Reversing firmware using radare2 [H2HC]

A. Kochkov
October, 2014

Motives

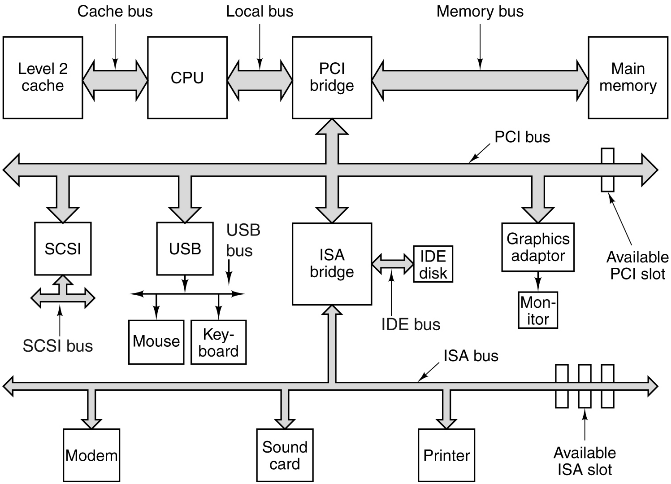
- Implement FOSS alternative (coreboot, OpenEC)
- Figure out possible attack vectors via firmware trojans

We will take only case of modern PC/Laptop/Server firmware(s).

Why?

Because it is a HUGE work!

Simple old computer diagram

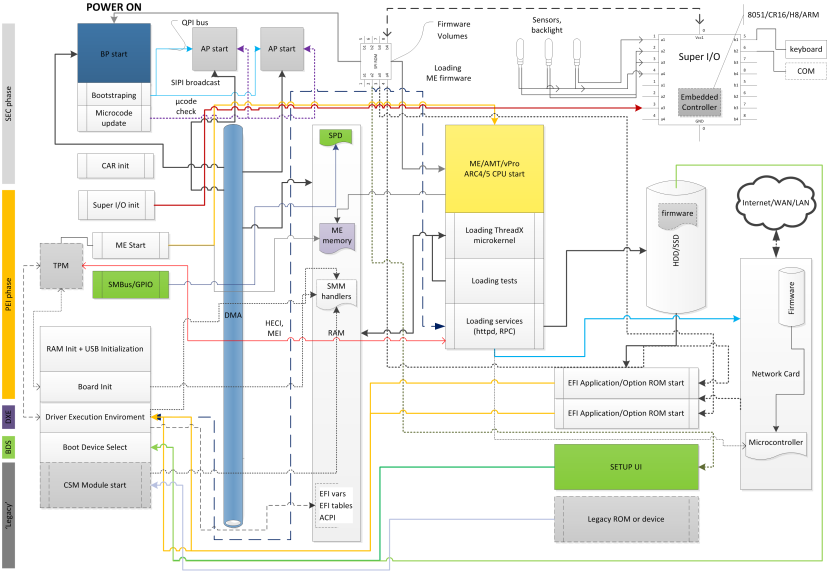


CPU

Nothing really new. Usual x86/x86_64. But we just talking about early boot stages. As in the very ancient times CPU still starts in the 16bit emulation mode. Instead of old good 386 modern processors (like Intel ones) can check signature of the reset vector. But all after that can be tampered very easy.

```
r2 -a x86 -b 16 some-bios.bin
[f000:fff0]> pd 1
            ;-- entry0;
            f000:fff0     e9f591    jmp 0xf91e8
[f000:fff0]>
```

Intel Laptop booting process (simplified)



CPU uCode

Main purpose - to fix hardware bugs. Sometimes you can see interesting erratas. Modern CPU microcode firmware is signed for both AMD and Intel (2048 bits) (PKCS#1 v1.5 padding, SHA-1, later SHA-2)[1]
There is no public reversing of the microcode, while it possibly (speculation?) allow to patch MOV instruction behaviour to copy important data somewhere

[1] Ben Hawker (2012-2013). *Notes on Intel Microcode Updates*.

