Praktische Angriffe auf Full Disk Encryption

Hassan Mohamad - IT-SECX 2022

Man Jarsalek

IT Security

Physical Access Attacks Against Unattended Computers

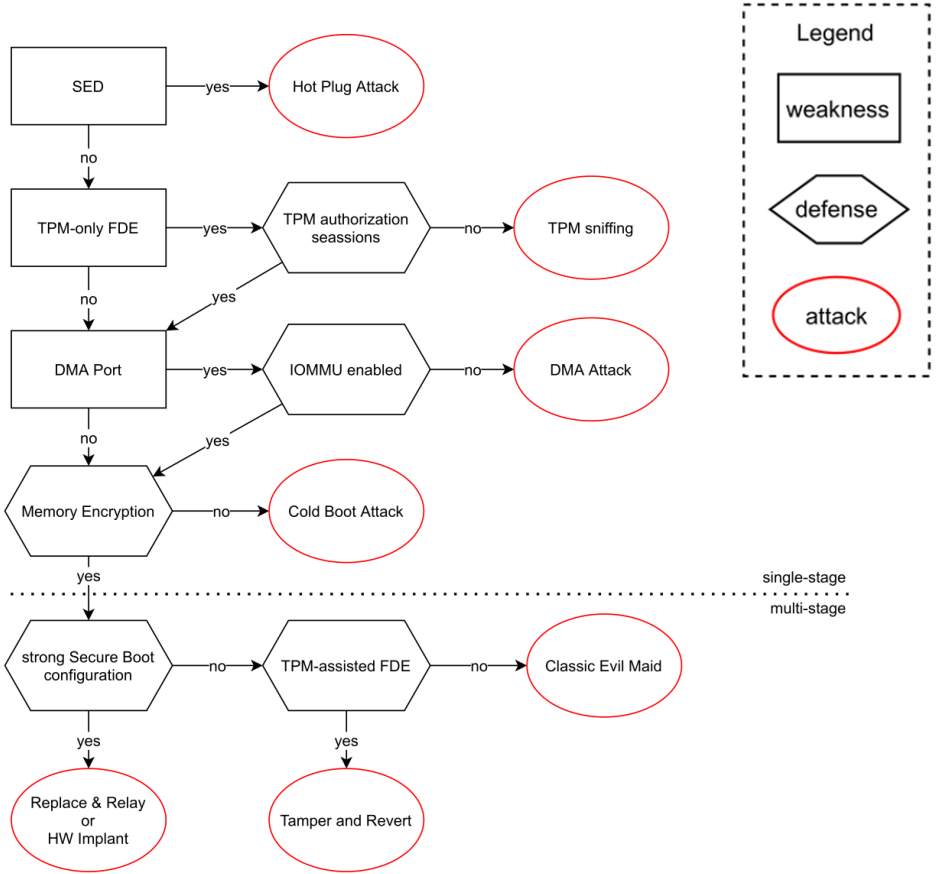
Bachelor thesis

Threat Modeling

- Full Disk Encryption
- Gerät ist gesperrt oder ausgeschalten
- Angreifer hat physischen Zugriff
- Algorithmen sind sicher (AES, SHA)
- Brute-Force is out of scope
- Angriffe in mehreren Schritten auch möglich

Ergebnis: Decision Tree

- Schwachstellen: Rechteck
- Schutzmaßnahmen: Hexagon
- Angriffe: Oval

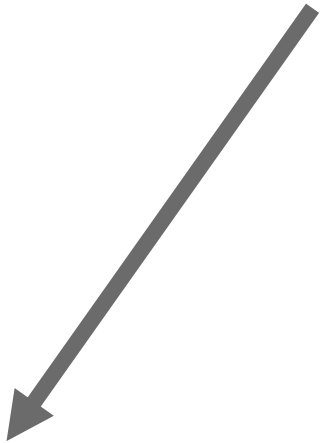


Windows (BitLocker)

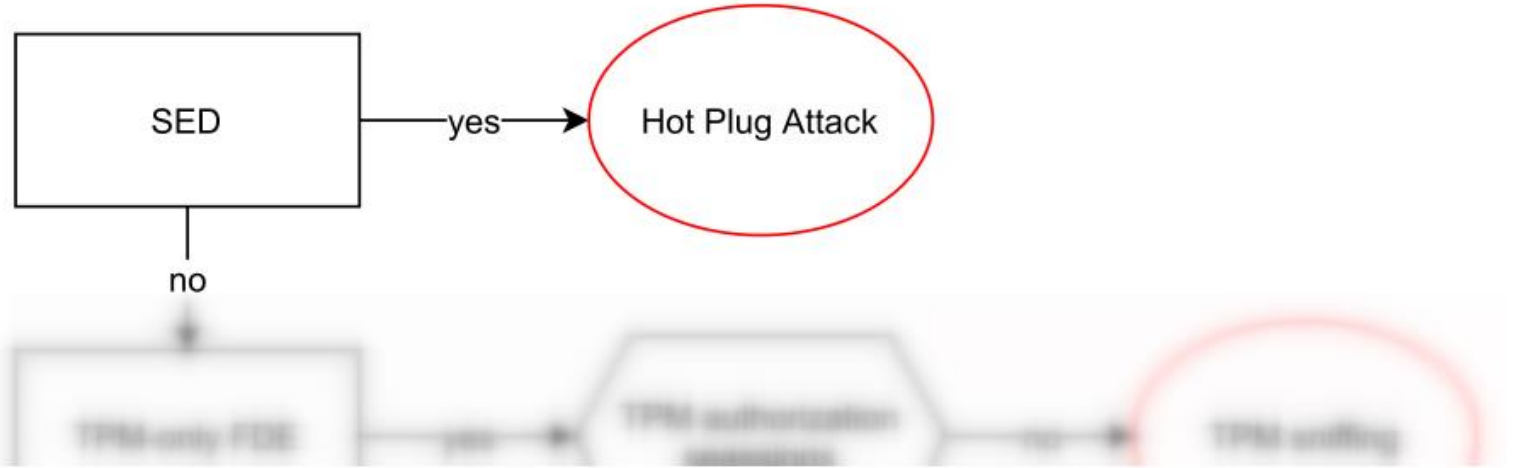
Linux (dm-crypt + LUKS)

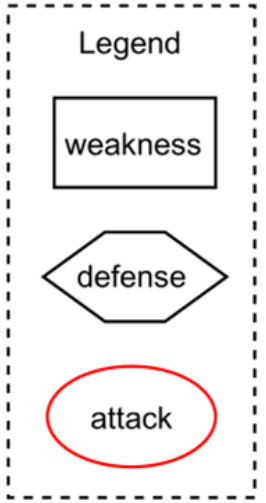
security research

Quellen!



ref: [99]


SED
yes
Hot Plug Attack
no
TPM-only FDE
yes
TPM authorization sessions
no
TPM sniffing

