Security Research

Evil Maids Hate This Trick

Hassan Mohamad

Security Research

Fragerunde

About me

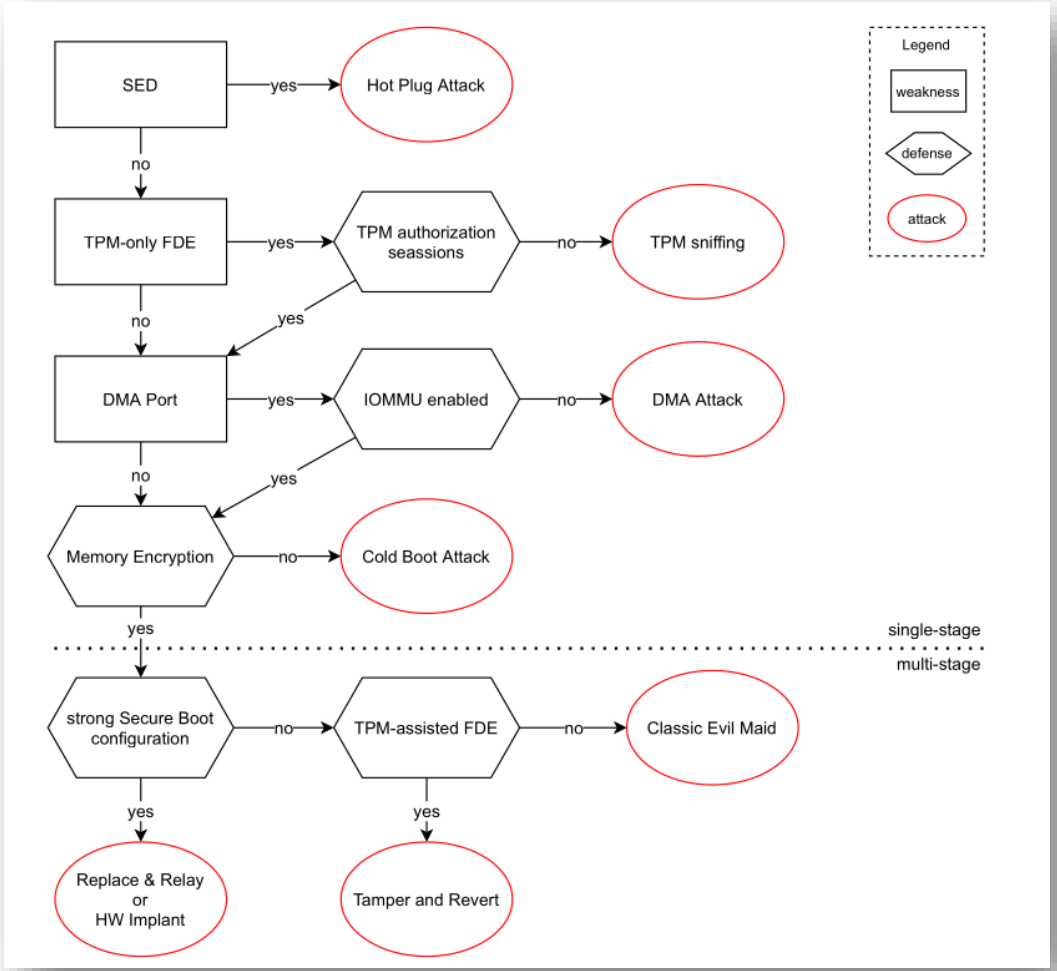
- Bachelor & Master IT Security @ FHSTP
- 3 Jahre Digital Forensics @ Deloitte
- Team Lead Offensive Security @ Sec-Research
  - Red Teaming
  - IT & OT
  - Hardware Testing

Threat Model

- Full Disk Encryption, vernünftiges PW
- Gerät ist gesperrt oder ausgeschalten
- Angreifer will Daten auslesen, verschafft sich
- Angriffe in mehreren Schritten auch möglich
- Out of Scope:
  - Angriffe auf Algorithmen (AES, SHA)
  - „Rubber-hose Cryptanalysis“

