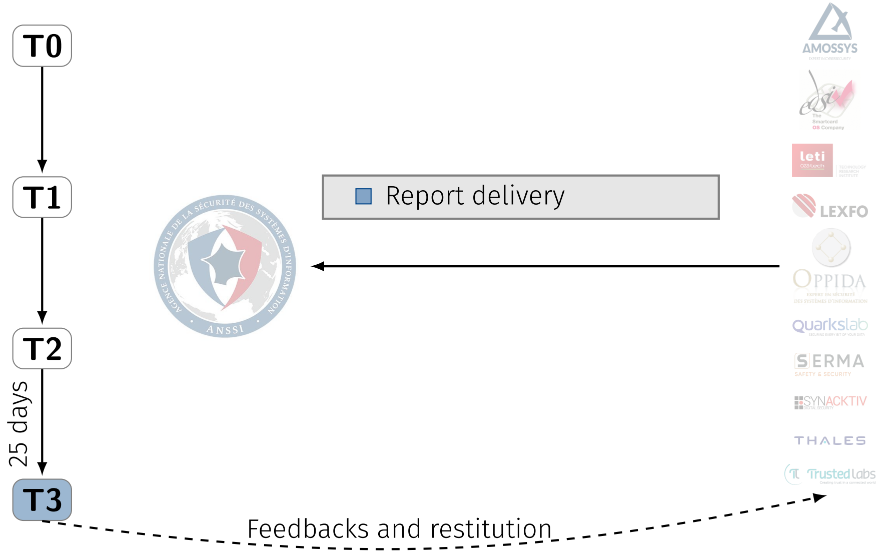


Inter-CESTI timeline

Way too many assets and security functions



Inter-CESTI timeline



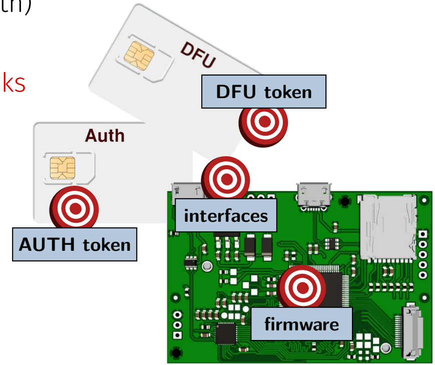
- Report delivery

Feedbacks and restitution

Identified attacks scope

- ⊕ Software attacks (pre and post-auth)
- ⊕ Pre-auth hardware attacks
- ⊕ Stealthy post-auth hardware attacks

- On the platform and the AUTH and DFU tokens



Selection of attack paths

Software

- Static analysis and fuzzing of exposed code
- Analysis of the Bootloader
- MPU policies analysis
- Javacard applets analysis

Hardware

- Side-channel attacks (SCA)
- Fault injection attacks (FIA)
- Eavesdropping/injection on buses
- TEMPEST

Selection of attack paths

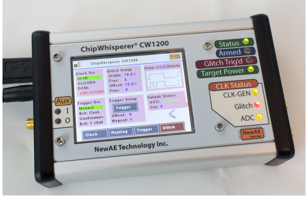
Software

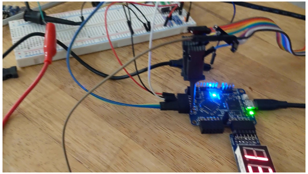
- Static analysis and fuzzing of exposed code
- Analysis of the Bootloader
- MPU policies analysis
- Javacard applets analysis

Hardware

- Side-channel attacks
- Fault injection A)
- Eavesdro ction on buses
- TEM

Use “cheap” material to fit in the CSPN constraints





Attacks details

A COMPREHENSIVE LIST OF ATTACKS

15 different attacks (see article)

All found and performed by ITSEFs

Transparency initiative

- Security target available
- Attacks details in the article:
  - Tools, settings and timings of attacks
  - Reproducible methodology
  - Mitigations

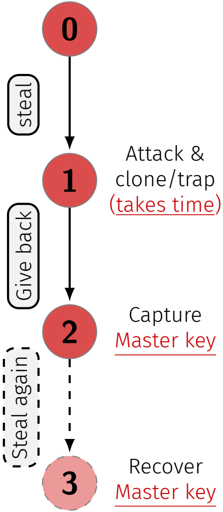
Publicly available

Findings

No direct attack path found

- Only partial attacks
- Seems like stealing once a WooKey will not allow much
- Multiple pilferage attacks needed
  - Practical attacks require physical access and cloning/trapping
  - Time required to perform cloning/trapping

Defense in depth seems useful!



