Hardware and software security research at ANSSI

Two case studies

Yves-Alexis Perez

Agence nationale de la sécurité des systèmes d'information

November, 20th 2019

1. Introduction

Who am I?

Yves-Alexis Perez

- team leader at ANSSI
- security researcher

Personal focus

- Linux security
- Devices security (especially PCIe)
- Platform security (Intel CSME, BMC etc.)

Agenda

- ANSSI, labs and research
- The WooKey project
- Supply chain

2. ANSSI

ANSSI: French national cybersecurity agency

Roles

- Reacting to cyber threats
- Supporting product and services development
- Providing information and advice
- Training
- Certification

Research labs

What?

expertise answering questions about various topics

research staying at or improving state of the art

prototyping proof of concepts

Who?

labs crypto, IC, wireless, networking, software, **systems**, detection

people around 60 people, 30 PHD

LAM

Software and hardware architecture lab

1 team leader

8 researchers

2 CLIP OS developers

Hardware...

- Processors and their security extensions
- Platform and devices security
- Embedded systems security

... and software architectures

- Micro-kernels and hypervisors
- Operating systems and distributions
- Mobile ecosystems

Research

Topics

- Linux hardening, containers etc.
- Devices, platforms and busses (PCIe/USB, Intel ME, BMC...)
- Processors and systems-on-chip
- Mobile devices (Android, iOS)
- Embedded systems and IoT
- Smart/autonomous/connected transports (cars, trains, planes...)

Development

Prototyping

CLIP-OS	multi-level and hardened operating systems[1]
WooKey	hardened USB mass storage device[5]
LandLock	unprivileged isolation/confining on Linux[3]
eWok	secure micro-kernel for microcontrollers

3. WooKey

Starting point

2014: Black Hat USA, *BadUSB*

- USB flash drives contain active components (microcontroller and firmware)
- no protection on the firmware, can be reflashed by an attacker
- USB is *universal*: HID, network, ...
- a genuine USB flash drive can be turned to an attacker device

Early ANSSI response

- CERT-FR news bulletin CERTFR-2014-ACT-043[6]
- answer questions about the matter
- first brainstorms around the security of USB devices themselves

Project start

Early 2015: GoodUSB project is born

Protyping an USB flash drive with state of the art local security mechanisms

Project focus

- USB flash drive
- in-house / trusted PCB and firmware design
- firmware integrity protection (update and boot-time)
- user data encryption
- open-source firmware
- open-hardware device

Timeline

2015-2016

- low priority
- few ressource
- slow pace

2017-2018

- new members to the team
- more time dedicated
- faster pace

People

- Mathieu Renard
- Ryad Benadjila
- Arnauld Michelizza
- Philippe Thierry
- Philippe Trébuchet
- ...

Recent work

Related projects

EwoK	micro-kernel for micro-controllers
Tataouine	SDK for embedded systems

WooKey as an USB flash drive

- Software tasks for USB, µSD, encryption etc.
- DFU[a] application for secure firmware update
- PCB with micro-controller and interfaces for USB and µSD
- Disabling of debug (UART/JTAG) on all active components
- 3D-printed case

[a] **Device Firmware Update protocol**

EwoK

Micro-kernels for embedded systems

- micro-controllers often run real-time (micro)-kernels
- focus is on cost and performance, not security

EwoK

Bring current operating best practice to embedded world:

- memory isolation between tasks with MPU
- high-level language with strong typing (Ada)

Tataouine

Why another SDK ?

- embedded development not always easy (cross compilation etc.)
- SoC providers usually provide their own toolchain, often outdated
- Hard to tune build options, use languages other than C and static code analysis

Tataouine

- based on standard and recent toolchains
- integrated with the EwoK μ-kernel
- easy integration of user-application (C for now, with Rust planned)
- brings good/secure development practices to the embedded world
- brings useful features (A/B updates for example)

Conclusion

Security concerns

- embedded world is conservative
- security (build and run-time) is lacking compared to more powerful environment
- embedded now more connected: IoT, connected/autonomous transport etc.