Intel ME/AMT/vPro

A lot of research, ARC4 was 'broken'[2] and can be exploited. ARC5 research is in progress[3], problems with unpacking (huffman tables, etc).[4]

Table: ARC hardware

Name	Generation 1	Generation 2	Generation 3
ME versions	1.x - 5.x	6.x - 10.x	BayTrail
Core	ARCTangent-A4	ARCTangent-A5	SPARC
ISA	ARC (32 bit)	ARCompact (both 32 and 16 bit)	SPARC v8
Manifest tag	$MAN	$MN2	$MN2
Module header tag	$MOD	$MME	$MME
Code compression	None, LZMA	None, LZMA, Huffman	None, LZMA

Table from Intel ME secrets talk[5]

[2] Iurii Bystrov Patrick Stewin (2013). "Persistent, Stealthy, Remote-controlled Dedicated Hardware Malware". In: 30C3. Hamburg, Germany.

[3] *MEre project* (2013-2014).

[4] *Intel ME 6.x Huffman algorithm* (2014).

[5] Igor Skochinsky (2014). "Intel ME Secrets". In: REcon.

AMD IMC

- Various peripheral and power management tasks
- Experimental open firmware is available from Rudolf Marek
- An embedded controller of sorts in the southbridge. The controller is either enabled by hardware strap option. Or if you provide a firmware, the controller is enabled via soft strapping the chipset. It is 8051 controller.

AMD SMU

Another embedded controller, The SMU seems to be handling PCIe power management stuff in AMD northbridges (from RS880 onwards?) the firmware is loaded during system boot. It is unknown if the firmware has to be loaded. The SMU is most likely Altera LM32 CPU.

Intel GB NIC

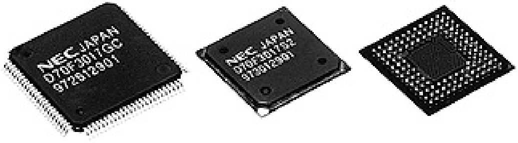
Intel 82574L ethernet controller has had at least a few problems. Including, but not necessarily limited to, EEPROM issues, ASPM bugs, MSI-X quirks, etc.[6] Sometimes internal CPU is so powerful that allows to run custom code on it, like e.g. SSH server.[7]

[6] Kristian Kielhofner (2013). *Packets of Death*.

[7] Arrigo Triulzi (2008). "A SSH server in your NIC". . In: PacSec; L.Duflot Y-A Perez (2010). "Can you still trust your network card?" In: CanSecWest.

USB3 (AMD)

Formerly NEC V850 architecture, now Renesas Electronics V850.[8] 32-bit RISC, gcc toolchain available. This firmware can modified, placed inside UEFI



[8] Luddy Harrison (2005). *NEC - V850 RISC Microcontroller*. University of Illinois, CS433.

HDD/SSD

ARM and MIPS are most common controllers. Part of firmware stored in embedded flash chip and rest of it - on the hidden sectors of disk.

- Seagate HDDs firmware research[9]
- Western Digital HDDs firmware research[10]
- Only Toshiba HDD firmware is not reversed (yet).

[9] Jonas Zaddach (2014). "Exploring the impact of a hard drive backdoor". In: REcon.

[10] Jeroen Domburg (2013). *Hard disk hacking*. OHM.

Mouse

ATmega32u2 in Logitech G600[11]
This is an AVR architecture ("r2 -a avr")

[11] Jacob Maskiewicz et al. (2014). "Mouse Trap: Exploiting Firmware Updates in USB Peripherals". In: *8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association.

Keyboard

KBT Poker II[12] - mechanical keyboard Nuvoton NUC122SC1AN ARM Cortex-M0 CPU

See firmware here: *Extracted Poker II binary*. gist.github.com

[12] *Finding the actual Thumb code in firmware*. RE stackechange.

EC (Embedded Controller)[14]

Keyboard controller, SPI/FWH flash access I2C bus master access

Table: Available vendors

Manufacturer	**Type**
ENE	8051 (8-bit)
Futjitsu	F2MC-16LX (16-bit)
ITE 8051	(8-bit)
Nuvoton (including former Winbond)	CR16 (16-bit), 8051 (8-bit)
Renesas	8051 (8-bit), H8S (16-bit), 740 (8-bit)
NSC	CR16 (16-bit), 8051 (8-bit)
SMSC	8051 (8-bit)
SST	8051 (8-bit)

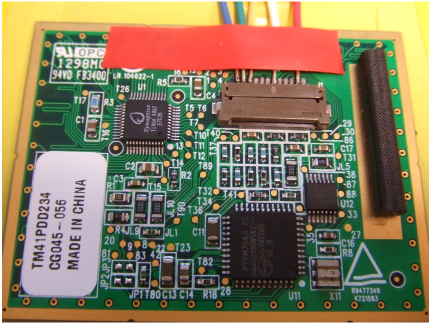
You can get dump of your EC registers using ectool.[13]

[13] *ECtool*. coreboot project.