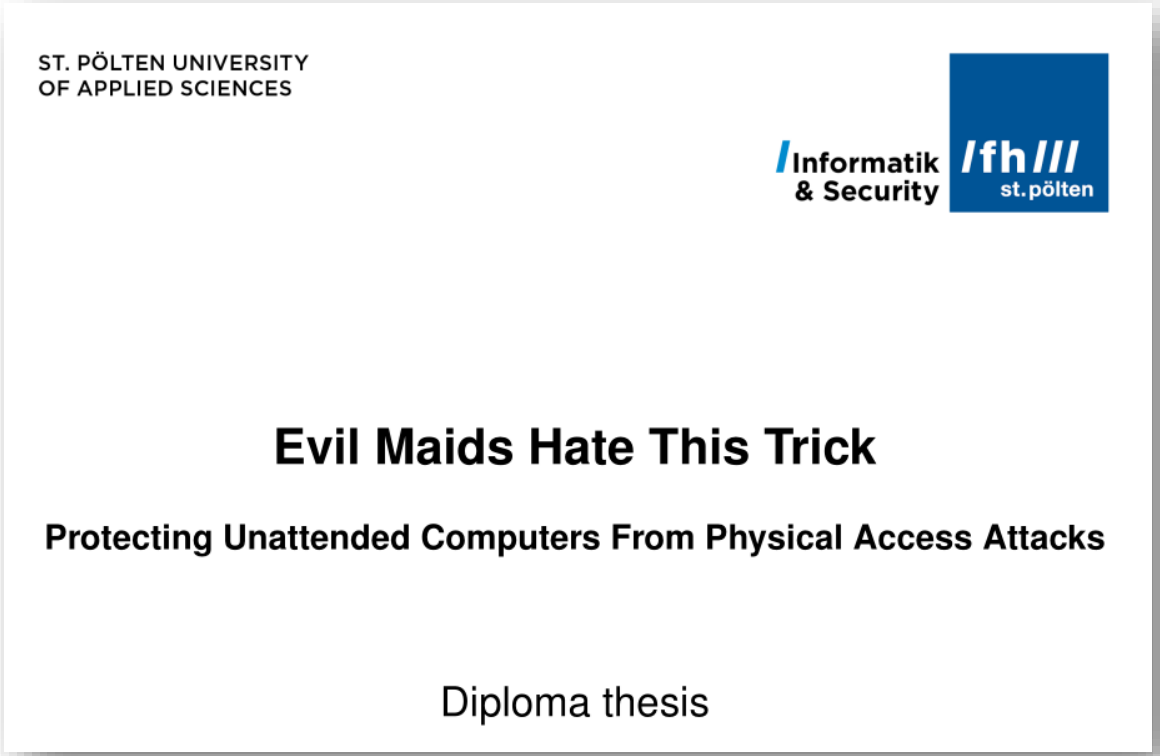
Letztes Jahr:

Ref: [5]


SED
yes
Hot Plug Attack
no
TPM-only FDE
yes
TPM authorization seassions
no
TPM sniffing
no
yes
DMA Port
yes
IOMMU enabled
no
DMA Attack
no
yes
Memory Encryption
no
Cold Boot Attack
yes
single-stage
multi-stage
strong Secure Boot configuration
no
TPM-assisted FDE
no
Classic Evil Maid
yes
yes
Replace & Relay or HW Implant
Tamper and Revert
Legend
weakness
defense
attack

Ref: [5]

Heuer:



ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik
& Security

fh
st.pölten

Evil Maids Hate This Trick

Protecting Unattended Computers From Physical Access Attacks

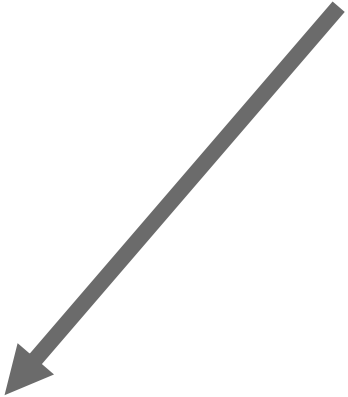
Diploma thesis

Countermeasure	Drive-by Attack									Evil Maid Attack					
	DMA attack (ext. port)	DMA attack (int. port)	Cold boot attack	SED attacks	TPM sniffing	TPM reset attack	Platform reset attack	fTPM fault injection	Invasive silicon attacks	Original evil maid	Tamper & revert	Replace & relay	Advanced R & R	Hardware keylogger	Hardware implants
DMA port authorization	◐	-	-	-	-	-	-	-	-	-	-	-	-	-	-
DMA remapping	◐	◐	-	-	-	-	-	-	-	-	-	-	-	-	-
Memory encryption	-	-	●	-	-	-	-	-	-	-	-	-	-	-	-
Software-based FDE	-	-	-	●	-	-	-	-	-	-	-	-	-	-	-
Power off or hibernate	●	●	●	◐	-	-	-	-	-	-	-	-	-	-	-
TPM + PIN	-	-	-	-	●	●	●	-	-	●	◐	◐	-	◐	-
Strong TPM + PIN impl.	-	-	-	-	●	●	●	◐	◐	●	◐	◐	-	◐	-
TPM + key file	-	-	-	-	●	●	●	●	●	●	◐	◐	-	●	-
TPM auth. sessions	-	-	-	-	●	-	-	-	-	-	-	-	-	-	-
Anti evil maid	-	-	-	-	-	-	-	-	-	◐	◐	-	-	-	-
TOTP-based AEM	-	-	-	-	-	-	-	-	-	●	●	◐	-	-	-
Hardened Secure Boot	-	-	-	-	-	◐	●	-	-	●	●	-	-	-	-
Tamper-evident seals	-	-	-	-	-	-	-	-	-	-	-	◐	◐	◐	◐
Case intrusion sensors	-	-	-	-	-	-	-	-	-	-	-	-	-	◐	◐
External tamper sensors	-	-	-	-	-	-	-	-	-	●	●	●	●	◐	◐
Sum of countermeasures	●	●	●	●	●	●	●	●	●	●	●	●	●	●	◐

● = prevents; ◐ = partially mitigates; - = does not mitigate;

Security Research

Quellen!



Ref: [x], [y]

Cold Boot Angriff

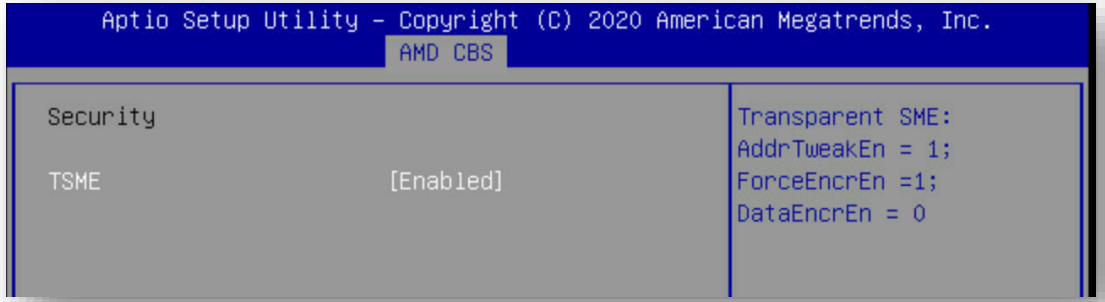
Cold Boot Angriff

- RAM kühlen
- (transplantieren)
- RAM auslesen (**`memimage`**)
- FDE Keys identifizieren (aes**`keyfind`**)
- Ggf. reparieren (**`aesfix`**)

Ref: [2], [56]—[60]

Memory Encryption

- AMD Transparent Secure Memory Encryption (TSME)
  - Aka *AMD Memory Guard* oder *Infinity Guard*
  - Verfügbarkeit: Ryzen PRO und EPYC
- Intel Total Memory Encryption (TME)
  - Verfügbarkeit: ab 11th Gen Core with vPro, ab 3rd Gen Xeon Scalable
- Völlig transparent
- Aktivierbar im BIOS



Ref: [73], [74]

DMA Angriffe

DMA-fähige Ports

- PCIe (auch M.2)
- Thunderbolt (auch via USB C)
- USB4
- Firewire, ExpressCard, ..

PCILeech

Step 1 – Load Kernel Modules
Target:
- Windows 7x64
- Windows 10x64
- Windows 10x64_3 (memmap method)