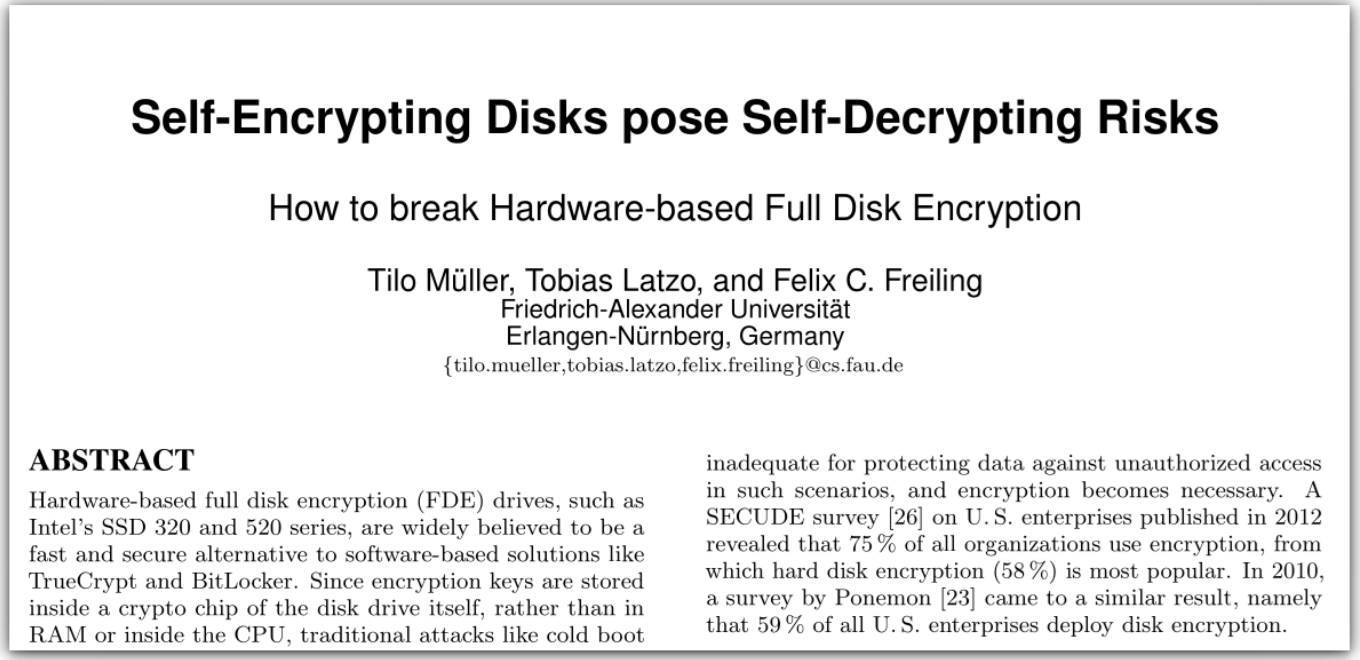

Legend
weakness
defense
attack

Self-Encrypting Disks

- Verschlüsselung durch SSD-/HDD-Controller
- Host-CPU wird entlastet
- OS liefert beim Bootvorgang Key zum entsperren
- Standards: TCG Opal & IEEE 1667
  - ➜ Microsoft eDrive
  - ➜ BitLocker Kompatibilität

ref: [6], [7]

Hot Plug Attack



Self-Encrypting Disks pose Self-Decrypting Risks

How to break Hardware-based Full Disk Encryption

Tilo Müller, Tobias Latzo, and Felix C. Freiling
Friedrich-Alexander Universität
Erlangen-Nürnberg, Germany
{tilo.mueller,tobias.latzo,felix.freiling}@cs.fau.de

ABSTRACT

Hardware-based full disk encryption (FDE) drives, such as Intel's SSD 320 and 520 series, are widely believed to be a fast and secure alternative to software-based solutions like TrueCrypt and BitLocker. Since encryption keys are stored inside a crypto chip of the disk drive itself, rather than in RAM or inside the CPU, traditional attacks like cold boot inadequate for protecting data against unauthorized access in such scenarios, and encryption becomes necessary. A SECUDE survey [26] on U. S. enterprises published in 2012 revealed that 75 % of all organizations use encryption, from which hard disk encryption (58 %) is most popular. In 2010, a survey by Ponemon [23] came to a similar result, namely that 59 % of all U. S. enterprises deploy disk encryption.

ref: [12]

Hot Plug Attack - Desktop (SATA)

- Computer im eingeschalteten Zustand -> SED ist entsperrt
- SATA abstecken
- SATA beim Angreifer anstecken
- …
- Profit

ref: [12]

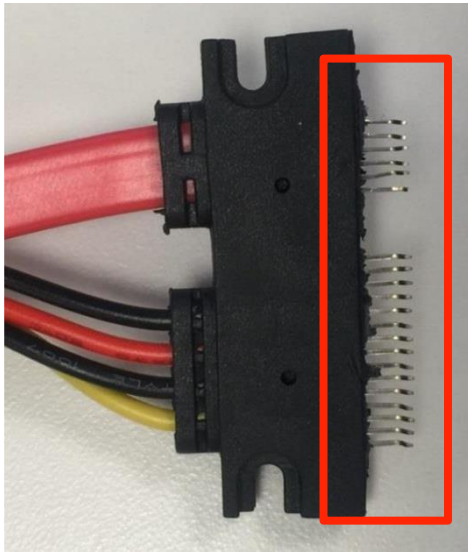
Hot Plug Attack - Laptop Edition (SATA)

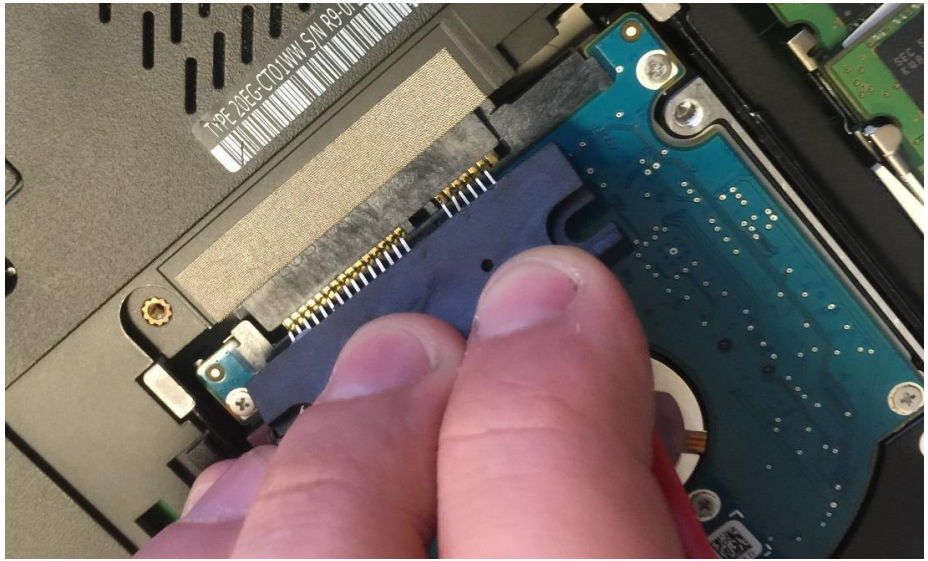
- Computer in den Sleep Mode versetzen
- SATA/Power Splitter zwischenschalten
- Aus Sleep Mode aufwecken

→ SSD wird automatisch entsperrt

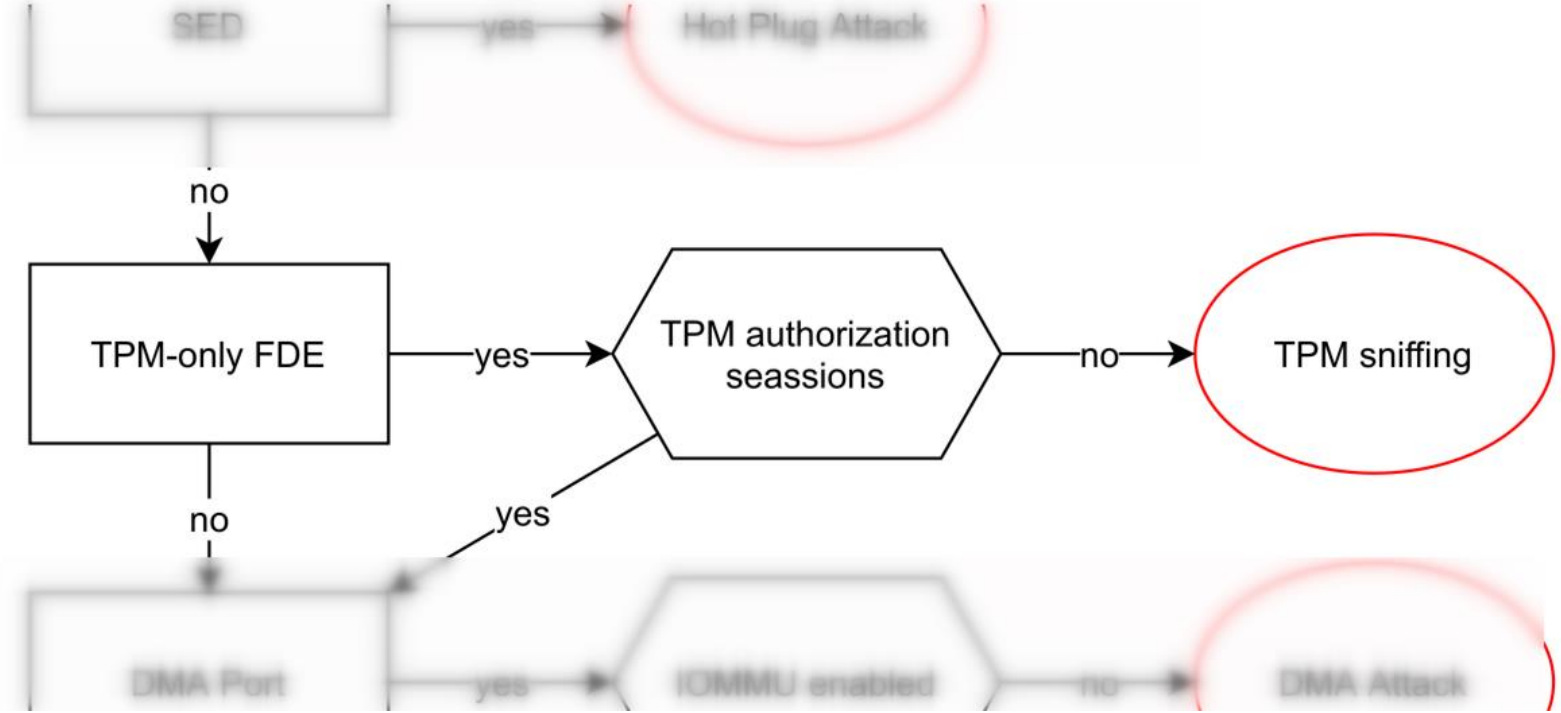
ref: [13]

