Security of BIOS/UEFI System Firmware from Attacker and Defender Perspectives

Introduction

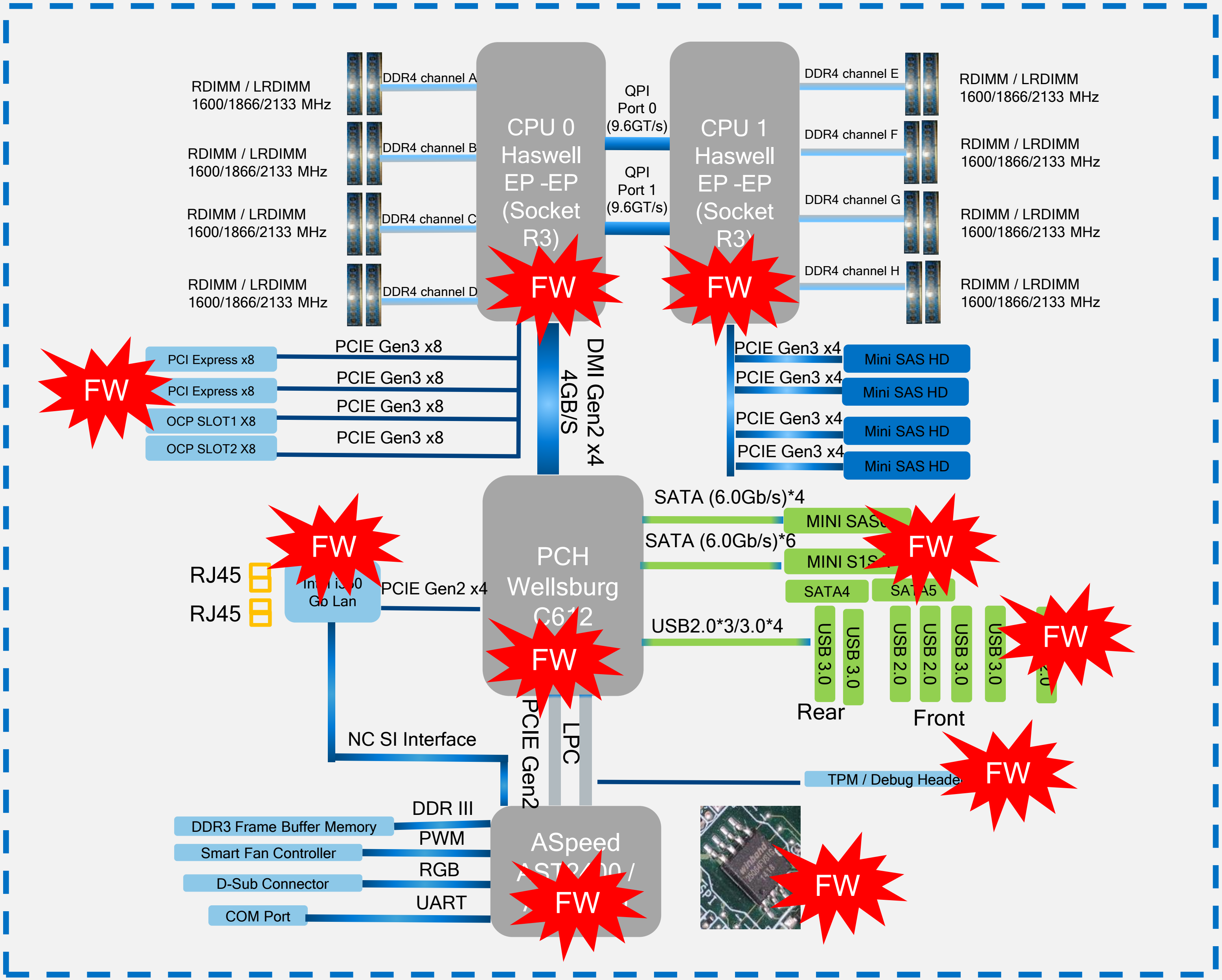
Yuriy Bulygin *
Alex Bazhaniuk *
Andrew Furtak *
John Loucaides **

* Advanced Threat Research, McAfee
** Intel

License

Provide the following attribution:

Derived from “Security of BIOS/UEFI System Firmware from Attacker and Defender Perspective” training by Yuriy Bulygin, Alex Bazhaniuk, Andrew Furtak and John Loucaides available at https://github.com/advanced-threat-research/firmware-security-training



RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel A

RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel B

RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel C

RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel D

CPU 0 Haswell EP -EP (Socket R3)

FW

QPI Port 0 (9.6GT/s)

QPI Port 1 (9.6GT/s)

CPU 1 Haswell EP -EP (Socket R3)

