Hardware Security is Hard:
How Hardware Boundaries Define Platform Security

Alex Matrosov
Chief Offensive Security Researcher, NVIDIA
Offensive Security REsearch at NVIDIA

Previously Principal Security Researcher @Cylance @Intel @ESET

Doing Security REsearch since 1997
Security Industry Visibility Point

Modern Persistence Techniques

https://www.platformsecuritysummit.com/2019/speaker/matrosov/
The Advanced Threats Evolution: REsearchers Arm Race

https://www.platformsecuritysummit.com/2019/speaker/matrosov/
HW THREAT MODEL
OR
FW THREAT MODEL
NOWADAYS IT’S HARD TO SPOT REAL BOUNDARIES BETWEEN HARDWARE AND FIRMWARE
HW THREAT MODEL
AND
FW THREAT MODEL
Identify Threats

- Threats can be identified by analyzing the security requirements and platform diagram
- Threats should be categorized for further analysis
  - Techniques for analyzing threats: STRIDE, DREAD, PASTA, LINDDUN, etc.
IT’S HARD TO FIND REAL SECURITY PROBLEMS IN PLATFORM DIAGRAM BASED ONLY ON REQUIREMENTS
Numbers of reported issues related to FW significantly increasing every year!

https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&query=firmware&search_type=last3years
Security Through Obscurity

- Firmware binaries are easily available online
- Tools to analyze binaries are available
- Most 3rd party reports received include disassembled code

HW/FW Security ≠ sum of all Boundaries
Hardware Security Boundaries

Most of those chips are:

- Not under direct control from hardware vendors
- Involved in security features implementation
- Connected to UEFI firmware (BIOS)
- Considered to generate trusted I/O
- Mostly out of the supervision scope of the main CPU

How can we trust anything that is not under our system control!
IN CURRENT REALITIES HW AND FW THREAT MODELING SHOULD BE UNDIVIDED
In current threat model HW considered trusted!
BMC is inside trusted boundaries 😈

- UEFI firmware blindly trust most of the hardware
- But hardware can attack UEFI firmware

How many 3rd-party chips in your platform?

- TPM module
- USB controller
- Embedded Controller (EC)
- Fingerprint Reader
- Touchpad
- and many others
ASD - AT-SCALE DEBUG

AMI also offers solution for At-scale remote debugging solution via MegaRAC BMC and AMI Hardware Debugger. AMI Hardware Debugger communicates over network with BMC to perform Host debugging operation.
Intel DCI debug commoditized by recent research

https://github.com/ptresearch/IntelTXE-PoC
Counterfeit devices with HW implants not rare

https://www.youtube.com/watch?v=YFE4RqHRYOa

How external RoT on “Secure” chip can help?

https://github.com/opencomputeproject/Project_Olympus/tree/master/Project_Cerberus
Lenovo Thinkpad EC update process

Lenovo TDK update tool
- map EC update image to memory
- set NVRAM var 'LenovoEcfwUpdate'

Lenovo EcfwUpdateDxe (not SMM)
```
res = LoadFirmware();
if ( res >= 0 )
{
    res = ValidateFirmwareHeader();
    if ( res >= 0 )
    {
        UpdateEcfw(ecfw_bin);
        res = 0164;
    }
}
```

BIOS

Lenovo Thinkpad EC update process

```c
case 0x83u:
    v5 = "ECFW image file is invalid";
    break;

case 0x84u:
    v5 = "Failed to load ECFW image file";
    break;

case 0x85u:
    v5 = "This system BIOS supports signed ECFW image only.";
    break;

case 0x86u:
    v5 = "This system BIOS supports unsigned ECFW image only.";
```

Recently we released efiXplorer plugin to make UEFI Firmware RE more enjoyable

https://github.com/binarily-io/efiXplorer
Defeating Cisco Trust Anchor (inside FPGA)

https://www.usenix.org/system/files/woot19-paper_kataria_0.pdf
A little bootloader inside FPGA is immutable

https://media.hardwear.io/hardware-security-evaluation-of-intel-max-10-fpgas/
How open silicon helps to reduce the risk?

https://opentitan.org
Google recalls some Titan security keys after finding Bluetooth vulnerability
SECURE BOOT FIX EVERYTHING?
STAGE 0

BOOTROM

VERIFIES, LOADS & EXECUTES

STAGE 1

...

STAGE N

VERIFIES, LOADS & EXECUTES

STAGE N+1

...

Silicon bugs stay forever with the customers

Another good example Intel CSME (CVE-2019-0090)

CSME ROM initialize page directory, turns-on paging and maps ROM. IOMMU is turned-on too late an attacker can remap execution pages to arbitrary physical address (SPI 😈)

SYSTEM FAILURE
WE TRUST BLINDLY ANYTHING WHICH IS SIGNED AND COME FROM TRUSTED SOURCE
https://www.sifive.com/chip-designer
Fault injection attacks do not scale well, but their results do! Whenever something is extracted (E.g secrets, keys, firmware and vulnerabilities identified in the firmware), it will be distributable! **Fault injection attacks are a first step in a complete chain of attacks!**

Niek Timmers (@tieknimmers)
HARDWARE SECURITY IS HARD!
WE REALLY NEED TO RETHINK MEANING HARDWARE SECURITY IN REALITIES OF MODERD THREAT LANDSCAPE
Thank You!

@matrosov