[14] *Embedded Controller*. coreboot project.

TouchPad

AVR or PIC architecture[15][16]



[15] *Synaptics RMI3 Interfacing Guide* (2008).

[16] *Synaptics TouchPad Interfacing Guide* (2001).

WebCam

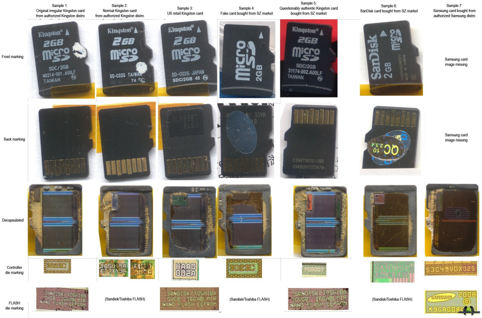
Full featured computer, including CPU and video processor. Very often 8051, H8, AVR or ARM based For example Vimicro VC0343[17] 8051 based one. Can be exploited using the Device Firmware Update (DFU) standard. It allows to start the update without administrator privilegies (for Windows systems).[18]

[17] *Vimicro VS0343 - USB 2.0 Camera Processor* (2011).

[18] Robert Graham (2013). *How to disable webcam light on Windows*.

SD/MMC cards

8051 and H8 processors[19][20][21]


Sample 1:
Original irregular Kingston card from authorized Kingston distro
Sample 2:
Normal Kingston card from authorized Kingston distro
Sample 3:
US retail Kingston card
Sample 4:
Fake card bought from SZ market
Sample 5:
Questionably authentic Kingston card bought from SZ market
Sample 6:
SanDisk card bought from SZ market
Sample 7:
Samsung card bought from authorized Samsung distro
Front marking
Samsung card image missing
Back marking
Samsung card image missing
Decapsulated
Controller die marking
FLASH die marking
(Sandisk/Toshiba FLASH)
(Sandisk/Toshiba FLASH)
(Sandisk/Toshiba FLASH)

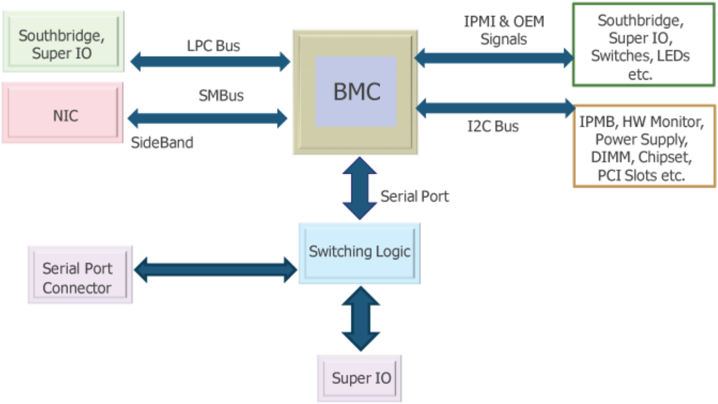
[19] "The Exploration and Exploitation of an SD Memory Card" (2013). In: 30C3.
[20] xobs (2013). *Disassembler and Debugger for AX211 and AX215 8051-based CPU*. . https://github.com/xobs/ax2xx-code.
[21] *Phison microcontroller firmwares and flashers*. usbdev.ru.

BMC

The baseboard management controller is the implementation of IPMI. It is a specialised microcontroller embedded on the mainboard of the server. There are a few various vendors of BMC/IPMI:

- HP iLO
- Dell iDRAC
- IBM RSA
- Intel AMT
- DTMF DASH
- and less common

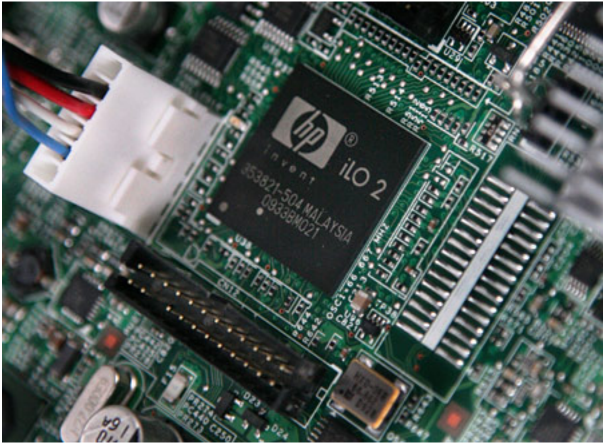
BMC and IPMI



IPMI Block Diagram

HP iLO

- iLO 2 - 66 MHz NEC v850
- table iLO 3/4 - ARM cpu + NAND flash to store firmware (up to 4Gb)