FW

DDR4 channel E

RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel F

RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel G

RDIMM / LRDIMM 1600/1866/2133 MHz

DDR4 channel H

RDIMM / LRDIMM 1600/1866/2133 MHz

FW

PCI Express x8 — PCIE Gen3 x8

PCI Express x8 — PCIE Gen3 x8

OCP SLOT1 X8 — PCIE Gen3 x8

OCP SLOT2 X8 — PCIE Gen3 x8

DMI Gen2 x4 4GB/S

PCIE Gen3 x4 — Mini SAS HD

PCIE Gen3 x4 — Mini SAS HD

PCIE Gen3 x4 — Mini SAS HD

PCIE Gen3 x4 — Mini SAS HD

FW

RJ45

RJ45

Intel i350 Gb Lan

PCIE Gen2 x4

PCH Wellsburg C612

FW

SATA (6.0Gb/s)*4 — MINI SAS

SATA (6.0Gb/s)*6 — MINI SAS

FW

SATA4

SATA5

USB2.0*3/3.0*4

USB 3.0

USB 3.0

Rear

USB 2.0

USB 2.0

USB 3.0

USB 3.0

2.0

Front

FW

NC SI Interface

PCIE Gen2

LPC

TPM / Debug Header

FW

DDR III — DDR3 Frame Buffer Memory

PWM — Smart Fan Controller

RGB — D-Sub Connector

UART — COM Port

ASpeed AST2400 /

FW

FW

Firmware Everywhere

- GBe NIC, WiFi, Bluetooth, WiGig
- Baseband (3G, LTE) Modems
- Sensor Hubs
- NFC, GPS Controllers
- HDD/SSD
- Keyboard and Embedded Controllers
- Battery Gauge
- Baseboard Management Controllers (BMC)
- Graphics/Video
- USB Thumb Drives, keyboards/mice
- Chargers, adapters
- TPM, security coprocessors
- Routers, network appliances
- Main system firmware (BIOS, UEFI firmware, coreboot)

In-the-wild Firmware Attacks

- Legacy Bootkits (TDL4, Gapz…)
- Mebromi BIOS rootkit
- Stuxnet
- EQUATION Group HDD firmware malware
-] Hacking Team [UEFI rootkit
- Petya MBR Ransomware
- Legitimate BIOS “backdoors”: Superfish, Computrace

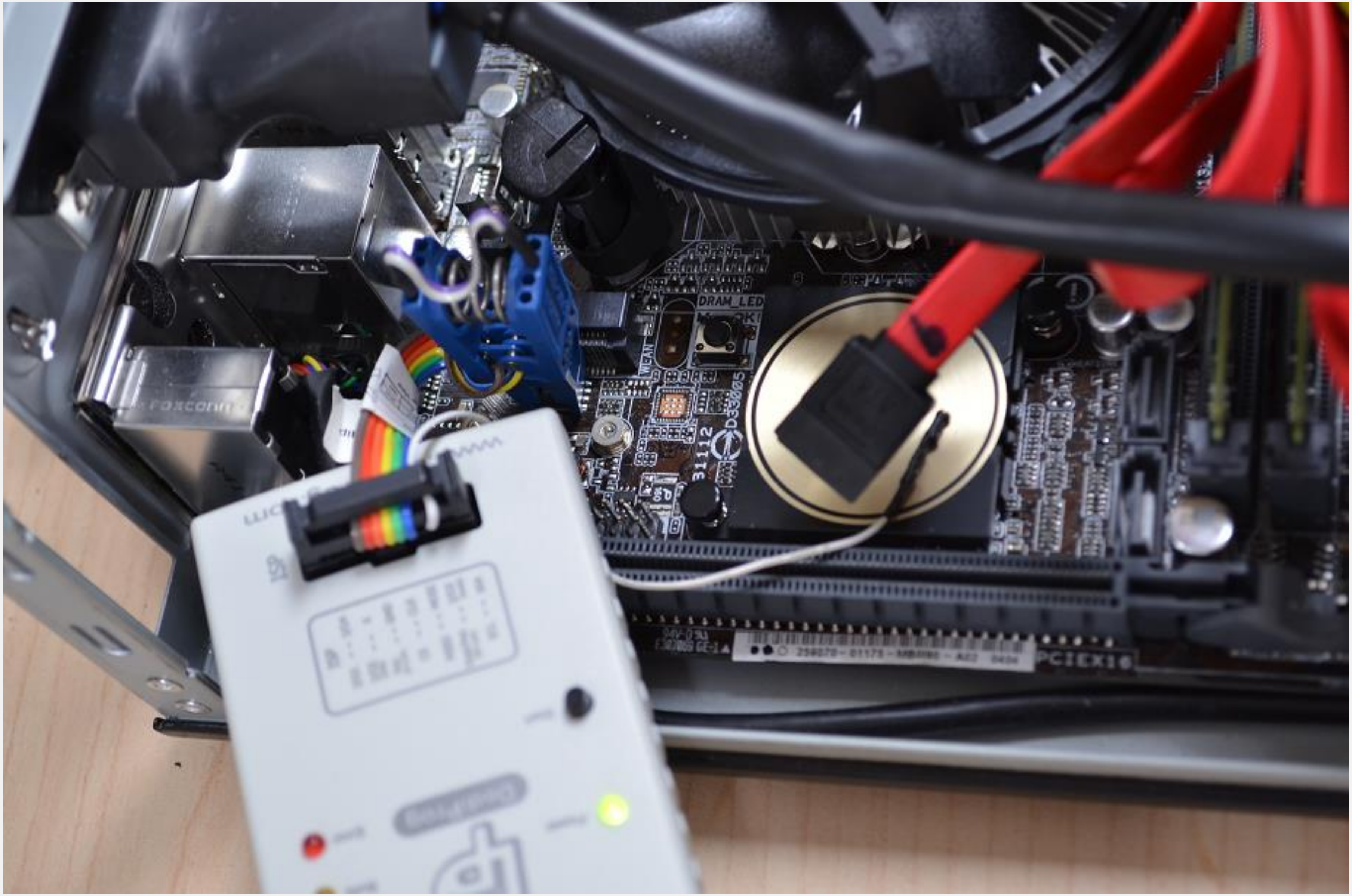
Why Attack Firmware?