Hot **Un**plug Attack - Laptop, NVMe



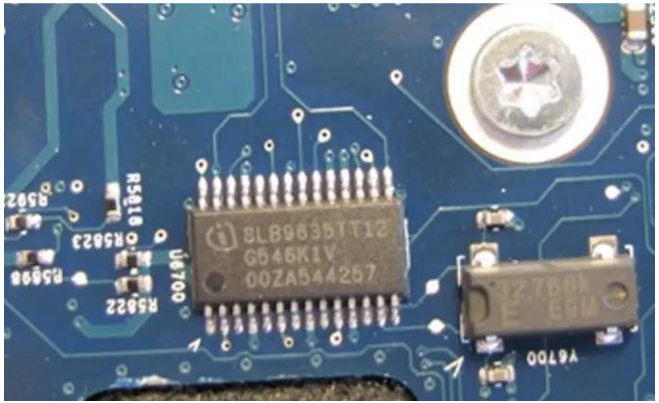


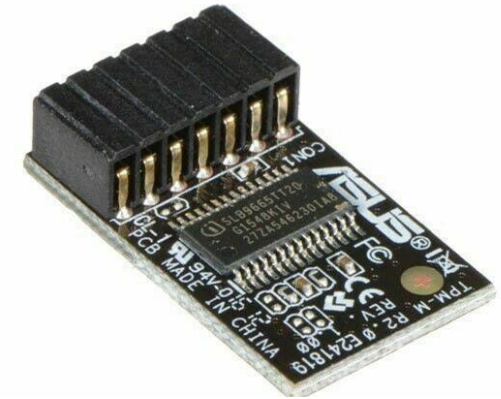
ref: [13]


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
Legend
weakness
defense
attack

TPM - Trusted Platform Module

- Dedizierter Chip für Crypto-Operationen
- Manipulationssicher
- Kann Schlüssel aufbewahren
- Messung der Integrität des Systems
- Schlüssel an Bedingung geknüpft





TPM - Measured Boot

PCR Nr.	Verwendung	Bsp. Inhalt (Hash)
0	Core System Firmware	`b026324c6904b2a9cb4b88d6…`
1	Core System Firmware Config	`26ab0db90d72e28ad0ba1e22…`
4	UEFI Boot Manager	`6d7fce9fee471194aa8b5b6e…`
5	GPT / Partition Table	`48a24b70a0b376535542b996…`
7	UEFI Secure Boot State	`1dcca23355272056f04fe8bf…`
11	BitLocker Access Control	`9ae0ea9e3c9c6e1b9b6252c8…`

TPM - Measured Boot

PCR Nr.	Verwendung	Bsp. Inhalt (Hash)
0	Core System Firmware	b026324c6904b2a9cb4b88d6…
1	Core System Firmware Config	7c5aba41f53293b712fd86d0…
4	UEFI Boot Manager	31d30eea8d0968d6458e0ad0…
5	GPT / Partition Table	166d77ac1b46a1ec38aa35ab…
7	UEFI Secure Boot State	2737b49252e2a4c0fe4c342e…
11	BitLocker Access Control	aa6ed9e0f26a6eba784aae82…

2005 - TPM Sniffing

Analyzing trusted platform communication *

Klaus Kursawe, Dries Schellekens **, and Bart Preneel

Katholieke Universiteit Leuven
Department Electrical Engineering-ESAT/SCD-COSIC,
Kasteelpark Arenberg 10, 3001 Heverlee, Belgium
{klaus.kursawe,dries.schellekens,bart.preneel}@esat.kuleuven.be
http://www.esat.kuleuven.be/cosic/

Abstract. In this paper we discuss the analysis of trusted platform communication. While the trusted platform module itself is considered reasonably tamper resistant, the communication channel between this module and the rest of the trusted platform turns out to be comparatively insecure. Passive attacks can be mounted on the communication interface with fairly inexpensive equipment and allow eavesdropping of

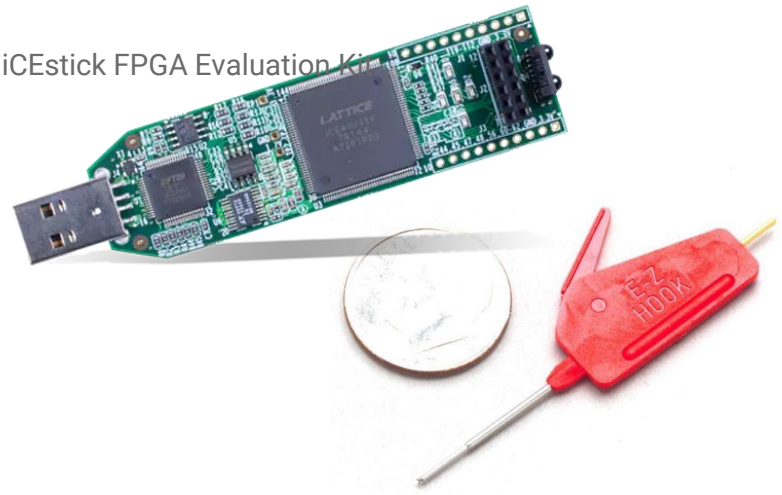
ref: [63]

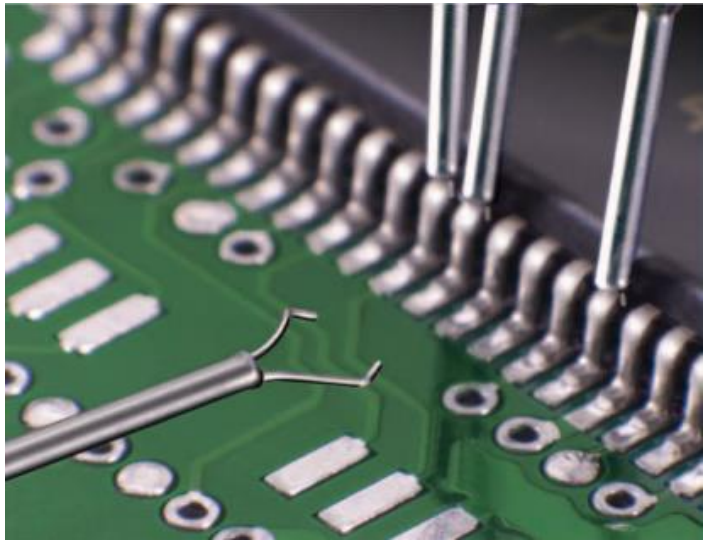
IT-SECX 2019 - TPM Sniffing

ref: [66]