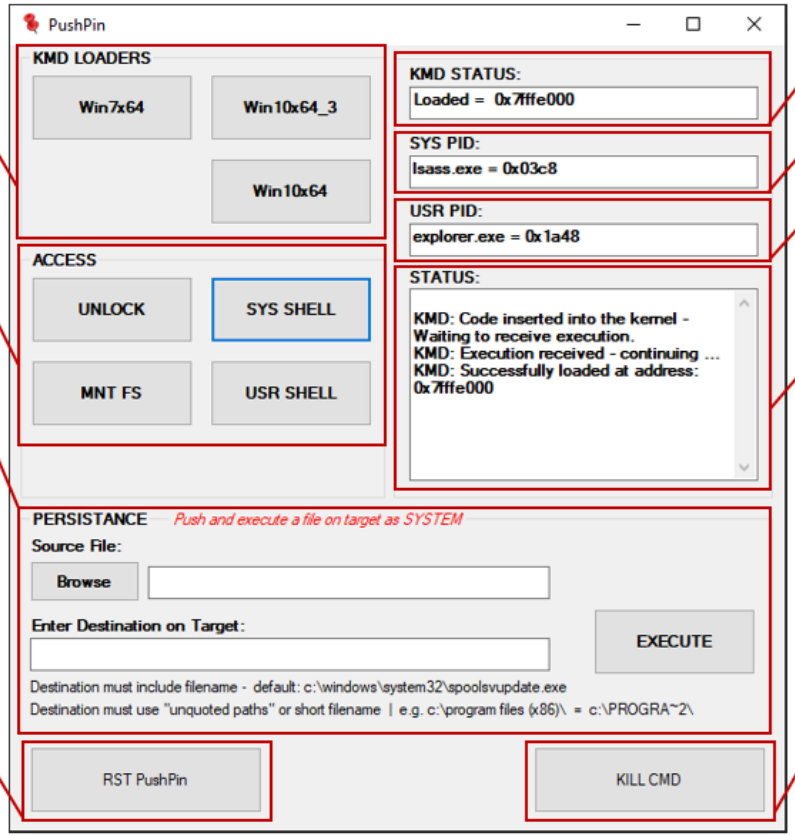
Step 2 – Load Kernel Implants
- Unlock/bypass password login
- USER or SYSTEM CMD Shell
- Mount the File system/memory

Step 2 – Load Kernel Implants
- Push and execute a file on the target as SYSTEM.

You control the source and destination file. This is tested with exes. You must use a unquoted destination path or use short filename format and include the filename with extension. If you don't provide a path the default is c:\windows\system32\spoolsvupdate.exe

Be careful this function will create or overwrite whatever file you point it at.

Reset Button
- Clears all status windows
- Resets stored values



KMD Status Window
- Shows the address of the loaded KMD
- This address is stored and used in attacks

SYS PID Window
- The PID of lsass.exe is always SYSTEM
- This address is stored and used in attacks

USR PID Window
- The PID of explorer.exe is always a USER
- This address is stored and used in attacks

STATUS Window
- Displays PCILeech and other status messages
- Look here if things aren't working