Attacks overview (from the article)

	static code analysis/review	Software exploitation	Software fuzzing	Hardware fuzzing	MPU Analysis	Bus sniffing	Bus injection	Crypto attack	SCA	FIA	TEMPEST
01 Javacard applet analysis	X								X	X	
02 libiso7816 and libtoken fuzzing			X								
03 libiso7816 glitch attacks	X	X								X	
04 EwoK privilege escalation		X	X								
05 MPU configuration review			X		X						
06 PetPIN bruteforce attack							X	X			
07 Secure Channel review	X					X		X			
08 ECDSA physical attacks	X								X		
09 HMAC physical attacks									X		
10 Bootloader RDP2 downgrade	X									X	
11 Bootloader EM Faults	X									X	
12 Bootloader Anti-rollback bypass	X									X	
13 SDIO bus analysis				X		X					
14 SPI bus analysis						X					
15 SPI TEMPEST											X

Attacks overview (from the article)

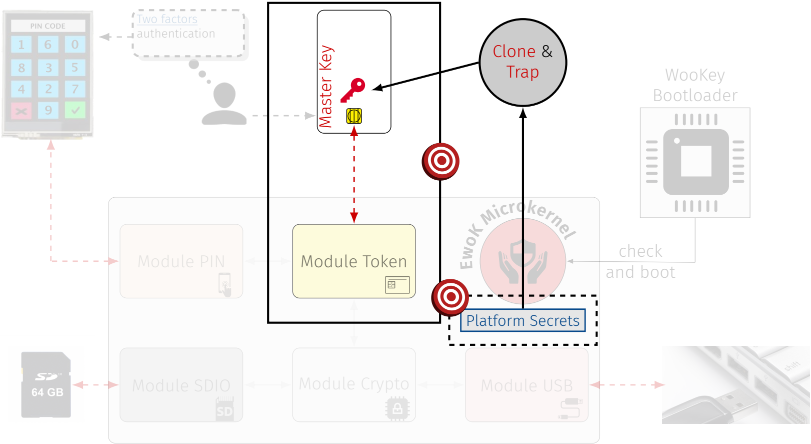
	static code analysis/review	Software exploitation	Software fuzzing	Hardware fuzzing	MPU Analysis	Bus sniffing	Bus injection	Crypto attack	SCA	FIA	TEMPEST
01 Javacard applet analysis	X								X	X	
02 libiso7816 and libtoken fuzzing			X								
03 libiso7816 glitch attacks	X	X								X	
04 EwoK privilege escalation		X	X								
05 MPU configuration review			X		X						
06 PetPIN bruteforce attack							X	X			
07 Secure Channel review	X					X		X			
08 ECDSA physical attacks	X								X		
09 HMAC physical attacks									X		
10 Bootloader RDP2 downgrade	X									X	
11 Bootloader EM Faults	X									X	
12 Bootloader Anti-rollback bypass	X									X	
13 SDIO bus analysis				X		X					
14 SPI bus analysis						X					
15 SPI TEMPEST											X

Attacks with cloning and trapping

Attacks with stealthy spying and stealing

Attack libiso7816: why?

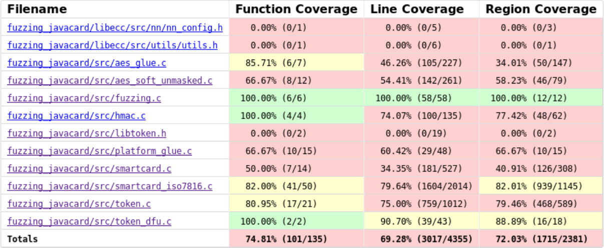
Goal: Get the Platform Secrets, then clone and trap to get the Master Key



LIBISO7816: TOWARDS A HYBRID ATTACK

02 libiso7816 fuzzing

- Software: code analysis and fuzzing didn't reveal any vulnerability



Filename	Function Coverage	Line Coverage	Region Coverage
fuzzing_javacard/libecc/src/nn/nn_config.h	0.00% (0/1)	0.00% (0/5)	0.00% (0/3)
fuzzing_javacard/libecc/src/utils/utils.h	0.00% (0/1)	0.00% (0/6)	0.00% (0/1)
fuzzing_javacard/src/aes_glue.c	85.71% (6/7)	46.26% (105/227)	34.01% (50/147)
fuzzing_javacard/src/aes_soft_unmasked.c	66.67% (8/12)	54.41% (142/261)	58.23% (46/79)
fuzzing_javacard/src/fuzzing.c	100.00% (6/6)	100.00% (58/58)	100.00% (12/12)
fuzzing_javacard/src/hmac.c	100.00% (4/4)	74.07% (100/135)	77.42% (48/62)
fuzzing_javacard/src/libtoken.h	0.00% (0/2)	0.00% (0/19)	0.00% (0/2)
fuzzing_javacard/src/platform_glue.c	66.67% (10/15)	60.42% (29/48)	66.67% (10/15)
fuzzing_javacard/src/smartcard.c	50.00% (7/14)	34.35% (181/527)	40.91% (126/308)
fuzzing_javacard/src/smartcard_iso7816.c	82.00% (41/50)	79.64% (1604/2014)	82.01% (939/1145)
fuzzing_javacard/src/token.c	80.95% (17/21)	75.00% (759/1012)	79.46% (468/589)
fuzzing_javacard/src/token_dfu.c	100.00% (2/2)	90.70% (39/43)	88.89% (16/18)
Totals	**74.81% (101/135)**	**69.28% (3017/4355)**	**72.03% (1715/2381)**