TPM Sniffing - Hardware

iCEstick FPGA Evaluation Kit



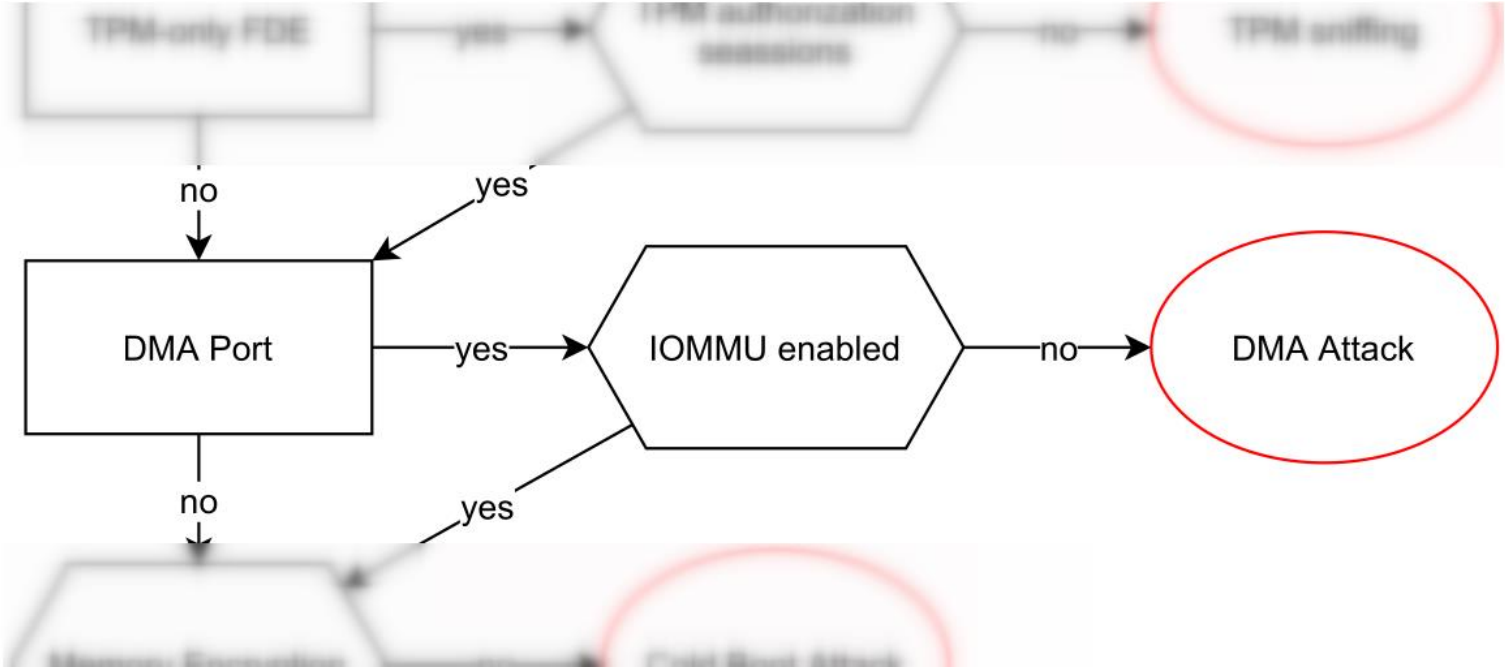


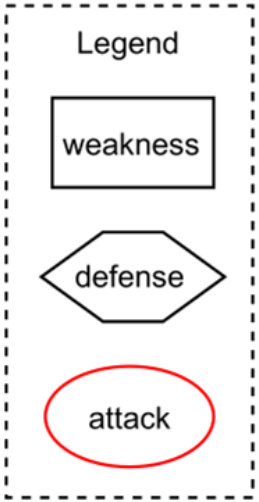
E-Z-Hook X2015

TPM 2.0 - Authorization Sessions

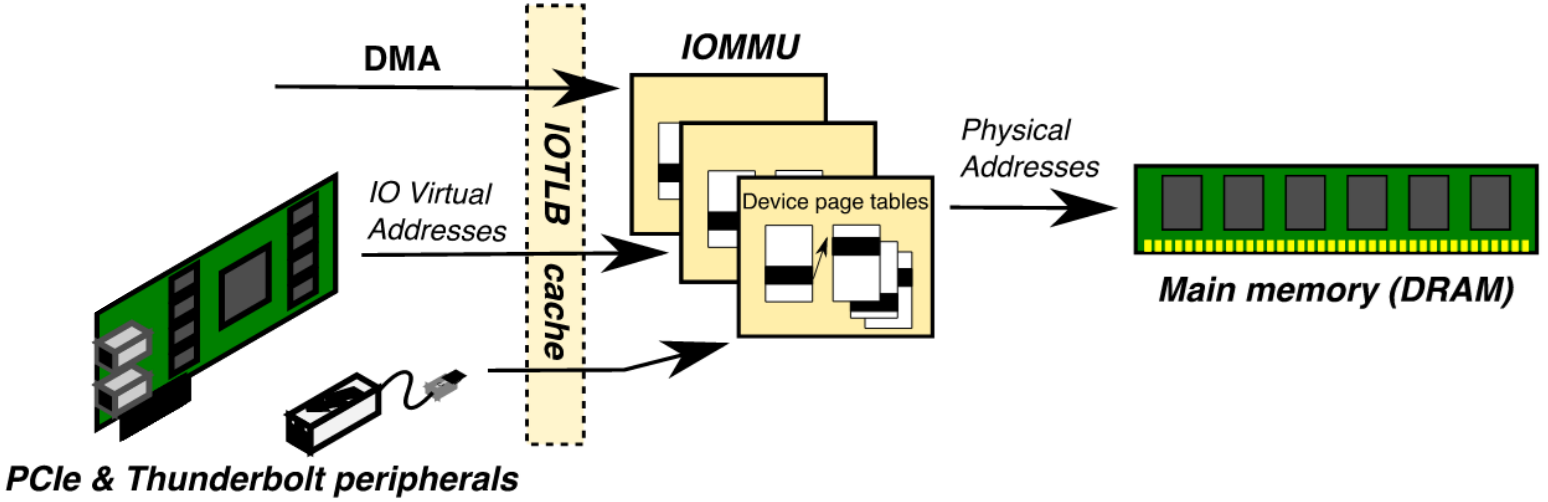
- Neues Feature im TPM 2.0 Standard
- Authentifizierte und verschlüsselte Kommunikation mit Host
- Verwendung ist optional
- Nicht von Bitlocker unterstützt

ref: [8]


TPM-only FDE
yes
TPM sniffing
no
yes
DMA Port
yes
IOMMU enabled
no
DMA Attack
no
yes


Legend
weakness
defense
attack

Direct Memory Access (DMA)

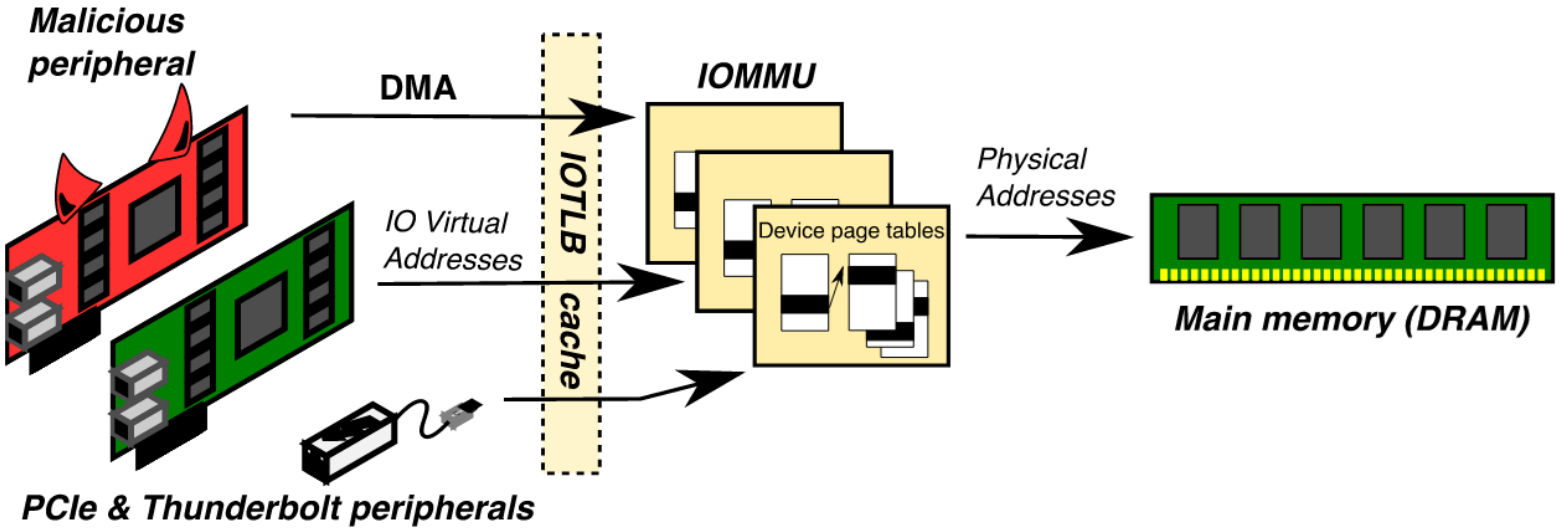


ref: [24]