- Extreme persistence
- Stealth
- Bypass software (OS or VMM) based security
- Unfettered access to hardware
- OS independence
- Making the system unbootable (bricking)

Extreme Persistence

- System firmware rootkit (in SMM or BIOS/UEFI)
- Replaces OS boot loader every boot
- Which patches OS kernel
- Firmware rootkit is protected by the hardware write protections

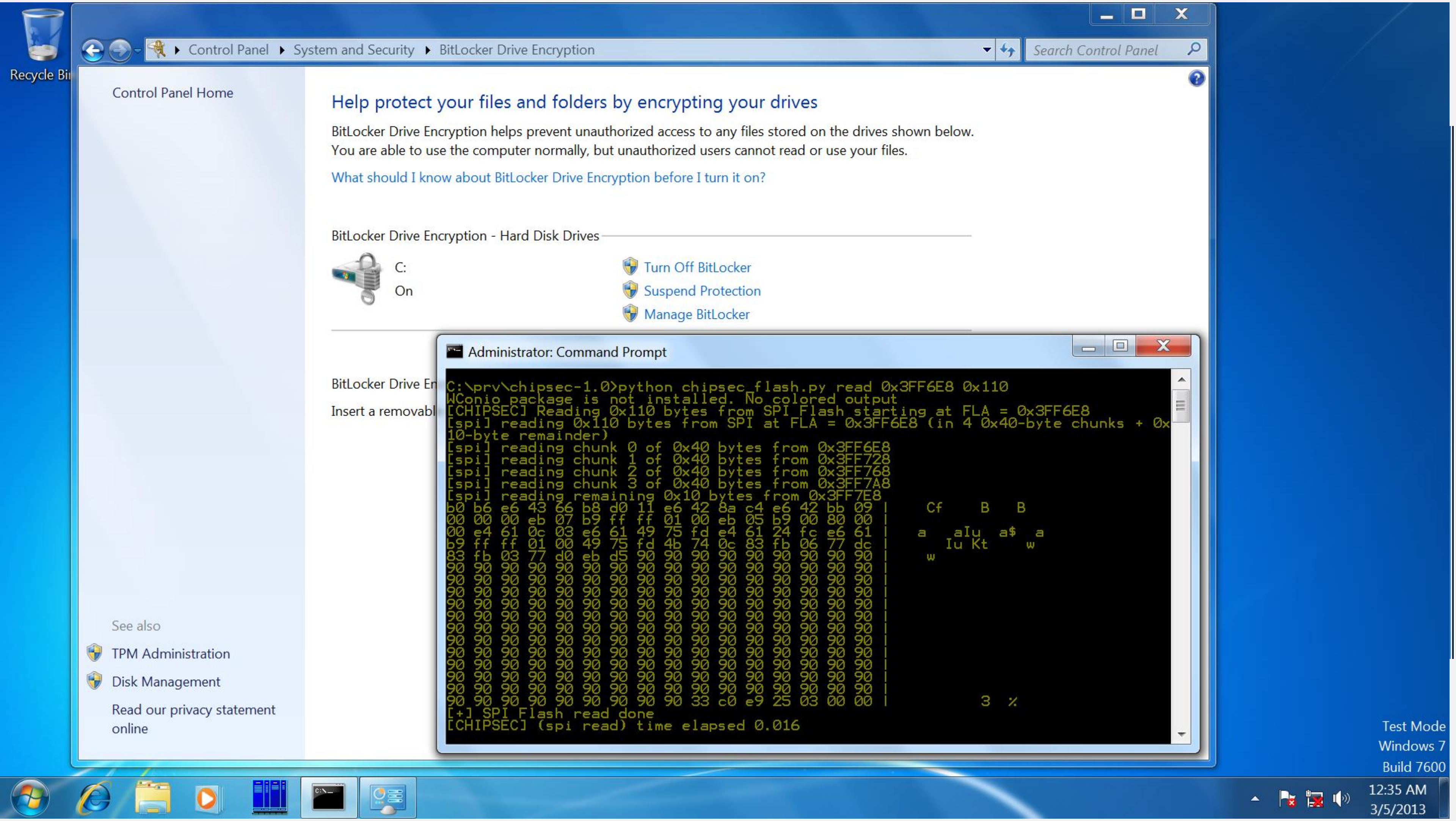
- Only way to fully remove the infection is to physically re-flash the flash “ROM” chip


DRAM_LED
Foxconn
PCIEX16

Stealth

- Security software usually doesn’t monitor all firmware on the platform
- How can software reliably tell infected from good firmware
- Devices use obscure hardware interfaces to their firmware
- Which tool do we use to find BIOS/UEFI infection? And rootkit in firmware of SSD, NIC, EC, BMC, modem, USB thumb-drive, battery gauge, charger?