Dell iDRAC

Table: Available versions

Family	**Type**
DRAC II - 5[22]	External PCI/PCIe card
iDRAC 6 - 7	Integrated on motherboard

[22] Ruben (2011). *Reversing Dell's DRAC Firmware.*

BadUSB - USB Flash sticks

8051 and H8 controllers (similar to SD/MMC cards) Alcor Micro, CION, Etron, Hisun, ITE, JMicron, KTC, Netac, OTi, Phison[23], Prolific, SanDisk, TM, Winyatek and many others.

[23] *Phison 2251-03 (2303) Custom Firmware and Existing Firmware Patches.*

PCI/PCIe Option Roms

Each PCI/PCIe device can provide its firmware to start on the main CPU, in the BIOS/UEFI environment, as a driver. So we can just use the same tools and techniques as for BIOS/UEFI reverse engineering.
A lot of research has been done here already.[24][25][26]

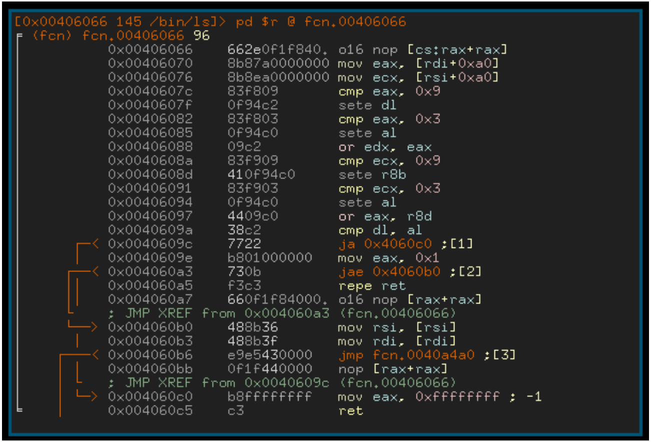
[24] Darmawan Salihun. *Building a Kernel in PCI Expansion ROM*. .

[25] Darmawan Salihun (2006). *BIOS Disassembly Ninjutsu Uncovered*. A-List Publishing. ISBN: 1931769605.

[26] Shikhin Sethi (2014). “Option ROMs: A Hidden (But Privileged) World”. In: H2HC.

What is radare2

This is reverse engineering framework and toolset. Main tool (r2) have two modes of work: command line and visual (V* commands). Also there is a bokken GTK GUI. But we'll use r2 tool instead.



```
[0x00406066 145 /bin/ls]> pd $r @ fcn.00406066
┌ (fcn) fcn.00406066 96
│           0x00406066    662e0f1f840. o16 nop [cs:rax+rax]
│           0x00406070    8b87a0000000 mov eax, [rdi+0xa0]
│           0x00406076    8b8ea0000000 mov ecx, [rsi+0xa0]
│           0x0040607c    83f809       cmp eax, 0x9
│           0x0040607f    0f94c2       sete dl
│           0x00406082    83f803       cmp eax, 0x3
│           0x00406085    0f94c0       sete al
│           0x00406088    09c2         or edx, eax
│           0x0040608a    83f909       cmp ecx, 0x9
│           0x0040608d    410f94c0     sete r8b
│           0x00406091    83f903       cmp ecx, 0x3
│           0x00406094    0f94c0       sete al
│           0x00406097    4409c0       or eax, r8d
│           0x0040609a    38c2         cmp dl, al
│       ┌─< 0x0040609c    7722         ja 0x4060c0 ;[1]
│       │   0x0040609e    b801000000   mov eax, 0x1
│      ┌──< 0x004060a3    730b         jae 0x4060b0 ;[2]
│      ││   0x004060a5    f3c3         repe ret
│      ││   0x004060a7    660f1f84000. o16 nop [rax+rax]
│      └    ; JMP XREF from 0x004060a3 (fcn.00406066)
│      └──> 0x004060b0    488b36       mov rsi, [rsi]
│       │   0x004060b3    488b3f       mov rdi, [rdi]
│     ┌───< 0x004060b6    e9e5430000   jmp fcn.0040a4a0 ;[3]
│     │ │   0x004060bb    0f1f440000   nop [rax+rax]
│     │ └   ; JMP XREF from 0x0040609c (fcn.00406066)
│     │ └─> 0x004060c0    b8ffffffff   mov eax, 0xffffffff ; -1
└     │     0x004060c5    c3           ret
```