DMA-fähige Ports

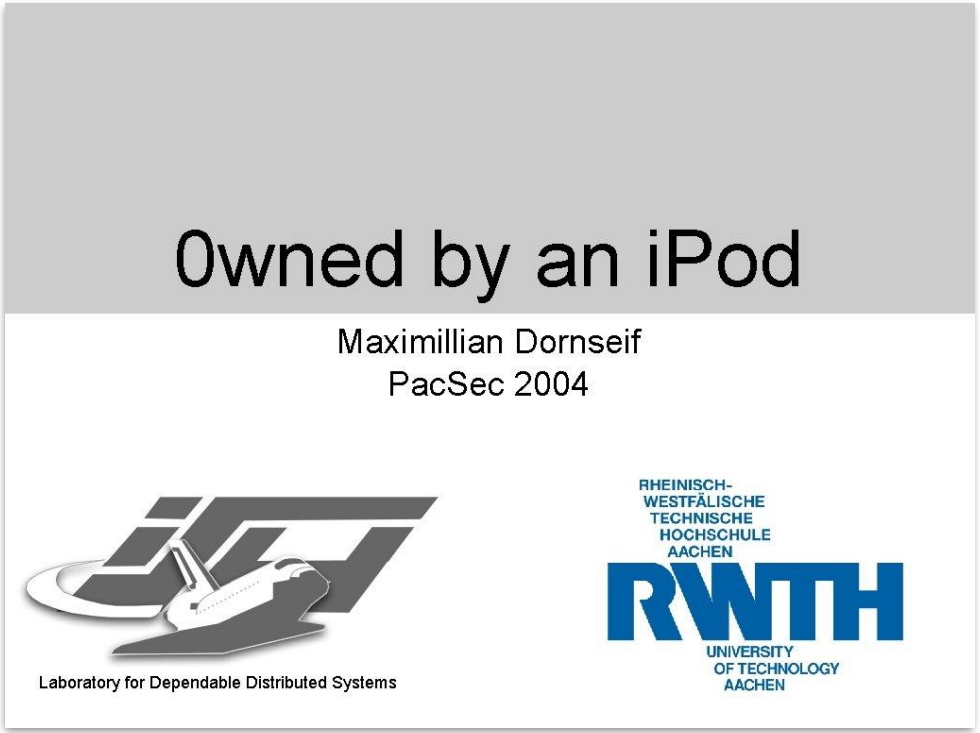
- PCIe (auch M.2)
- Thunderbolt (auch via USB C)
- (USB 4 v2.0 Gen 3 4x4)
- Firewire, ExpressCard, ..

Direct Memory Access (DMA)



ref: [24]

2004


0wned by an iPod
Maximillian Dornseif
PacSec 2004
Laboratory for Dependable Distributed Systems
RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN
RWTH
UNIVERSITY
OF TECHNOLOGY
AACHEN

ref: [14]

LambdaConcept Screamer M.2 USB-C

- PCIe (Opfer) -> USB-C (Angreifer)
- Xilinx FPGA
- 64-Bit Unterstützung
- PCILeech Unterstützung

ref: [26]

PCILeech

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

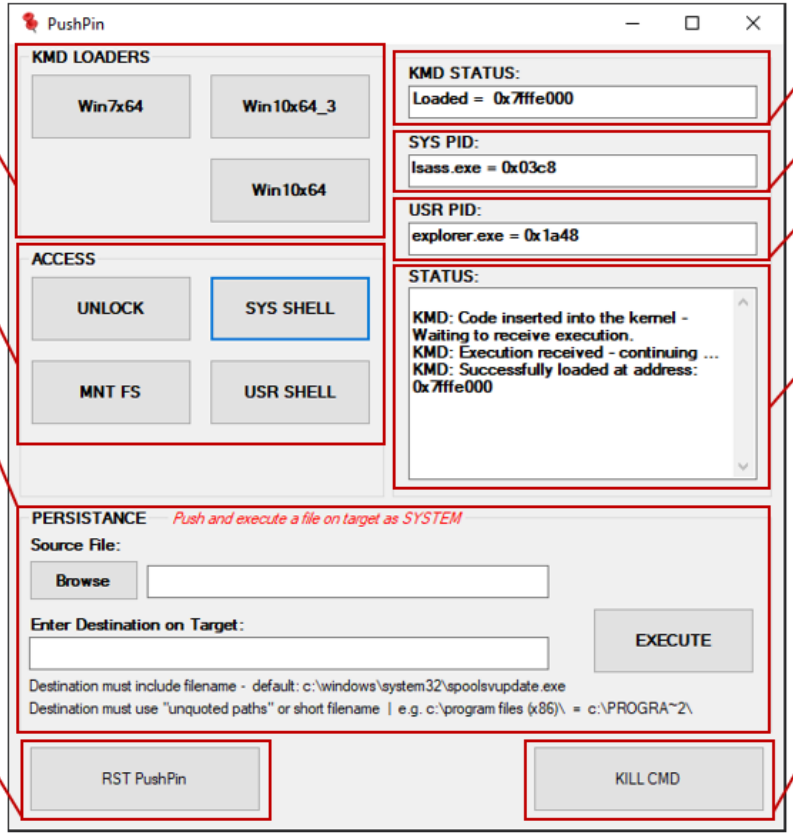
Step 2 – Load Kernel Implants
- Unlock/bypass password login
- USER or SYSTEM CMD Shell
- Mount the File system/memory

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

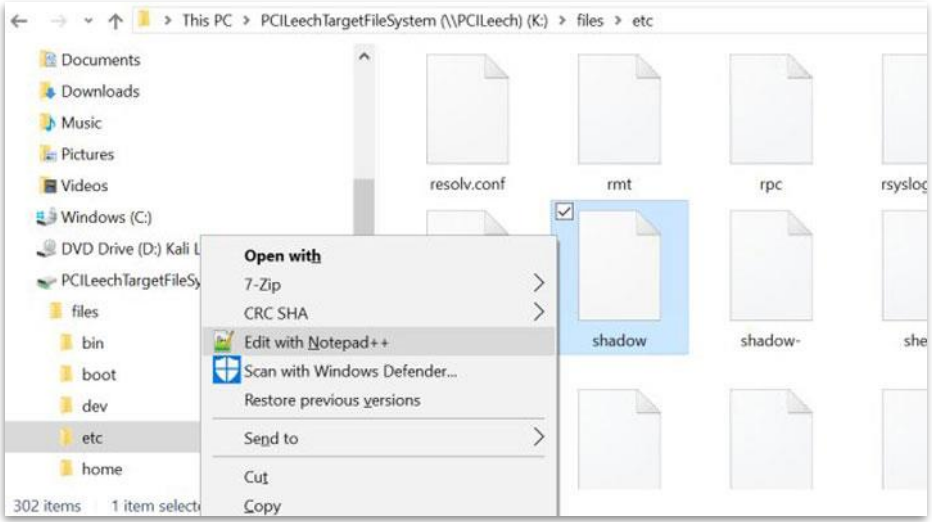
USR PID Window
- The PID of explorer.exe is always a USER
- This address is stored and used in attacks