WooKey is a proposal to improve the situation

- implementation of reusable and portable modules:
  DFU, protocol stacks (SCSI, SDHC, ISO7816)
- software architecture with security in mind (task isolation, µkernel etc.)
- good integration between hardware and software security features
- facilitate evaluation

4. Supply chain

Starting point

2015

- Trafic linked to Computrace software was detected in a French administration network
- Unauthorized Computrace agent was found on freshly bought and installed laptops

Computrace

- Computrace is an *anti-theft* module relying on a BIOS part[a] and an OS agent
- Lock the platform in case of theft but also remote control (high platform privileges)
- Kaspersky published two whitepapers on vulnerabilities in Computrace (2009, 2014[7])

[a] **PCI Option ROM**

Investigation

What happened?

- December 2015, Lenovo documentation: *Unintended Computrace activation*[8]
- Lenovo laptops where bought by the French administration in 2015
- Some laptops where part of a batch with Computrace enabled
- OS agent was in turn deployed on those laptops
- Those laptops where used to generate the master for a whole deployment

Response

Short term

- coordinate with Lenovo to investigate the fix
- identify relevant laptops and fix them

Long term

- make sure the *hardware* also has security updates
- BIOS/UEFI, firmwares, Intel CSME are usually hard to update
- identify relevant security/hardening features applying to hardware
- make sure devices procured by the administration follow best practices
- raise level of security awareness of OEM and providers

Requirements

Preparation

- identify specific and useful ones
- coordinate with OEM and IT services to validate them
- find a way to test them at procurement time

Published[2] on ANSSI website and split in four blocks

- Control over the platform
- Hardware specifications
- Firmware specifications
- Security updates

Details

Control over the platform

- make sure the owner actually *owns* the plaform (not Intel, not the OEM, not Microsoft)
- have a complete list of the various components in the platforms
  especially communication interfaces
- have a complete list of the firmware versions

Hardware specifications

- enforce the presence of useful security features: I/OMMU, TPM etc.

Details (2)

Firmware specifications

- ensure the owner can configure basic security features (boot order, admin password...)
- ensure the firmware have some basic protection (integrity checks, RO flash etc.)
- avoid zero-touch / default-enabled out-of-band management solution
- make sure the BIOS correctly configures the platform

Security updates

- make sure OEMs provide security updates for all firmware they ship
- covers BIOS/UEFI, but also Intel CSME, TPM, network adapter firmwares etc.
- don't depend on a specific OS for applying updates (cf. control)

Validation

How to validate requirements?

OEMs provide:

- documentation (components and firmware version lists)
- test hardware

ANSSI then tests the hardware

When?

Mostly during the tender process:

- every machine selected goes through the test process
- non conforming offers are rejected

Possibility to do random sampling afterwards

Test means

Platform configuration

- Intel platforms require some CPU/chipset settings to be properly set by BIOS
- Failure can open large vulnerabilities
- Chipsec is an Intel tool which helps check those settings
- Small support for AMD platform as well

Procedure

On the sample machine:

- test the BIOS security features (password etc.)
- boot a chipsec-based USB key to check platforms configuration
- change the Secure Boot keys and make sure it works

Tools and procedure available online[4]

Conclusion

Key points

- supply chain security is hard
- lot of people and companies along the way
- it's possible make progress, albeit slowly
- we hope that by sharing our requirements and tools we can progress faster
- we may have blind spots

The end

Questions?

References

[1] ANSSI.
CLIP OS.
Available from: https://clip-os.org.

[2] ANSSI.
Hardware security requirements for x86 platforms.
Available from: https://www.ssi.gouv.fr/en/administration/guide/hardware-security-requirements-for-x86-platforms/.

[3] ANSSI.
Landlock.
Available from: https://landlock.io.

References (cont.)

[4] ANSSI.
Tools for testing requirements.
Available from: https://github.com/anssi-fr/chipsec-check.

[5] ANSSI.
Wookey project.
Available from: https://wookey-project.github.io/.

[6] CERT-FR.
Certfr-2014-act-043.
Available from:
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2014-ACT-043/.

References (cont.)

[7] Kaspersky.
Absolute computrace revisited.
Available from:
https://securelist.com/absolute-computrace-revisited/58278.

[8] Lenovo.
Unintended computrace activation.
Available from: https://support.lenovo.com/fr/fr/solutions/ht105220.