KILL CMD Button
- Closes all CMD shell windows

Security Research

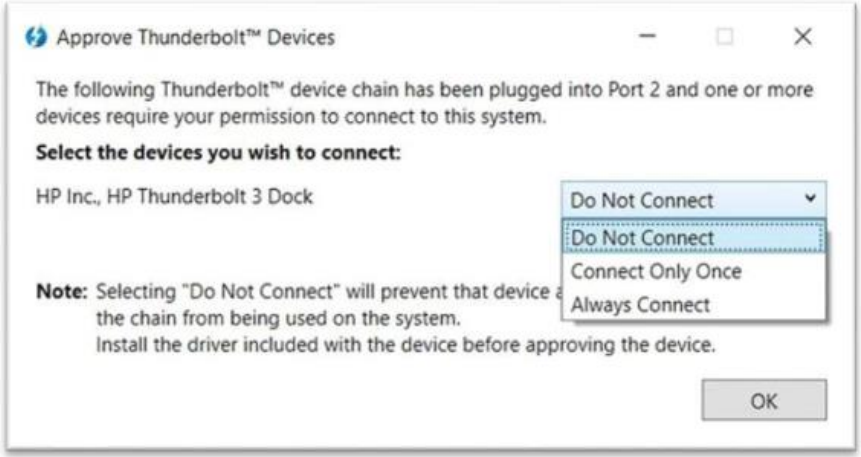
Thunderbolt “Security” Levels

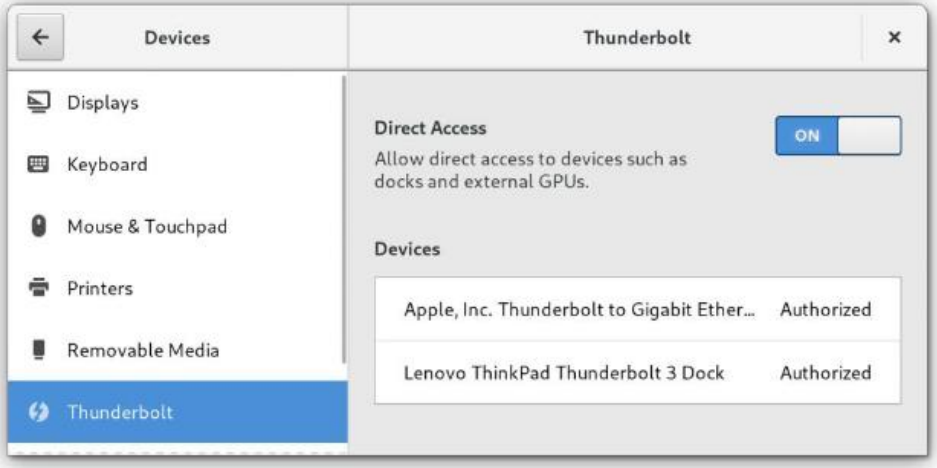
- Thunderbolt 2+ / USB4
- Verschiedene Sicherheitsstufen
  - No Security (SL0)
  - User Authorization (SL1)
  - Secure Connect (SL2)
  - Disable PCIe (SL3)
- Im BIOS konfigurierbar

Ref: [33], [34]

Security Research

Thunderbolt “Security” Levels





Ref: [33], [34]

THUNDERSPY (2020)

- UUID spoofing
- SPI Chip ungeschützt
- Abwärtskompatibilität ausnutzbar
- Intel: “use the IOMMU!”

Ref: [34]—[36]

Security Research

IO Memory Management Unit

+ Analog zur MMU für Prozessisolierung
+ Beschränkt DMA auf dedizierte Bereiche
– Benötigt OS- und Treiber-Support
– Page (4 KB) Granularity
– Delayed Invalidation
– Address Translation Services (ATS)

Ref: [32], [48]—[50]

Security Research

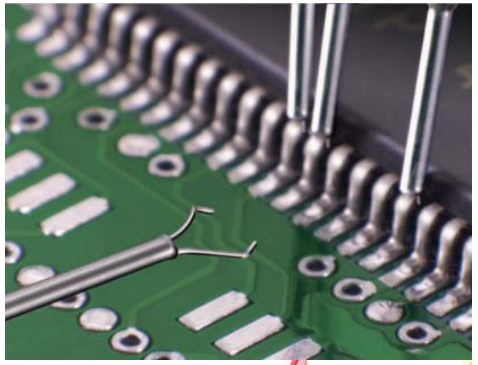
Best-Effort Schutz

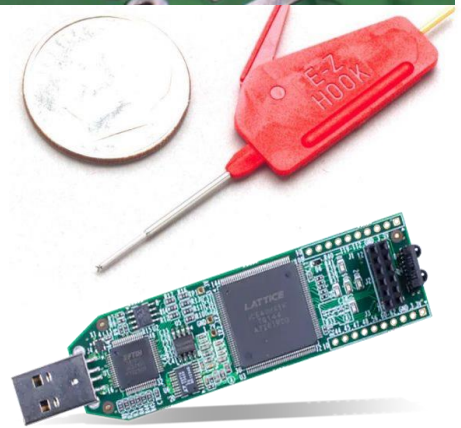
- Thunderbolt Security Level: SL3
- IOMMU aktivieren:
  - AMD: BIOS Setting “AMD V” oder “SVM”
  - Intel: BIOS Setting “Intel VT-d” + Kernel Parameter `intel_iommu=on`
- IOMMU Hardening Kernel Parameter:
  - `efi=disable_early_pci_dma`
  - `iommu.strict=1`
  - `pci=noats`
- Ungenutzte PCIe Slots deaktivieren
- Vollständiger Schutz: Computer ausschalten/hibernate

TPM Angriffe

TPM Angriffe

- Bei TPM-based FDE relevant
- discrete TPM (dTPM)
  - Anfällig für TPM Sniffing, TPM Reset Attacks etc.
  - Lösung: Authorization Sessions, PIN
- firmware TPM (fTPM)
  - Anfällig für Angriffe auf das Trusted Execution Environment (TEE)
- dTPM gilt als sicherer
  - PIN oder Key File als 2. Faktor





Ref: [79]--[89]