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

KILL CMD Button
- Closes all CMD shell windows

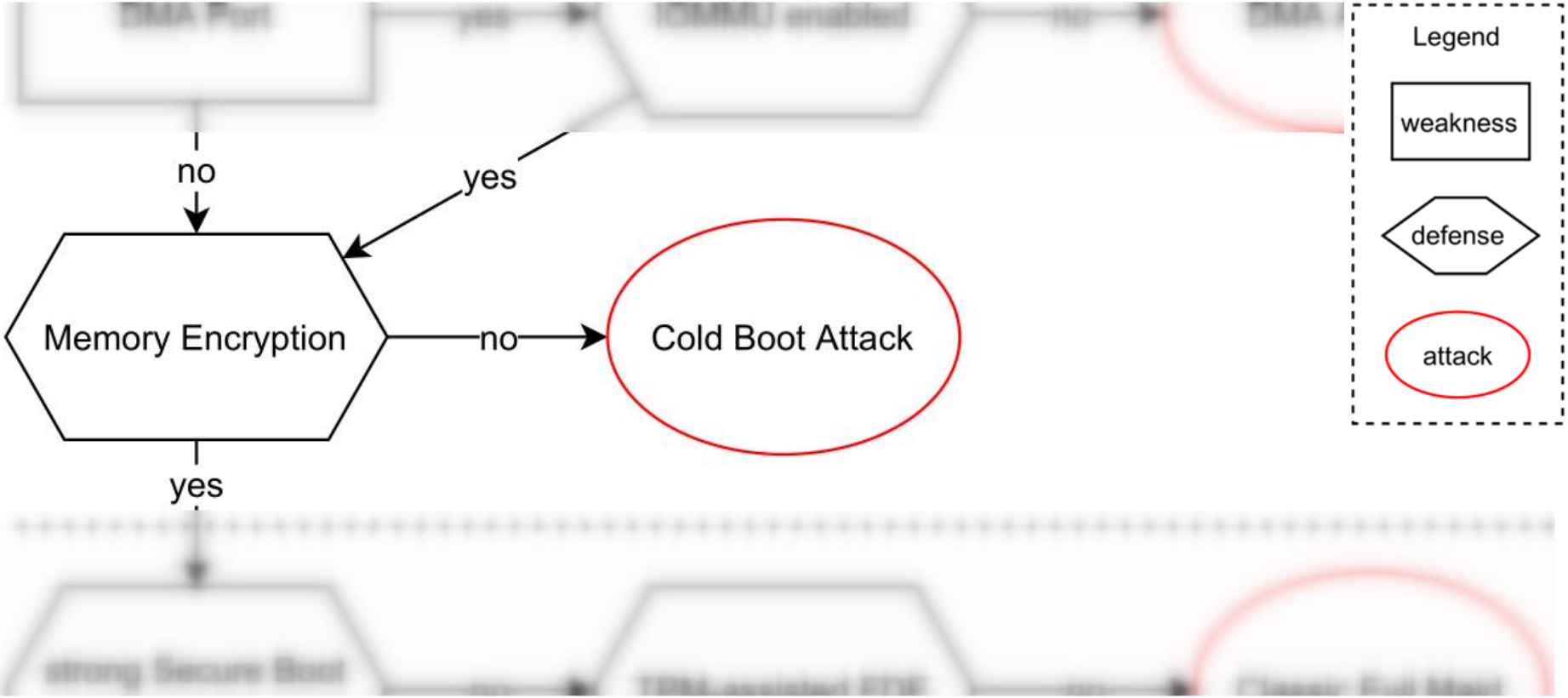
ref: [23]

PCILeech




```
 Current Action: Dumping Memory
 Access Mode:    KMD (kernel module assisted DMA)
 Progress:       8678 / 8678 (100%)
 Speed:          173 MB/s
 Address:        0x000000021E600000
 Pages read:     2050967 / 2221568 (92%)
 Pages failed:   170601 (7%)
Memory Dump: Successful.
```

ref: [23]

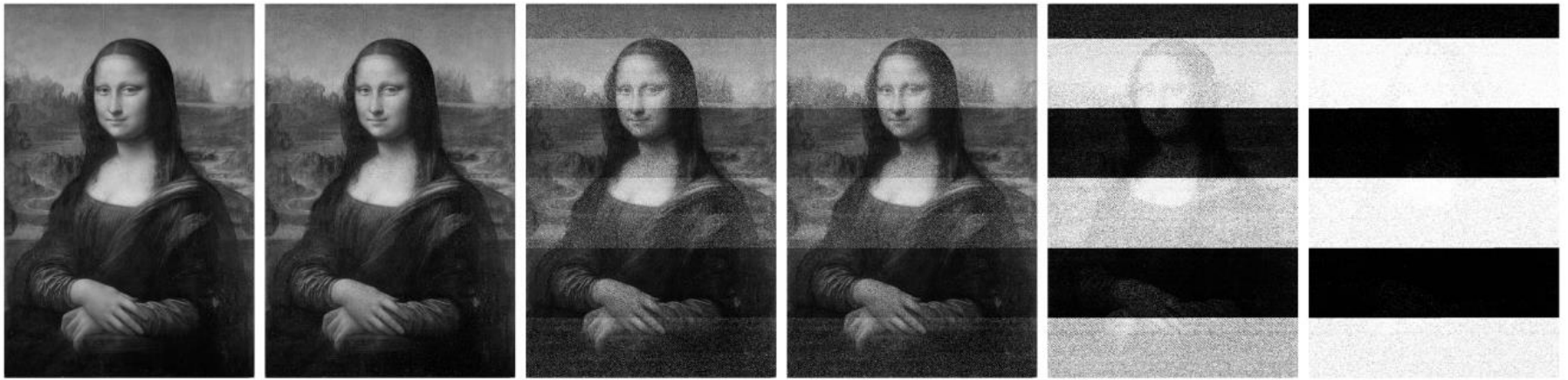

no
yes
Memory Encryption
no
Cold Boot Attack
yes
Legend
weakness
defense
attack

Cold-Boot

- RAM kühlen
- (transplantieren)
- RAM auslesen
- Crypto Keys identifizieren

ref: [38]

Memory Remanence Effect



(a) 0 sec / 100% **(b)** 2 sec / 99.2% **(c)** 3 sec / 93.4% **(d)** 4 sec / 93.1% **(e)** 5 sec / 61.4% **(f)** 6 sec / 51.9%

ref: [39]

2009

Lest We Remember: Cold Boot Attacks on Encryption Keys

J. Alex Halderman*, Seth D. Schoen†, Nadia Heninger*, William Clarkson*, William Paul‡,
Joseph A. Calandrino*, Ariel J. Feldman*, Jacob Appelbaum, and Edward W. Felten*

*Princeton University †Electronic Frontier Foundation ‡Wind River Systems

{jhalderm, nadiah, wclarkso, jcalandr, ajfeldma, felten}@cs.princeton.edu
schoen@eff.org, wpaul@windriver.com, jacob@appelbaum.net

ref: [38]

MEMORY RESEARCH PROJECT SOURCE CODE

« Back

July 16, 2008 — This page contains source code for some of the software that we developed in the course of this research. These prototype applications are intended to illustrate the techniques described in the paper; we are unable to provide technical support.

Memory imaging

USB / PXE Imaging Tools	bios_memimage-1.2.tar.gz	(sig)
EFI Netboot Imaging Tools	efi_memimage-1.0.tar.gz	(sig)

Automatic key-finding

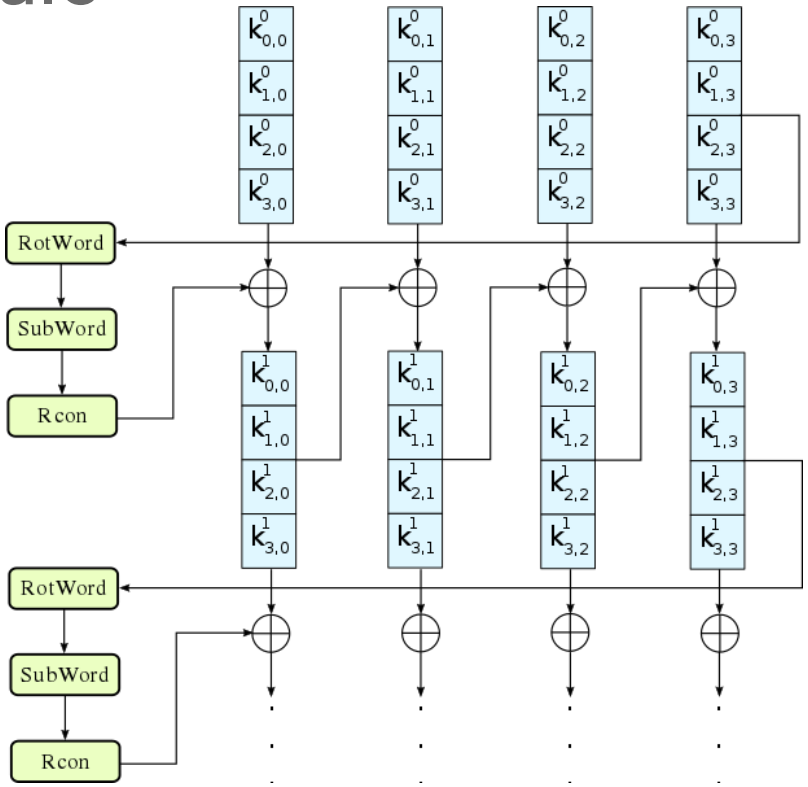
AESKeyFinder	aeskeyfind-1.0.tar.gz	(sig)
RSAKeyFinder	rsakeyfind-1.0.tar.gz	(sig)