Bypass Software Security – FDE



Control Panel ▸ System and Security ▸ BitLocker Drive Encryption

Search Control Panel

Control Panel Home

Help protect your files and folders by encrypting your drives

BitLocker Drive Encryption helps prevent unauthorized access to any files stored on the drives shown below. You are able to use the computer normally, but unauthorized users cannot read or use your files.

What should I know about BitLocker Drive Encryption before I turn it on?

BitLocker Drive Encryption - Hard Disk Drives

C:
On

Turn Off BitLocker
Suspend Protection
Manage BitLocker

BitLocker Drive En

Insert a removabl

See also

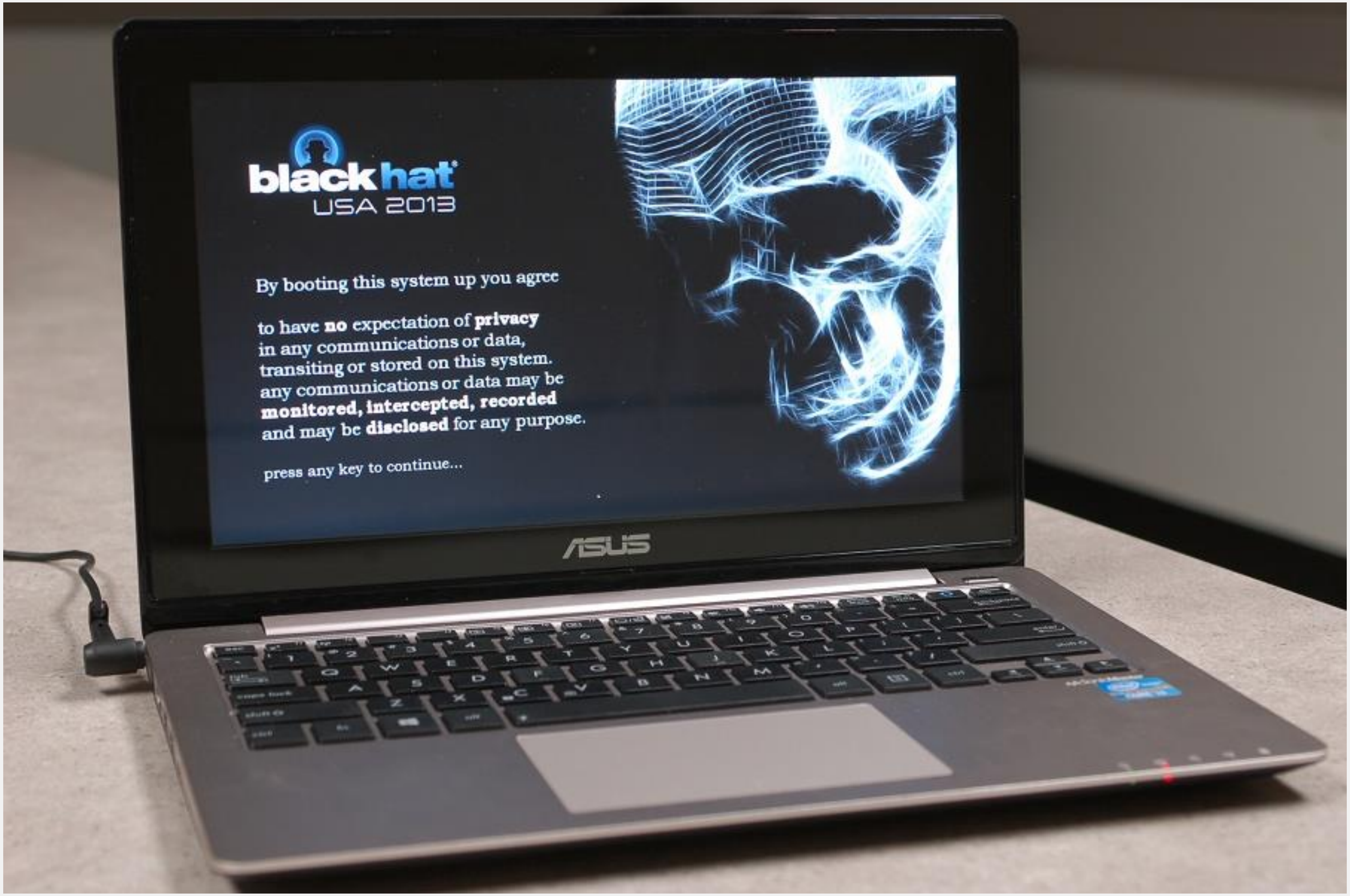
TPM Administration
Disk Management
Read our privacy statement online