Security Research

Linux FDE Lösungen

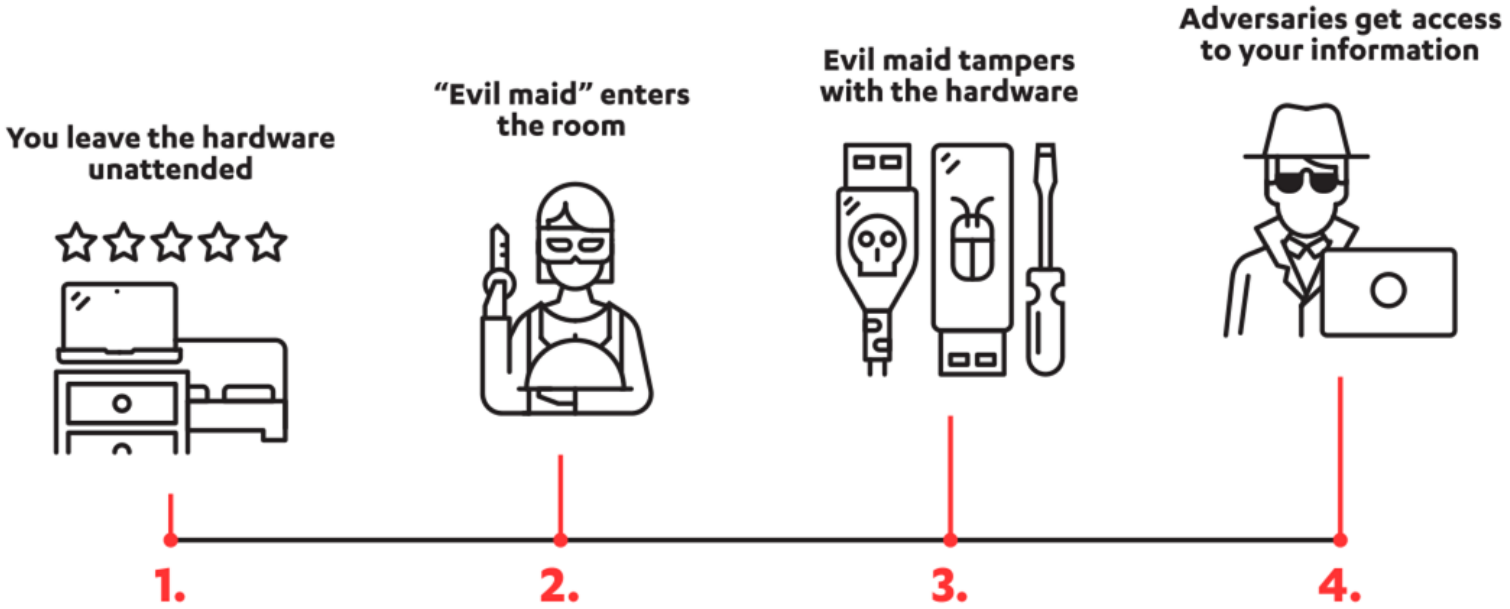
Solution (version)	Param. enc.	TPM authenticity check	TPM + PIN	TPM + key file
Clevis (19)	-	-	-	-
LUKS TPM2 (2.1.2)	-	-	◐	◐
safeboot (0.7)	-	-	◐	-
systemd-cryptenroll (254)	●	●	◐	-
BitLocker	-	-	●	●

● = implemented; ◐ = partially/insecurely implemented; - = not implemented;

Evil Maid Angriffe

Security Research

Evil Maid Angriff - Ablauf



Evil Maid: Software-basiert

- Manipulation von Boot-Komponenten
  - Software Keylogger (BitLocker, LUKS, TrueCrypt)
  - Auch Keyfiles betroffen
- Unser Ziel: Manipulation verhindern/erkennen
- Unsere Mittel:
  - Secure Boot
  - Mutual Authentication

Ref: [3], [4]

UEFI/BIOS Hardening

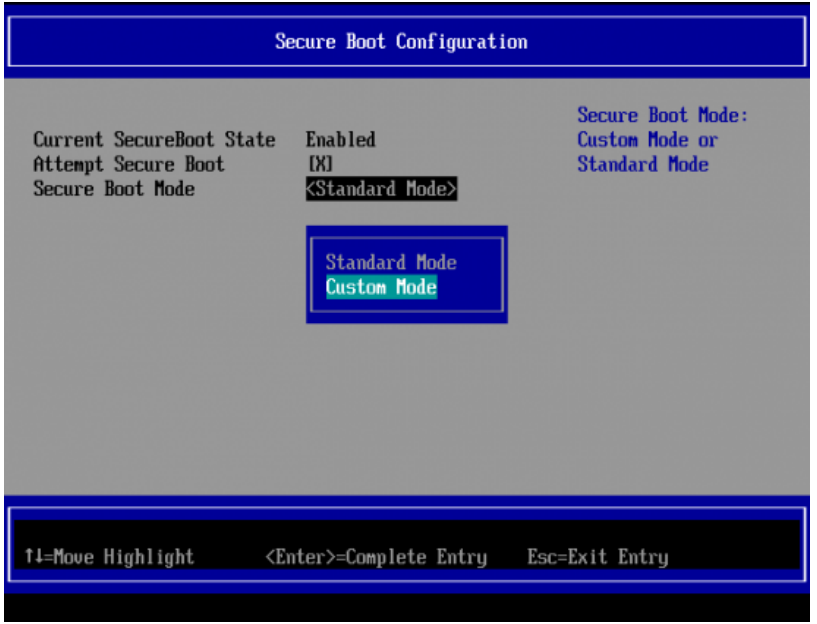
- Administrator/Supervisor Passwort setzen
- “Lock UEFI BIOS settings”
- Fast-Boot deaktivieren
- Regelmäßige Firmware Updates

