WOOKEY: DESIGNING A TRUSTED AND EFFICIENT USB DEVICE

Ryad BENADJILA\textsuperscript{1}  Mathieu RENARD\textsuperscript{1}  Arnauld MICHELIIZZA\textsuperscript{1}
Philippe THIERRY\textsuperscript{1}  Philippe TREBUCHET\textsuperscript{1}

\textsuperscript{1}ANSSI, prenom.nom@ssi.gouv.fr

13 December 2019
USB: Usages and Threats

Peripheral type?

Keyboard, mouse, ...
THREATS
**THREATS**

USB Controller
**Threats**

Flash
**THREATS**

- Flash

---

**USB**

- USB Controler
- Flash

**FIRMWARE**

- FIRMWARE
- BadUSB
THREATS

USB Controller

BadUSB
Threat Model

Stealing the SD card and read data
**Threat Model**

**Stealing** the SD card and **read data**

**Software Attack** on the **USB key**
**Threat Model**

- **Stealing** the SD card and **read data**
- **Hardware Attacks**
- **Software Attack** on the **USB key**
Open Solutions

USB Armory
- 2014
- Cortex-A = smartphone SoC
- Complex architecture
- Non deactivatable BootROM
- Costly
- Development Platform

Nitrokey
- 2016
- AVR
- software AES
- No memory protection (MPU)
- Host application
THE WOOKEY PROJET : REALIZATIONS

Components
- Modules
  - SPARK/Ada
  - Micro Kernel

Github
- Prototype
  - Efficient
  - OpenSource/Hardware

Wookey project
- Hardened
  - Hardware
  - Open solutions
HARDWARE ARCHITECTURE

MCU = Cortex-M4 STM32F439
2 MB of flash, 192 kB of SRAM
USB (FS et HS)
HardwareAES
Effective deactivation of debug interfaces and BootROM
Easy to find and cheap (≠ FPGA)
Token extractable

66mm

44mm
## Hardware Architecture

- 2 MB of flash, 192 kB of SRAM
- MPU: Memory Protection Unit
- USB (FS et HS)
- Hardware AES
- *Effective* deactivation of *debug* interfaces and BootROM
- Easy to find and cheap (≠ FPGA)

**MCU = Cortex-M4 STM32F439**
**HARDWARE ARCHITECTURE**

**Hardware Architecture**

Token extractable

---

**MCU = Cortex-M4 STM32F439**

- 2 MB of flash, 192 kB of SRAM
- MPU: Memory Protection Unit
- USB (FS et HS)
- HardwareAES
- Effective deactivation of debug interfaces and BootROM

Easy to find and cheap (̸ = FPGA)

Token extractable
Token extractable: Javacard
<table>
<thead>
<tr>
<th>Introduction</th>
<th>Hardware</th>
<th>Software</th>
<th>EwoK micro-kernel</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware Architecture</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Token extractable: Javacard</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Javacard 3.0.1, Global Platform 2.2.1**

**NXP JCOP JD081**
**Token Extractable: Javacard**

- Javacard 3.0.1, Global Platform 2.2.1
- Evaluation CC EAL 4+ VAN5: Protection against side channel and faults

**NXP JCOP JD081**

**Common Criteria Certified EAL4+**
WooKey: the prototype

Hardware Architecture

Artifacts Evaluated
Reusable

acm

open hardware
open source
Modules and services of WooKey

- Module Token
- Module PIN
- Module Crypto
- Module USB
- Module SDIO

Two factors authentication:
- extractable Token
- PET Pin/User PIN Code
**Modules and services of WooKey**

Two factors authentication:
- extractable Token
- PETPin/User PIN Code
Modules and services of WooKey

- Module Token
- Module PIN
- Module SDIO
- Module Crypto
- Module USB
- Master Key

Two factors authentication:
- extractable Token
- PET Pin / User PIN Code
**Micro-kernel: Confinement**