Administrator: Command Prompt

```
C:\prv\chipsec-1.0>python chipsec_flash.py read 0x3FF6E8 0x110
WConio package is not installed. No colored output
[CHIPSEC] Reading 0x110 bytes from SPI Flash starting at FLA = 0x3FF6E8
[spi] reading 0x110 bytes from SPI at FLA = 0x3FF6E8 (in 4 0x40-byte chunks + 0x
10-byte remainder)
[spi] reading chunk 0 of 0x40 bytes from 0x3FF6E8
[spi] reading chunk 1 of 0x40 bytes from 0x3FF728
[spi] reading chunk 2 of 0x40 bytes from 0x3FF768
[spi] reading chunk 3 of 0x40 bytes from 0x3FF7A8
[spi] reading remaining 0x10 bytes from 0x3FF7E8
b0 b6 e6 43 66 b8 d0 11 e6 42 8a c4 e6 42 bb 09 |   Cf     B   B
00 00 00 eb 07 b9 ff ff 01 00 eb 05 b9 00 80 00 |
00 e4 61 0c 03 e6 61 49 75 fd e4 61 24 fc e6 61 |   a   aIu  a$  a
b9 ff ff 01 00 49 75 fd 4b 74 0c 83 fb 06 77 dc |      Iu Kt    w
83 fb 03 77 d0 eb d5 90 90 90 90 90 90 90 90 90 |    w
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 |
90 90 90 90 90 90 90 90 90 33 c0 e9 25 03 00 00 |          3  %
[+] SPI Flash read done
[CHIPSEC] (spi read) time elapsed 0.016
```

Source: Evil Maid Just Got Angrier: Why Full-Disk Encryption with TPM is not Secure on Many Systems

Bypass Software Security – Secure Boot



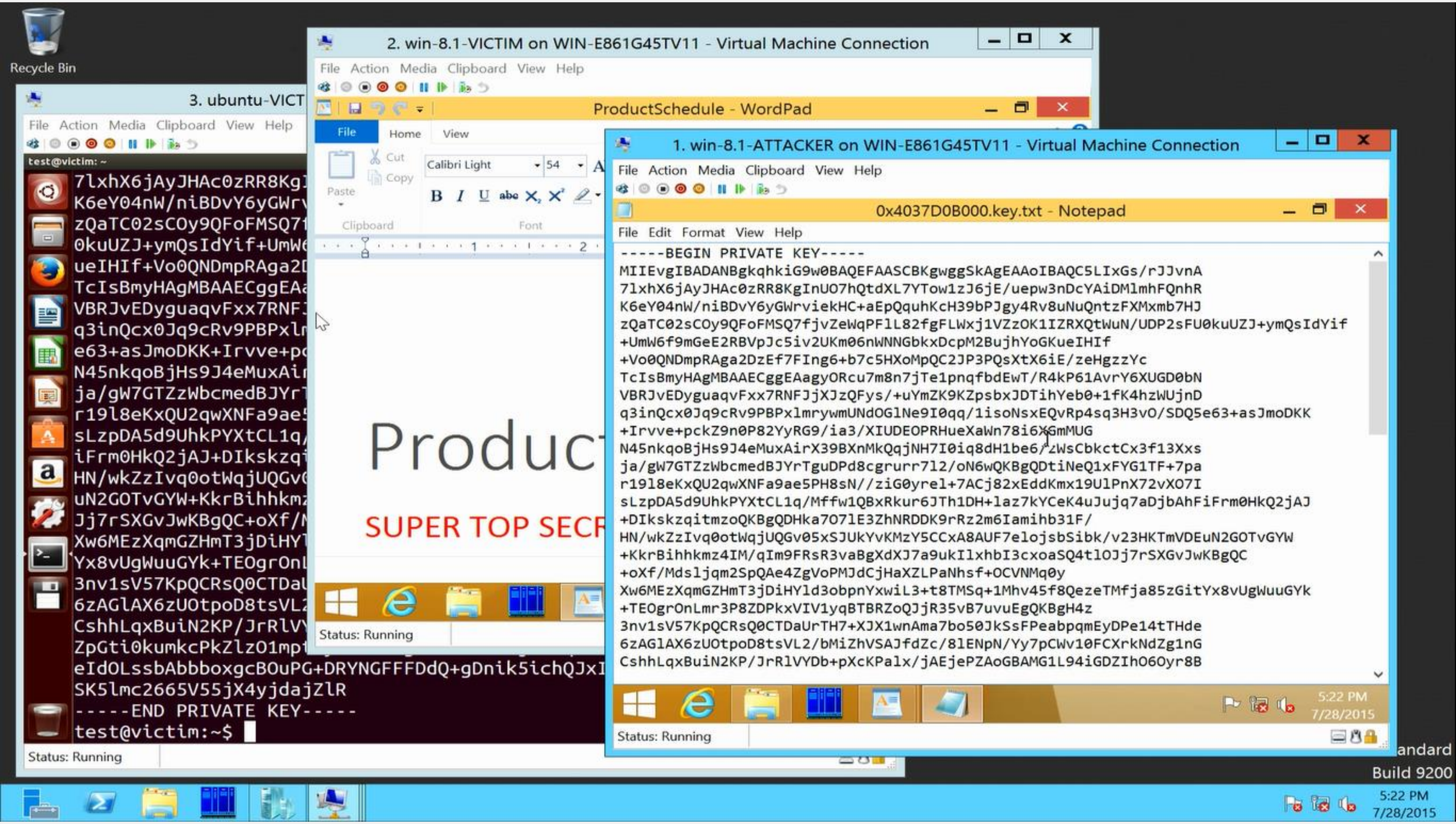
By booting this system up you agree

to have **no** expectation of **privacy** in any communications or data, transiting or stored on this system. any communications or data may be **monitored, intercepted, recorded** and may be **disclosed** for any purpose.

press any key to continue...