Ref: [142]

Secure Boot

- Prüft Signatur von EFI Programmen
- Default Keys:
  - Microsoft Windows Production CA
  - Microsoft 3rd Party UEFI CA
- Tausende EFI Programme signiert
- BootHole Schwachstelle als Beispiel

--> Eigene Keys Verwenden



Ref: [112]

Meet sbctl

1. Secure Boot Keys erstellen:
   ```
   $ sbctl create-keys
   ```
2. Unified Kernel image (UKI) erstellen:
   ```
   $ sbctl create-bundle …
   ```
3. UKI signieren:
   ```
   $ sbctl sign $UKI
   ```
4. Keys einspielen:
   ```
   $ sbctl enroll-keys
   ```
5. Secure Boot aktivieren

Ref: [144]

Mutual Auth – TPM2-TOTP

- Selbes Prinzip wie bei 2FA
- TOTP-Secret mit TPM versiegelt
- Secret verfügbar wenn SB intakt

Ref: [108]

Evil Maid: Hardware-

- Hardware Keylogger
- Auch Laptops betroffen
- Akustisches Keylogging
- Snowden Leaks 2013
  - NSA ANT Katalog (2009)
  - USB, JTAG, PCIe Implants

TOP SECRET//COMINT//REL TO USA, FVEY

RAGEMASTER

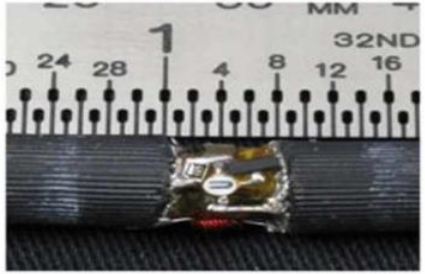
ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing

Ref: [4], [115]—[121], [124]—[128]

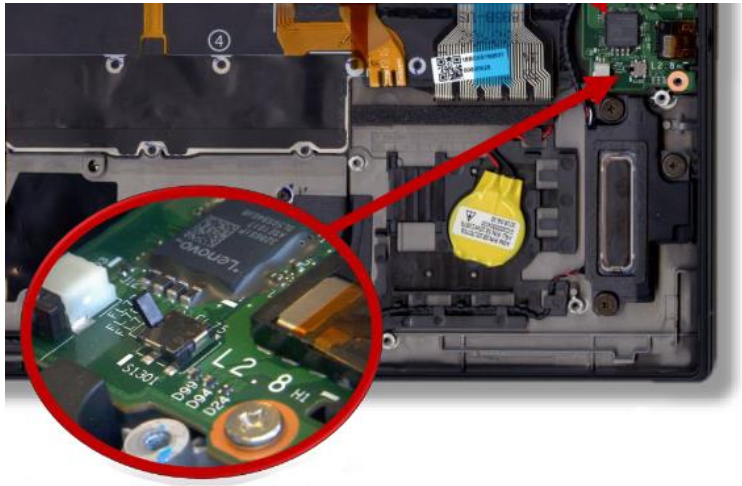
Evil Maid: Hardware-basiert (2/2)

- Hardware-Tausch (Evil Twin – Replace & R
- Unser Ziel: Manipulation ~~verhindern~~/erkenn
- Unsere Mittel:
  - Siegel
  - Sensoren
  - Alamierung des Users

Ref: [4], [115]—[121], [124]—[128]

Case Intrusion Sensors

- Lenovo ThinkPads
  - Boot-Warnung, BIOS Passwort
- HP TamperLock
  - Boot Warnung, BIOS Passwort
  - TPM clear, Instant Shutdown