Simplest options

Important commands:

- pd - print disassembly
- f - set/show flag
- s - seek
- af - add function
- CC - add comment
- Cd - mark as data
- w* - write back to the file
- Vp - visual modes (note pressing 'p' to switch between them)

x86 radare

Here we do:

- Open legacy BIOS file to reverse
- Open modern system UEFI firmware
- Open PCIe device option rom

Demo 1

DEMO 1

ARM

Used for iLO and iDRAC. You need to properly manage loading adress.

- S - sections command
- io.va - virtual addresses evaluation

```
r2 -a arm -b 32 -e io.va=true some-arm-firmware.bin
[0000000]> S 0 0x10000 0x2000 0x2000 load rwx
```

Demo 2

DEMO 2

8051

Using as part of:

- EC (Embedded Controller)
- Webcam controller
- SD/MMC card controller
- USB Flash sticks controller
- AMD IMC controller
- HDD servo control

Demo 3

DEMO 3

ARC

- Using as part of Intel ME/AMT
- We will open both ARC4 and ARC5 examples

Demo 4

DEMO 4

CR16/CR16+ (CompactRISC16)

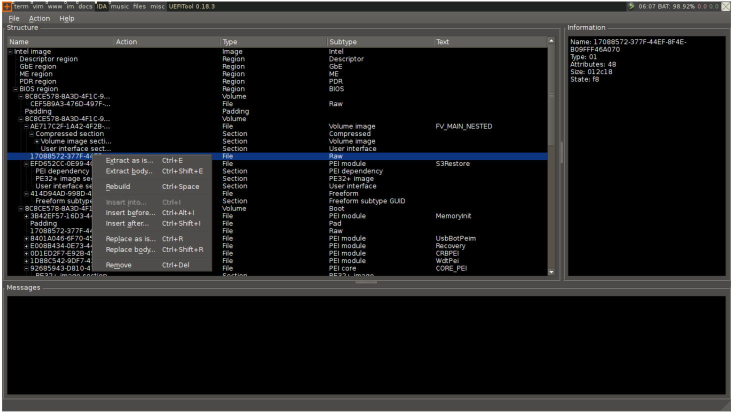
Using as part of EC (Embedded Controller)

Demo 5

DEMO 5

Reversing HP Omnibook 500 EC firmware

UEFITool[27]



Name	Action	Type	Subtype	Text
Intel image		Image	Intel	
Descriptor region		Region	Descriptor	
GbE region		Region	GbE	
ME region		Region	ME	
PDR region		Region	PDR	
BIOS region		Region	BIOS	
8C8CE578-8A3D-4F1C-9...		Volume		
CEF5B9A3-476D-497F-...		File	Raw	
Padding		Padding		
8C8CE578-8A3D-4F1C-9...		Volume		
AE717C2F-1A42-4F2B-...		File	Volume image	FV_MAIN_NESTED
Compressed section		Section	Compressed	
Volume image secti...		Section	Volume image	
User interface sect...		Section	User interface	
17088572-377F-44		File	Raw	
EFD652CC-0E99-40		File	PEI module	S3Restore
PEI dependency		Section	PEI dependency	
PE32+ image se		Section	PE32+ image	
User interface se		Section	User interface	
414D94AD-998D-4		File	Freeform	
Freeform subtype		Section	Freeform subtype GUID	
8C8CE578-8A3D-4F1		Volume	Boot	
3B42EF57-16D3-44		File	PEI module	MemoryInit
Padding		File	Pad	
17088572-377F-44		File	Raw	
8401A046-6F70-45		File	PEI module	UsbBotPeim
E008B434-0E73-44		File	PEI module	Recovery
0D1ED2F7-E92B-45		File	PEI module	CRBPEI
1D88C542-9DF7-42		File	PEI module	WdtPei
92685943-D810-47		File	PEI core	CORE_PEI
PE32+ image section		Section	PE32+ image	

Name: 17088572-377F-44EF-8F4E-B09FFF46A070
Type: 01
Attributes: 48
Size: 012c18
State: f8

This tool have both GUI and CLI versions

[27] Nicolaj Shlej (2013). https://github.com/LongSoft/UEFITool.