Source: A Tale of One Software Bypass of Windows 8 Secure Boot

Bypass Software Security - VMM

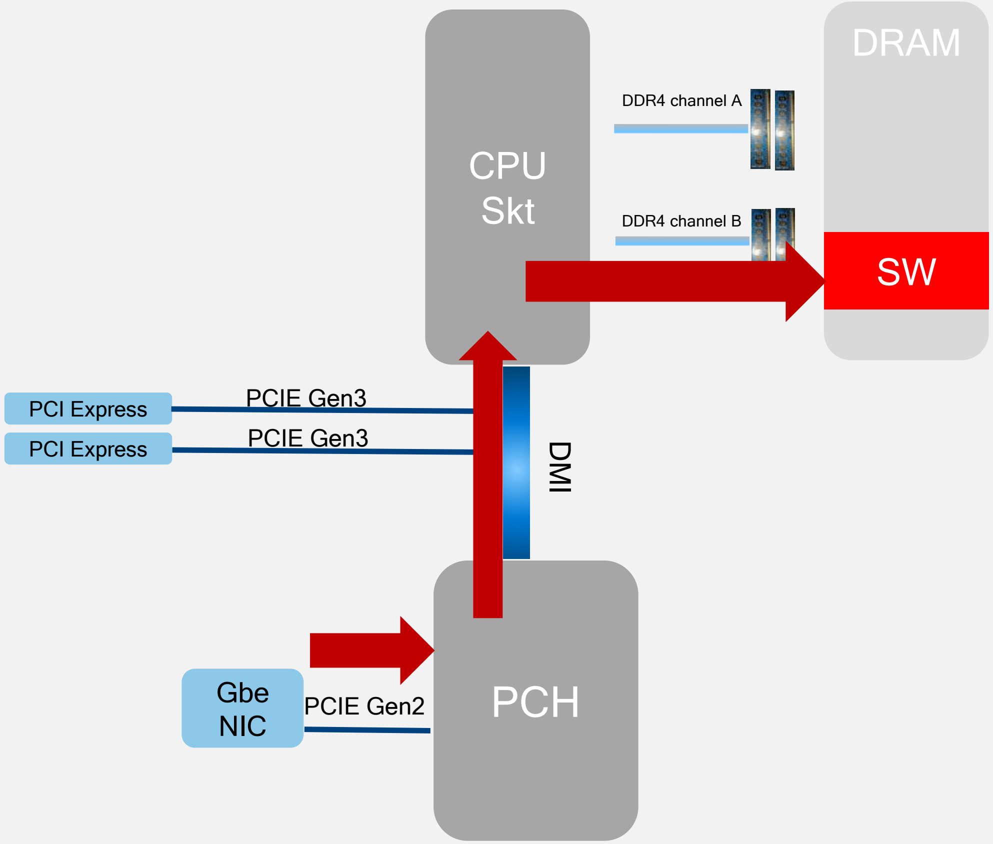

Recycle Bin
3. ubuntu-VICT
File Action Media Clipboard View Help
test@victim: ~
2. win-8.1-VICTIM on WIN-E861G45TV11 - Virtual Machine Connection
File Action Media Clipboard View Help
ProductSchedule - WordPad
File Home View
Paste Cut Copy Clipboard
Calibri Light 54 Font
Produc
SUPER TOP SECR
Status: Running
1. win-8.1-ATTACKER on WIN-E861G45TV11 - Virtual Machine Connection
File Action Media Clipboard View Help
0x4037D0B000.key.txt - Notepad
File Edit Format View Help
5:22 PM
7/28/2015
Status: Running
andard
Build 9200
5:22 PM
7/28/2015

```
7lxhX6jAyJHAc0zRR8KgI
K6eY04nW/niBDvY6yGWrv
zQaTC02sCOy9QFoFMSQ7f
0kuUZJ+ymQsIdYif+UmW6
ueIHIf+Vo0QNDmpRAga2D
TcIsBmyHAgMBAAECggEAa
VBRJvEDyguaqvFxx7RNFJ
q3inQcx0Jq9cRv9PBPxlr
e63+asJmoDKK+Irvve+pc
N45nkqoBjHs9J4eMuxAir
ja/gW7GTZzWbcmedBJYrT
r19l8eKxQU2qwXNFa9ae5
sLzpDA5d9UhkPYXtCL1q/
iFrm0HkQ2jAJ+DIkskzqi
HN/wkZzIvq0otWqjUQGv0
uN2GOTvGYW+KkrBihhkmz
Jj7rSXGvJwKBgQC+oXf/M
Xw6MEzXqmGZHmT3jDiHYl
Yx8vUgWuuGYk+TEOgrOnL
3nv1sV57KpQCRsQ0CTDaU
6zAGlAX6zUOtpoD8tsVL2
CshhLqxBuiN2KP/JrRlVY
ZpGti0kumkcPkZlzO1mpt
eIdOLssbAbbboxgcBOuPG+DRYNGFFFDdQ+gDnik5ichQJxI
SK5lmc2665V55jX4yjdajZlR
-----END PRIVATE KEY-----
test@victim:~$
```