Error-correction for AES key schedules

AESFix	aesfix-1.0.1.tar.gz	(sig)

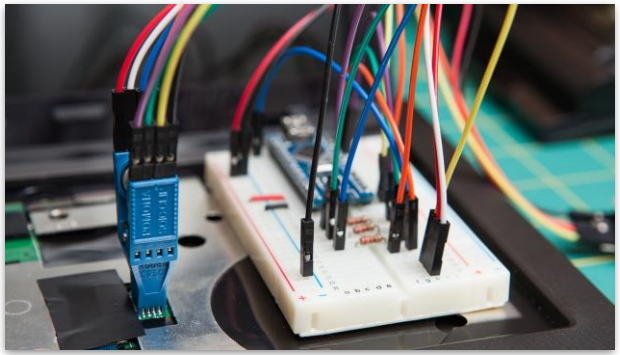
ref: [38]

AES Key Schedule

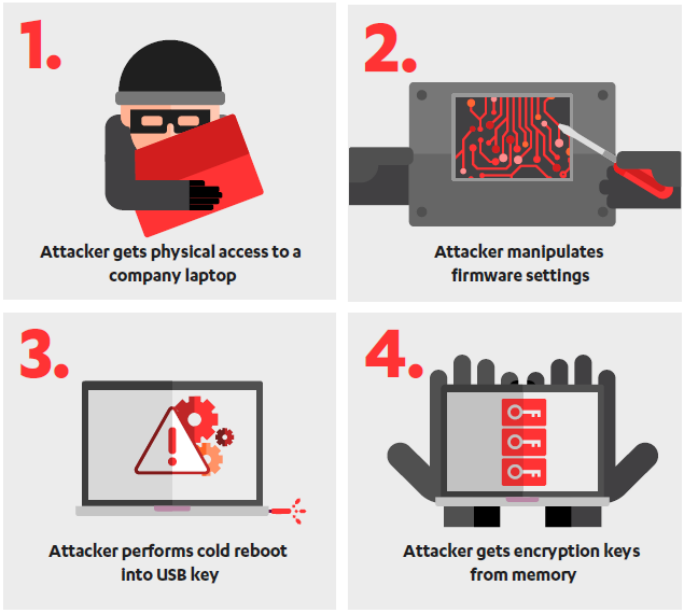


2018

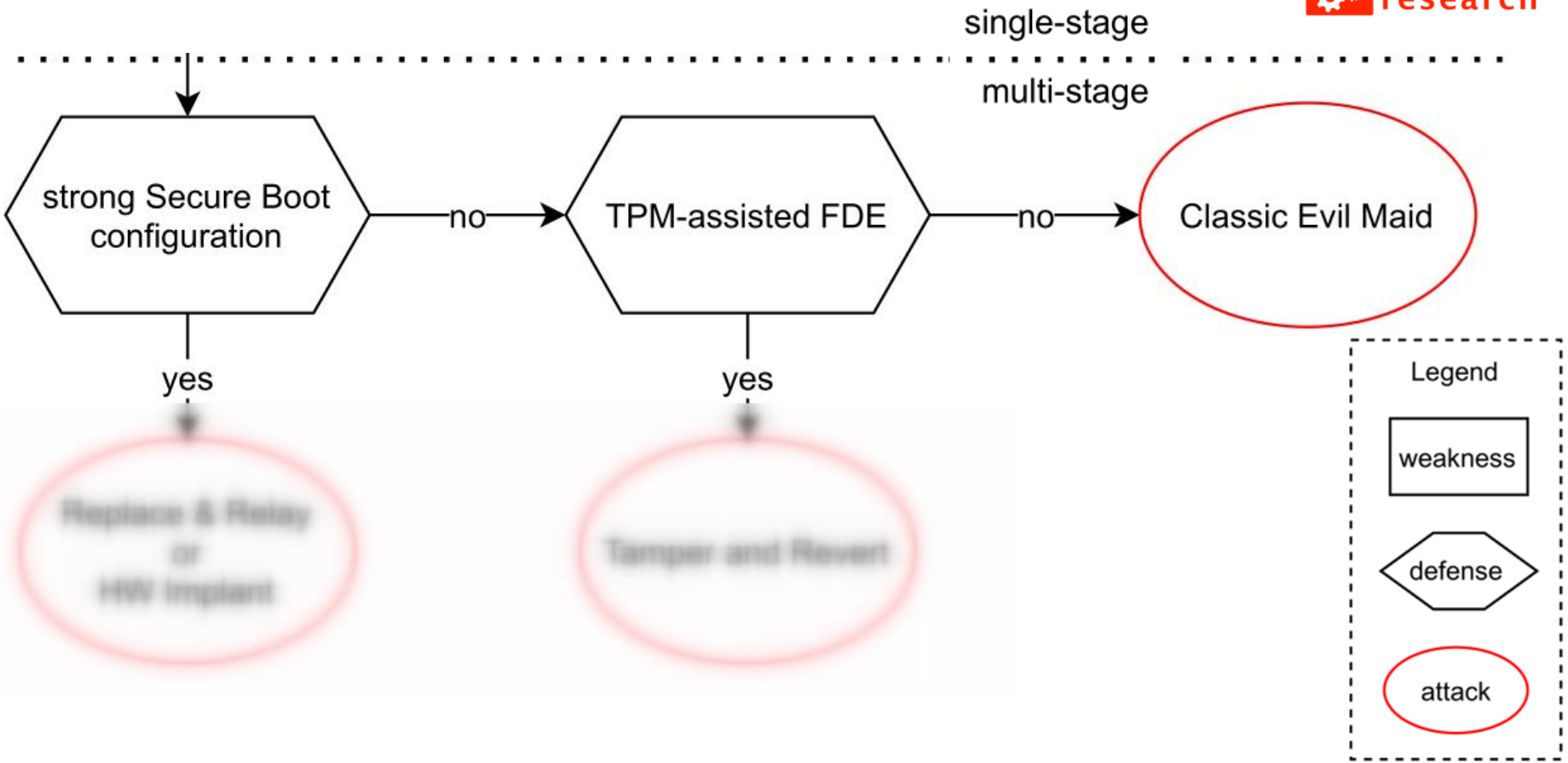
- “Hot-Reboot”-Angriff
- Kühlung nicht zwingend notwendig
- Umgehung von Firmware-Security