Rest of tools

- bios_extract[28]
- dump from memory
- dump from device (using some equipment)
- copy file from the linux sources (for uploadable firmwares)

[28] *Bios_extract*.

Emulation

- SerialICE[29]
- S2E/Avatar[30]
- PANDA[31]

We can use these tools with r2, due to support of gdb:// protocol

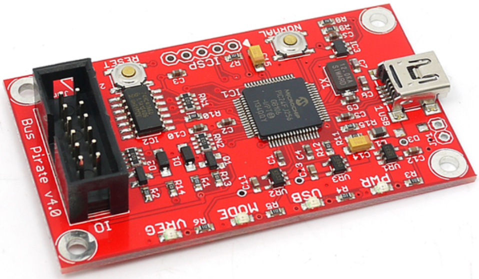
[29] *SerialICE.*. Tracing PC firmware using patched QEMU.

[30] *Avatar - dynamic firmware analysis framework*. based on QEMU.

[31] *PANDA - Platform for Architecture-Neutral Dynamic Analysis*. based on QEMU.

BIOS/UEFI

- UEFI Tool
- + flashrom[32]
- + external programmer (rpi/buspirate)



[32] *flashrom - crossplatform PC firmware flashing tool.*

Embedded Controller

- external programmer
- + patched flashrom or
- + some custom tools

END OF STORY

Thanks for your attention!

Questions?

A lot of them I

- *Avatar - dynamic firmware analysis framework*. based on QEMU.
- *Bios_extract*.
- Domburg, Jeroen (2013). *Hard disk hacking*. OHM.
- *ECtool*. coreboot project.
- *Embedded Controller*. coreboot project.
- *Extracted Poker II binary*. gist.github.com.
- *Finding the actual Thumb code in firmware*. RE stackechange.
- *flashrom - crossplatform PC firmware flashing tool*.
- Graham, Robert (2013). *How to disable webcam light on Windows*.
- Harrison, Luddy (2005). *NEC - V850 RISC Microcontroller*. University of Illinois, CS433.
- Hawker, Ben (2012-2013). *Notes on Intel Microcode Updates*.
- *Intel ME 6.x Huffman algorithm* (2014).
- Kielhofner, Kristian (2013). *Packets of Death*.

A lot of them II

- Maskiewicz, Jacob et al. (2014). “Mouse Trap: Exploiting Firmware Updates in USB Peripherals”. In: *8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association.
- *MEre project* (2013-2014).
- *PANDA - Platform for Architecture-Neutral Dynamic Analysis*. based on QEMU.
- Patrick Stewin, Iurii Bystrov (2013). “Persistent, Stealthy, Remote-controlled Dedicated Hardware Malware”. In: 30C3. Hamburg, Germany.
- *Phison 2251-03 (2303) Custom Firmware and Existing Firmware Patches*.
- *Phison microcontroller firmwares and flashers*. usbdev.ru.
- Ruben (2011). *Reversing Dell’s DRAC Firmware*.
- Salihun, Darmawan. *Building a Kernel in PCI Expansion ROM*.
- — (2006). *BIOS Disassembly Ninjutsu Uncovered*. A-List Publishing. ISBN: 1931769605.

A lot of them III

- *SerialICE*. Tracing PC firmware using patched QEMU.
- Sethi, Shikhin (2014). “Option ROMs: A Hidden (But Privileged) World”. In: H2HC.
- Shlej, Nicolaj (2013). `https://github.com/LongSoft/UEFITool`.
- Skochinsky, Igor (2014). “Intel ME Secrets”. In: REcon.
- *Synaptics RMI3 Interfacing Guide* (2008).
- *Synaptics TouchPad Interfacing Guide* (2001).
- “The Exploration and Exploitation of an SD Memory Card” (2013). In: 30C3.
- Triulzi, Arrigo (2008). “A SSH server in your NIC”. In: PacSec.
- *Vimicro VS0343 - USB 2.0 Camera Processor* (2011).
- xobs (2013). *Disassembler and Debugger for AX211 and AX215 8051-based CPU*. `https://github.com/xobs/ax2xx-code`.
- Y-A Perez, L.Duflot (2010). “Can you still trust your network card?” In: CanSecWest.

A lot of them IV

Zaddach, Jonas (2014). “Exploring the impact of a hard drive backdoor”. In: REcon.