- Hardware: ITSEF successfully exploited power glitches

LIBISO7816 GLITCH EXPLOITATION

03 libiso7816 glitch attack

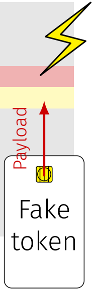
Vulnerability:

- A glitch during a masking instruction allows a buffer overflow

  + Stack canaries misconfiguration

  ⇒ Code execution in the *SMART* task

```
int SC_get_ATR (SC_ATR * atr) {
  [...]
  /* Get the historical bytes */
  atr->h_num = atr->t0 & 0x0f;
  for (i = 0; i < atr->h_num ; i++) {
    if (SC_getc_timeout(&(atr->h[i]), WT_wait_time)) {
      goto err;
    }
    checksum ^= atr->h[i];
  }
  [...]
```



- Demonstration of a hybrid attack

LIBISO7816: FROM CLONING TO TRAPPING

04 EwoK privilege escalation

- Fuzzing syscalls revealed kernel privilege escalation
  - Error in parsing the parameter of one syscall
    $\Rightarrow$ Deactivation of MPU

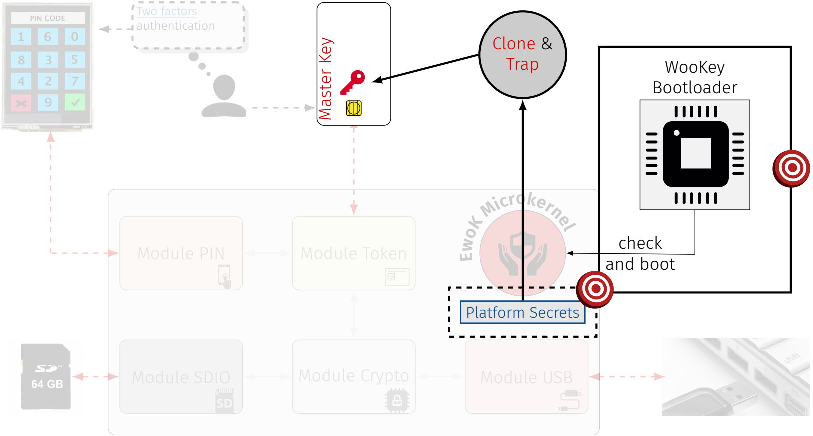
- Coupled with 03 libiso7816 glitch attack:

  $\Rightarrow$attacker can modify the firmware in place

  $\Rightarrow$trapping a closed platform is possible

Bootloader: RDP downgrade

Goal: Get the Platform Secrets, then clone and trap to get the Master Key

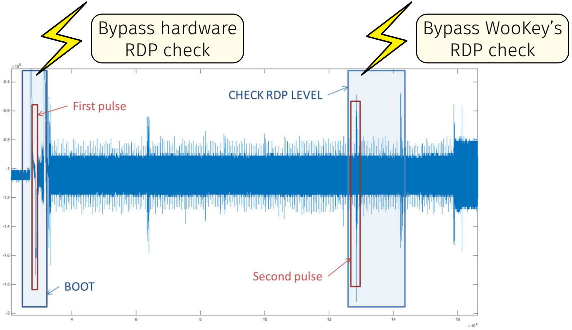


Bootloader and RDP downgrade

Vulnerabilities:

- One FIA on the STM32 for the RDP level downgrade
- One FIA on WooKey Bootloader to bypass the RDP level verification