- **App PIN**
- **App Token**
- **App Crypto**
- **App SDIO**
- **App USB**

**Libraries**

**USB Drivers**

**EwoK Micro Kernel**

**SoC Memory Map**

- PIN
- Token
- Crypto
- SDIO
- USB
- Micro-Kernel
- CRYP Registers
- USB Registers
- SDIO Registers

**User space**

**Kernel space**

**Supervisor**
**Micro-kernel: Confinement**

- **Details of the modules**
- **Firmware Architecture**

**EwoK micro-kernel**

- App PIN
- App Token
- App Crypto
- App SDIO
- App USB

**Libraries**

- USB Drivers

**Kernel space**

- EwoK Micro Kernel
  - Supervisor
  - Peripherals
  - MPU
  - RW
  - Flash
  - RX
  - RW
  - RAM
  - USB Registers

**User space**

- SoC Memory Map
  - USB
  - MPU RW
  - RAM
  - MPU RX
  - Flash
  - Peripherals
Ewok Micro-kernel at a glance

- App PIN
- App Token
- App Crypto
- App SDIO
- App USB

User space

Kernel space

Syscalls

Ewok Micro-Kernel

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Hardware</th>
<th>Software</th>
<th>Ewok micro-kernel</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details of the modules</td>
<td>Firmware Architecture</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Ewok Micro-kernel at a glance

- App PIN
- App Token
- App Crypto
- App SDIO
- App USB

User space

Kernel space

syscalls

Ewok Micro-Kernel

Ada/SPARK

Buffer overflows
Integer overflows
Dangling pointers

syscalls = attack surface

Ada/SPARK
**Flash: «A» and «B»**

**SoC Flash (2 MB)**

- **Part. B**
- **Part. A**
- **loader**

**Updates**
- Resilience
- Securization

**Partition «A»**

**Initial Bootloader**
Secure DFU mode

SoC Flash (2 MB)

Part. B

DFU A

Firmware A

Bootinfo A

loader

Updated Partition

Updates

- No Button Press
- Fault resilient

Nominal Firmware Boot
SoC Flash (2 MB)

Part. B

DFU A

Firmware A

Bootinfo A

loader

Updates
- Button Press
- Fault resilient

Updated Partition

Device Firmware Update

Signed and ciphered update
**Benchmarks**

<table>
<thead>
<tr>
<th>thumb</th>
<th>READ</th>
<th>WRITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wookey</td>
<td>6.2MB</td>
<td>4.4MB</td>
</tr>
<tr>
<td>Nitrokey</td>
<td>6MB</td>
<td>6MB</td>
</tr>
</tbody>
</table>

**MPU Based Architecture**

**Benchmarks**

![Graphs showing benchmarks for different operations (Read and Write) with kernel and user usage and % CPU usage.]

- **thumb**: READ 6.2MB, WRITE 4.4MB
- **Wookey**: 6MB, 6MB
- **Nitrokey**: 6MB, 6MB
Security primitives versus threats

- DFU+signature
- Hardware assisted cypher
- EwoK+Ada/SPARK
- Two factor+
  Strong Authentication
## Security Primitives versus Threats

<table>
<thead>
<tr>
<th>Security Primitives</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>DFU+signature</td>
<td>Basic Hardware attacks</td>
</tr>
<tr>
<td>Hardware assisted cypher</td>
<td>Advanced Hardware Attacks</td>
</tr>
<tr>
<td>EwoK+Ada/SPARK</td>
<td>BadUSB+ Software Attacks</td>
</tr>
<tr>
<td></td>
<td>Two factor+ Strong Authentication</td>
</tr>
</tbody>
</table>
Security primitives versus threats

- DFU+signature
- Hardware assisted cypher
- EwoK+Ada/SPARK

Two factor+
Strong Authentication

- BadUSB Software Attacks
- Basic Hardware Attacks
- Advanced Hardware Attacks