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC5LIxGs/rJJvnA
7lxhX6jAyJHAc0zRR8KgInUO7hQtdXL7YTow1zJ6jE/uepw3nDcYAiDMlmhFQnhR
K6eY04nW/niBDvY6yGWrviekHC+aEpQquhKcH39bPJgy4Rv8uNuQntzFXMxmb7HJ
zQaTC02sCOy9QFoFMSQ7fjvZeWqPFlL82fgFLWxj1VZzOK1IZRXQtWuN/UDP2sFU0kuUZJ+ymQsIdYif
+UmW6f9mGeE2RBVpJc5iv2UKm06nWNNGbkxDcpM2BujhYoGKueIHIf
+Vo0QNDmpRAga2DzEf7FIng6+b7c5HXoMpQC2JP3PQsXtX6iE/zeHgzzYc
TcIsBmyHAgMBAAECggEAagyORcu7m8n7jTe1pnqfbdEwT/R4kP61AvrY6XUGD0bN
VBRJvEDyguaqvFxx7RNFJjXJzQFys/+uYmZK9KZpsbxJDTihYeb0+1fK4hzWUjnD
q3inQcx0Jq9cRv9PBPxlmrywmUNdOGlNe9I0qq/1isoNsxEQvRp4sq3H3vO/SDQ5e63+asJmoDKK
+Irvve+pckZ9n0P82YyRG9/ia3/XIUDEOPRHueXaWn78i6XGmMUG
N45nkqoBjHs9J4eMuxAirX39BXnMkQqjNH7I0iq8dH1be6/zWsCbkctCx3f13Xxs
ja/gW7GTZzWbcmedBJYrTguDPd8cgrurr7l2/oN6wQKBgQDtiNeQ1xFYG1TF+7pa
r19l8eKxQU2qwXNFa9ae5PH8sN//ziG0yrel+7ACj82xEddKmx19UlPnX72vXO7I
sLzpDA5d9UhkPYXtCL1q/Mffw1QBxRkur6JTh1DH+laz7kYCeK4uJujq7aDjbAhFiFrm0HkQ2jAJ
+DIkskzqitmzoQKBgQDHka7O7lE3ZhNRDDK9rRz2m6Iamihb31F/
HN/wkZzIvq0otWqjUQGv05xSJUkYvKMzY5CCxA8AUF7elojsbSibk/v23HKTmVDEuN2GOTvGYW
+KkrBihhkmz4IM/qIm9FRsR3vaBgXdXJ7a9ukIlxhbI3cxoaSQ4tlOJj7rSXGvJwKBgQC
+oXf/Mdsljqm2SpQAe4ZgVoPMJdCjHaXZLPaNhsf+OCVNMq0y
Xw6MEzXqmGZHmT3jDiHYld3obpnYxwiL3+t8TMSq+1Mhv45f8QezeTMfja85zGitYx8vUgWuuGYk
+TEOgrOnLmr3P8ZDPkxVIV1yqBTBRZoQJjR35vB7uvuEgQKBgH4z
3nv1sV57KpQCRsQ0CTDaUrTH7+XJX1wnAma7bo50JkSsFPeabpqmEyDPe14tTHde
6zAGlAX6zUOtpoD8tsVL2/bMiZhVSAJfdZc/8lENpN/Yy7pCWv10FCXrkNdZg1nG
CshhLqxBuiN2KP/JrRlVYDb+pXcKPalx/jAEjePZAoGBAMG1L94iGDZIhO6Oyr8B
```

Source: Attacking Hypervisors via Firmware and Hardware

Unfettered Access to Hardware - DRAM



Attacks compromising firmware on peripheral I/O devices can use inbound direct memory access (DMA) to expose sensitive contents in DRAM or modify software directly in DRAM

Reference: I/O Attacks in Intel-PC Architecture and Countermeasures by F. Lone Sang et al

Unfettered Access to Hardware – HDD/SSD

Access to all data stored on HDD/SDD

Even when data is stored on self-encrypting drives (SED)

Example: Equation Group HDD firmware malware

- Destroying your hard driver is the only way to stop this super-advanced malware

Unfettered Access to Hardware

- NIC, WiFi, baseband modem firmware rootkits have direct access to network communications
- EC or BMC firmware rootkit has access to platform management functions (power, thermal, NIC, keystrokes)
- …

Making System Unbootable (Bricking)

- Corrupt firmware or
- Corrupt critical configuration
- Stored in flash “ROM” memory
- Of a device which is critical for system to boot or operate

References

UEFI/BIOS Security

- Security Issues Related to Pentium System Management Mode (CSW 2006)
- Implementing and Detecting an ACPI BIOS Rootkit (BlackHat EU 2006)
- Implementing and Detecting a PCI Rootkit (BlackHat DC 2007)
- Programmed I/O accesses: a threat to Virtual Machine Monitors? (PacSec 2007)
- Hacking the Extensible Firmware Interface (BlackHat USA 2007)
- BIOS Boot Hijacking And VMWare Vulnerabilities Digging (PoC 2007)
- Bypassing pre-boot authentication passwords (DEF CON 16)
- Using SMM for "Other Purposes“ (Phrack65)
- Persistent BIOS Infection (Phrack66)
- A New Breed of Malware: The SMM Rootkit (BlackHat USA 2008)
- Preventing & Detecting Xen Hypervisor Subversions (BlackHat USA 2008)
- A Real SMM Rootkit: Reversing and Hooking BIOS SMI Handlers (Phrack66)
- Attacking Intel BIOS (BlackHat USA 2009)
- Getting Into the SMRAM: SMM Reloaded (CSW 2009, CSW 2009)
- Attacking SMM Memory via Intel Cache Poisoning (ITL 2009)
- BIOS SMM Privilege Escalation Vulnerabilities (bugtraq 2009)