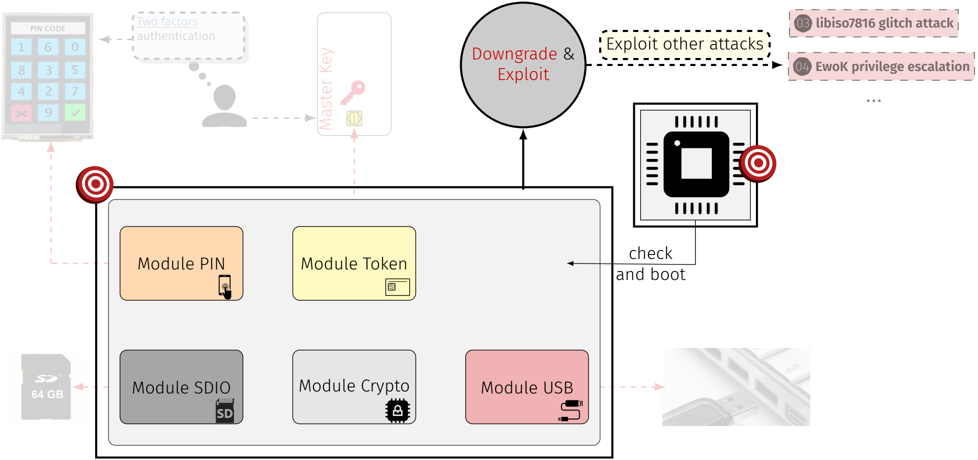
10 Bootloader RDP2 downgrade


Bypass hardware RDP check

Bypass WooKey's RDP check

FIRMWARE ROLLBACK

Goal: Exploit vulnerable firmware using version downgrade



Firmware rollback

⓬ **Bootloader Anti-rollback bypass**

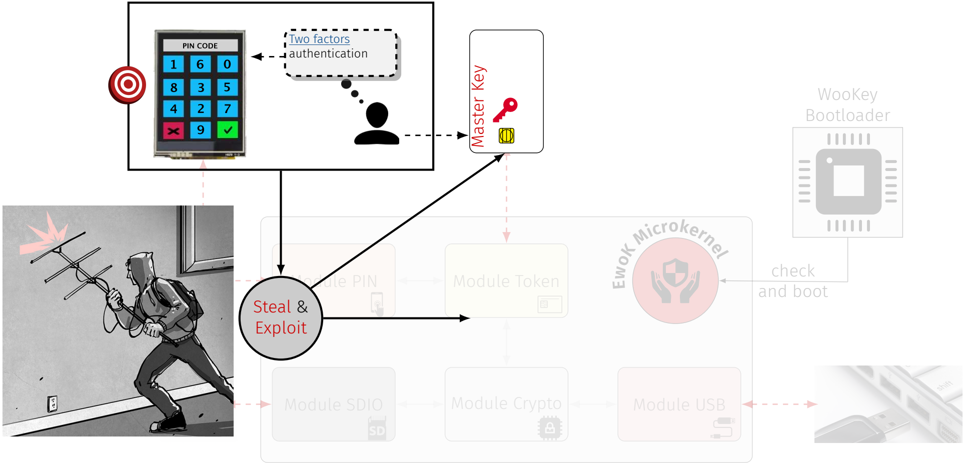
About: formal methods used for vulnerability analysis

- Software:
  - Frama-C used on Bootloader source code, but no vulnerability (RunTime Errors) found!
- Hardware:
  - Lazart, which simulates FIA found exploitable path in firmware version check
  - Exploited using a voltage glitch

Bypass firmware version check

TEMPEST

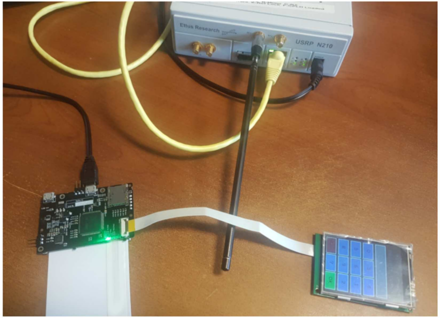
Goal: Get user PIN using EM leaks, then steal the platform and token



TEMPEST

15 SPI TEMPEST

- SPI bus between screen and PCB shows TEMPEST leaks
- More a characterization than a full attack



Conclusion

Conclusion

Inter-CESTI feedback

- Challenging for all entities
- Attacks efficiently performed by all ITSEFs (beyond their specialization)
- Results encourage the creation of a Hardware Device CSPN domain

Attacks feedback

- Cheap physical attacks quite easily achievable
- Hybrid attack paths and approaches are efficient
- Using accessible equipment with CSPN in mind

! This equipment will never scale for more hardware secured products (HSM, banking cards, etc.) !

Conclusion

Inter-CESTI feedback

- Challenging for all entities
- Attacks efficiently performed by all ITSEFs (beyond their specialization)
- Results encourage the creation of a Hardware Device CSPN domain

Attacks feedback

- Cheap physical attacks quite easily achievable
- Hybrid attack paths and approaches are efficient
- Using accessible equipment with CSPN in mind

WooKey project feedback

- Very interesting technical discussions
- New commits on WooKey's github: `https://github.com/wookey-project`

Inter-CESTI:
Questions?

ANSSI, Amossys, EDSI, LETI, Lexfo, Oppida, Quarkslab,
SERMA, Synacktiv, Thales, Trusted Labs