Ref: [134], [135]

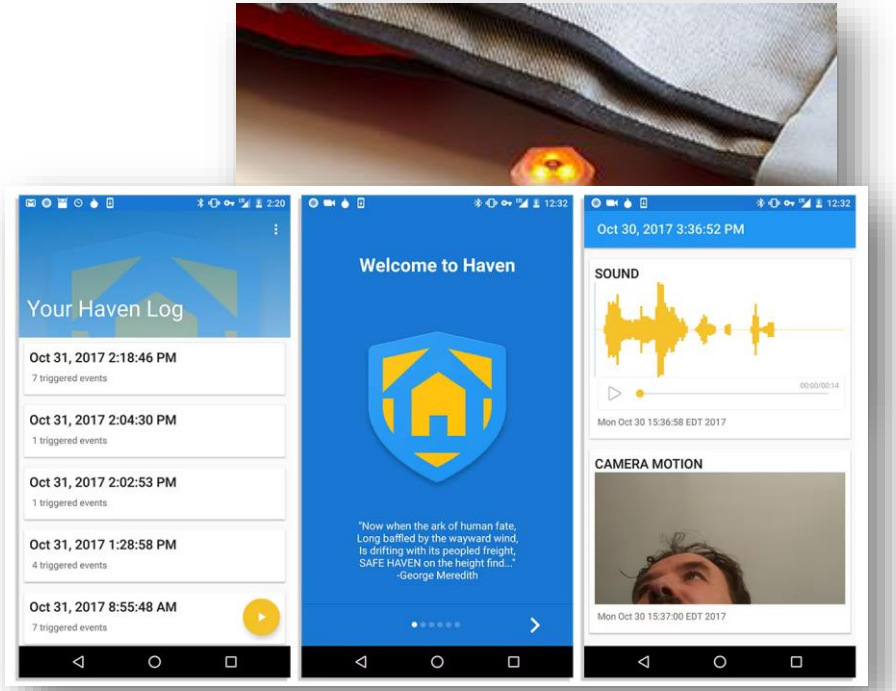
Glitzernagellack

- Über Schrauben lackieren
- Referenzfoto machen
- Bei Verdacht vergleichen
- App: Blink Comparison

Ref: [132], [133]

Sensoren!

- MetaSensor
  - Bewegungssensoren
  - Alert via Bluetooth
- Haven App
  - Ueberwacht alle Smartphone Sensoren
  - Alert via Mobilfunk



Ref: [136]

Ergebnis

Countermeasure	DMA attack (ext. port)	DMA attack (int. port)	Cold boot attack	SED attacks	TPM sniffing	TPM reset attack	Platform reset attack	fTPM fault injection	Invasive silicon attacks	Original evil maid	Tamper & revert	Replace & relay	Advanced R&R	Hardware keylogger	Hardware implants
	Drive-by Attack									Evil Maid Attack					
DMA port authorization	◐	-	-	-	-	-	-	-	-	-	-	-	-	-	-
DMA remapping	◐	◐	-	-	-	-	-	-	-	-	-	-	-	-	-
Memory encryption	-	-	●	-	-	-	-	-	-	-	-	-	-	-	-
systemd TPM + PIN FDE	-	-	-	●	●	●	●	-	-	●	◐	◐	-	◐	-
discrete TPM	-	-	-	-	-	-	-	●	-	-	-	-	-	-	-
Power off or hibernate	●	●	●	◐	-	-	-	-	-	-	-	-	-	-	-
TOTP-based AEM	-	-	-	-	-	-	-	-	-	●	●	◐	-	-	-
Hardened Secure Boot	-	-	-	-	-	◐	●	-	-	●	●	-	-	-	-
Case intrusion sensors	-	-	-	-	-	-	-	-	-	-	-	-	-	◐	◐
Haven app	-	-	-	-	-	-	-	-	-	●	●	●	●	◐	◐
Sum of countermeasures	●	●	●	●	●	●	●	●	-	●	●	●	●	◐	◐
Reference: Table 3.1	●	●	●	●	●	●	●	●	●	●	●	●	●	●	◐

● = mitigated; ◐ = partially mitigated; - = not mitigated;

Meet EMMA

- Evil Maid Misconduct Avoidance
- Prototyp: Waveshare RP2040
- Linux Daemon überwacht Sensoren
- Alerts via WiFi/LAN/LTE
- Heartbeat Mechanismus
- Shutdown & TPM Clear

Danke!

Slides und Diplomarbeit