- System Management Mode Design and Security Issues (IT Defense 2010)
- Analysis of building blocks and attack vectors associated with UEFI (SANS Institute)
- (U)EFI Bootkits (BlackHat USA 2012 @snare, SaferBytes 2012 Andrea Allievi, HITB 2013)
- Evil Maid Just Got Angrier (CSW 2013)
- A Tale of One Software Bypass of Windows 8 Secure Boot (BlackHat USA 2013)
- BIOS Chronomancy (NoSuchCon 2013, BlackHat USA 2013, Hack.lu 2013)
- Defeating Signed BIOS Enforcement (PacSec 2013, Ekoparty 2013)
- UEFI and PCI BootKit (PacSec 2013)
- Meet ‘badBIOS’ the mysterious Mac and PC malware that jumps airgaps (#badBios)
- All Your Boot Are Belong To Us (CanSecWest 2014 Intel and MITRE)
- Setup for Failure: Defeating Secure Boot (Syscan 2014)
- Setup for Failure: More Ways to Defeat Secure Boot (HITB 2014)
- Analytics, and Scalability, and UEFI Exploitation (INFILTRATE 2014)
- PC Firmware Attacks, Copernicus and You (AusCERT 2014)
- Thunderstrike (https://trmm.net/Thunderstrike)
- Extreme Privilege Escalation (BlackHat USA 2014)
- Attacks on UEFI Security (31C3)
- A new class of vulnerabilities in SMI Handlers (CanSecWest 2015)
- Attacking and Defending BIOS in 2015 (RECon 2015)
- Exploiting UEFI boot script table vulnerability (My aimful life)
- Technical details of the S3 resume boot script vulnerability (ATR)
- How you Mac firmware security is completely broken (reverse.put.as)
- Building reliable SMM backdoor for UEFI based systems (My aimful life)
- Breaking UEFI security with software DMA attacks (My aimful life)
- Attacking Hypervisors Using Firmware and Hardware (Black Hat USA 2015)
- Exploiting SMM Callout Vulnerabilities in Lenovo firmware (My aimful life)

Other Firmware Security

- CPU/SoC
  - ITL papers (website)
  - AMD x86 SMU firmware analysis (https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2503/original/ccc-final.pdf) by Rudolf Marek
  - The Memory Sinkhole (https://www.blackhat.com/docs/us-15/materials/us-15-Domas-The-Memory-Sinkhole-Unleashing-An-x86-Design-Flaw-Allowing-Universal-Privilege-Escalation.pdf) by Christopher Domas
  - Full TrustZone Exploit for MSM8974 (http://bits-please.blogspot.com/2015/08/full-trustzone-exploit-for-msm8974.html?m=1)
  - QSEE privilege escalation vulnerability CVE-2015-6639 (http://bits-please.blogspot.com/2016/05/qsee-privilege-escalation-vulnerability.html?m=1)
- USB
  - Turning USB Peripheral to BadUSB (https://srlabs.de/badusb/)
  - Practical BadUSB attack software (https://github.com/adamcaudill/Psychson)
- DRAM
  - Cold Boot attacks (https://citp.princeton.edu/research/memory/)
  - Exploiting the DRAM rowhammer bug (http://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html?m=1)
- Battery
  - Battery Firmware Hacking (https://reverse.put.as/wp-content/uploads/2011/06/Battery-Firmware-Hacking.pdf) by Charlie Miller
- NIC
  - NIC SSH Rootkit (http://cryptome.org/2014/02/nic-ssh-rootkit.htm) by Arrigo Triulzi
  - Project Maux Mk.II (http://www.alchemistowl.org/arrigo/Papers/Arrigo-Triulzi-PACSEC08-Project-Maux-II.pdf) by Arrigo Triulzi
- Management Controllers
  - IPMI: Freight Train to Hell (http://fish2.com/ipmi/bp.pdf) by Dan Farmer
  - Sticky finger and KBC custom shop (http://esec-lab.sogeti.com/static/publications/11-recon-stickyfingers_slides.pdf) by Alexandre Gazet
  - Illuminating the security issues surrounding Lights-Out server management (https://jhalderm.com/pub/papers/ipmi-woot13.pdf)

Training materials are available on Github

https://github.com/advanced-threat-research/firmware-security-training

Yuriy Bulygin	@c7zero
Alex Bazhaniuk	@ABazhaniuk
Andrew Furtak	@a_furtak
John Loucaides	@JohnLoucaides