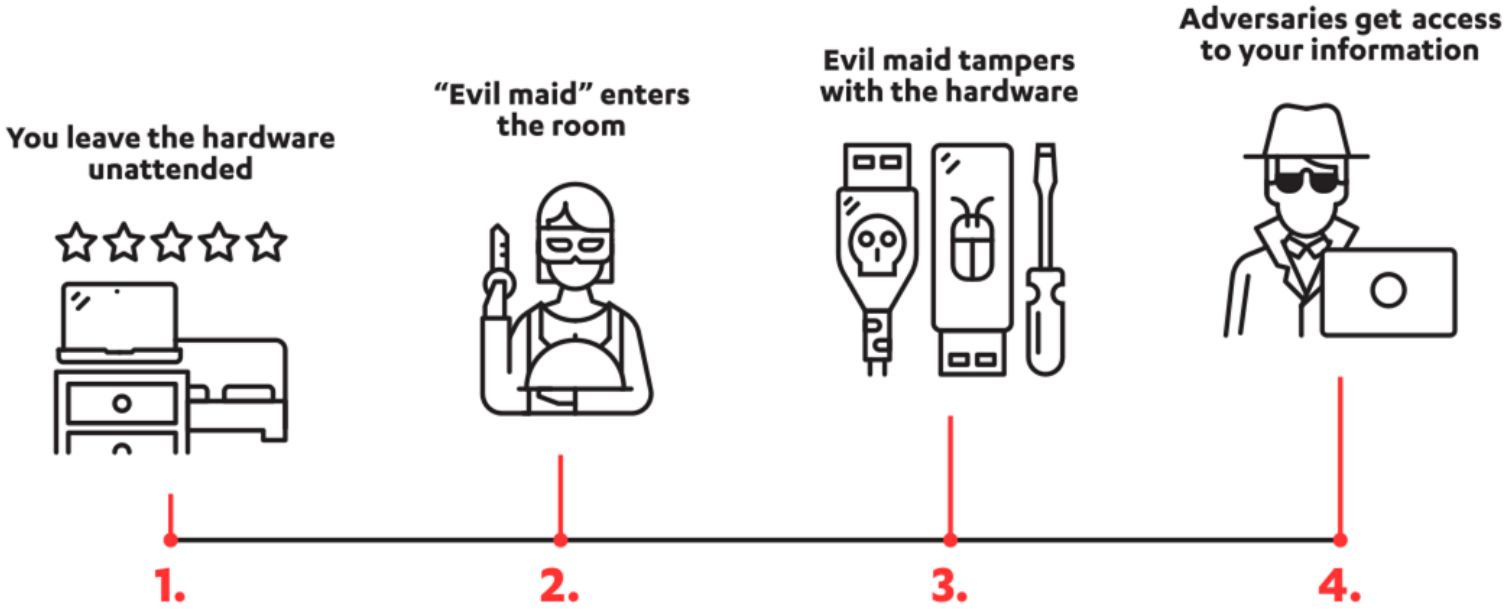
F-Secure



ref: [43]

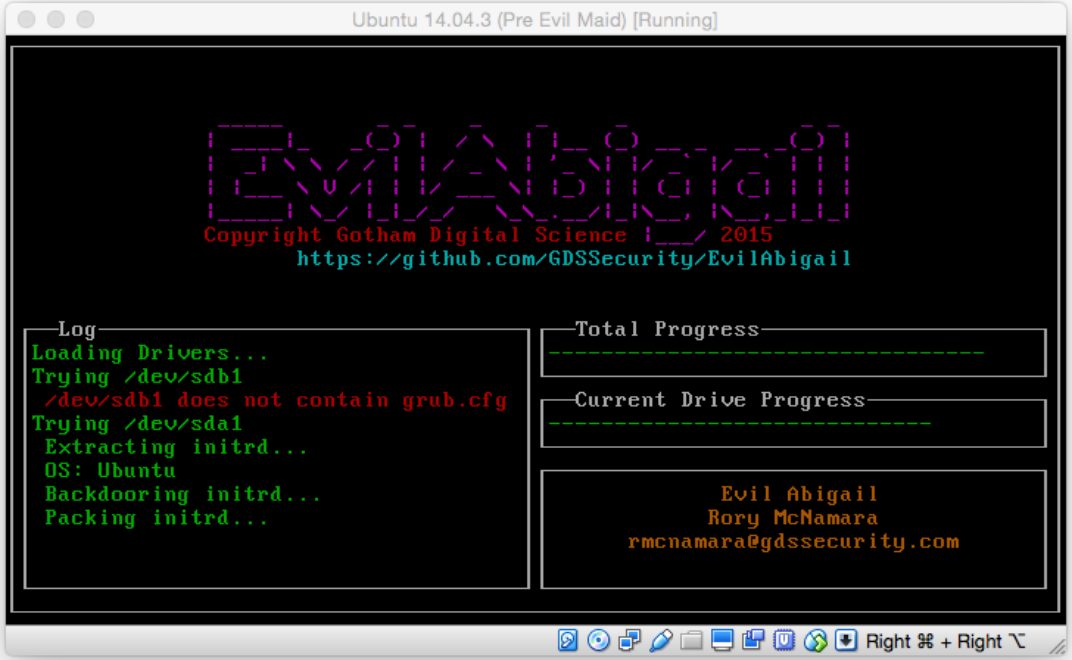

single-stage
multi-stage
strong Secure Boot configuration
no
TPM-assisted FDE
no
Classic Evil Maid
yes
yes
Replace & Relay or HW Implant
Tamper and Revert
Legend
weakness
defense
attack

Evil Maid Attack

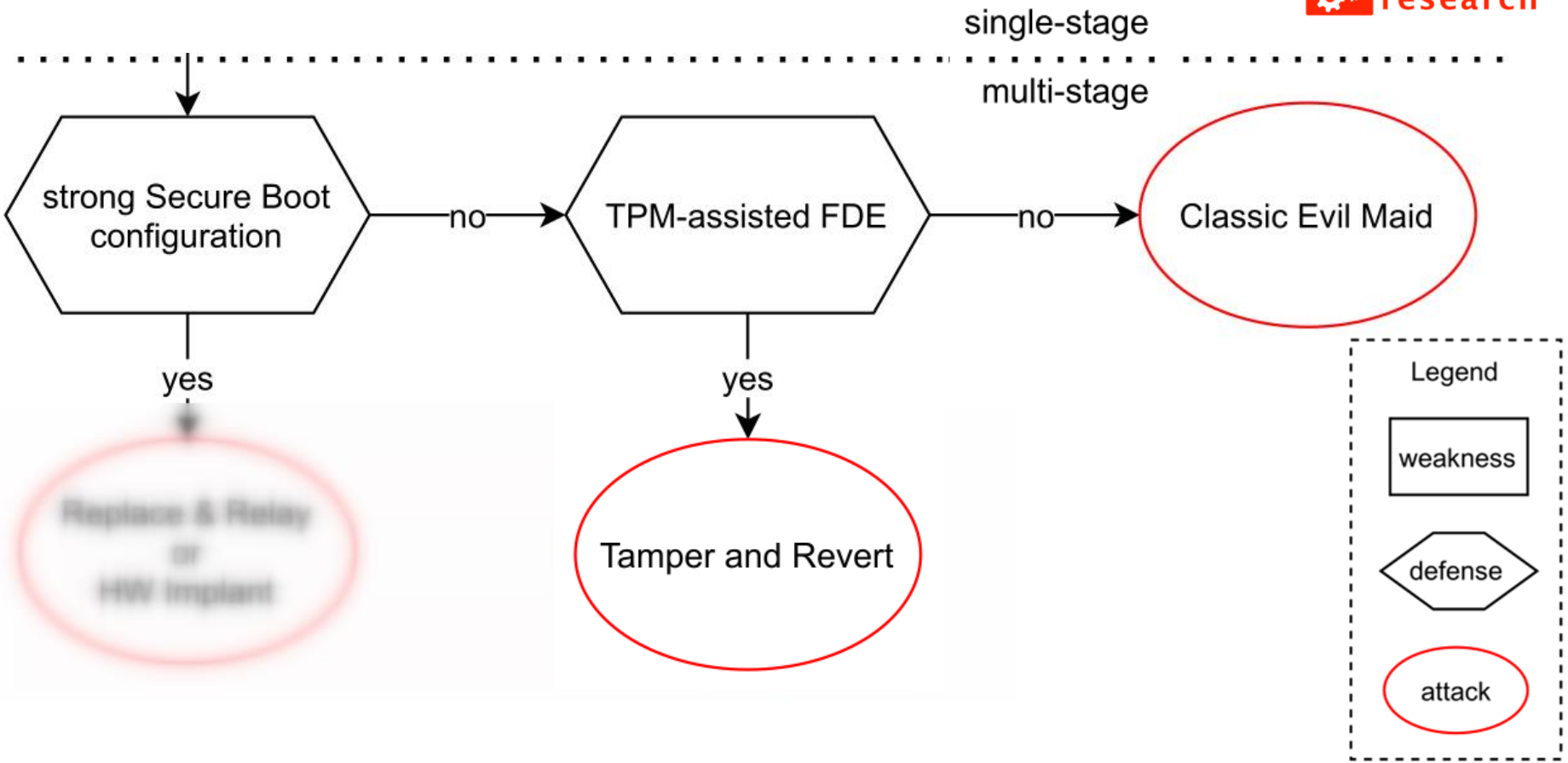


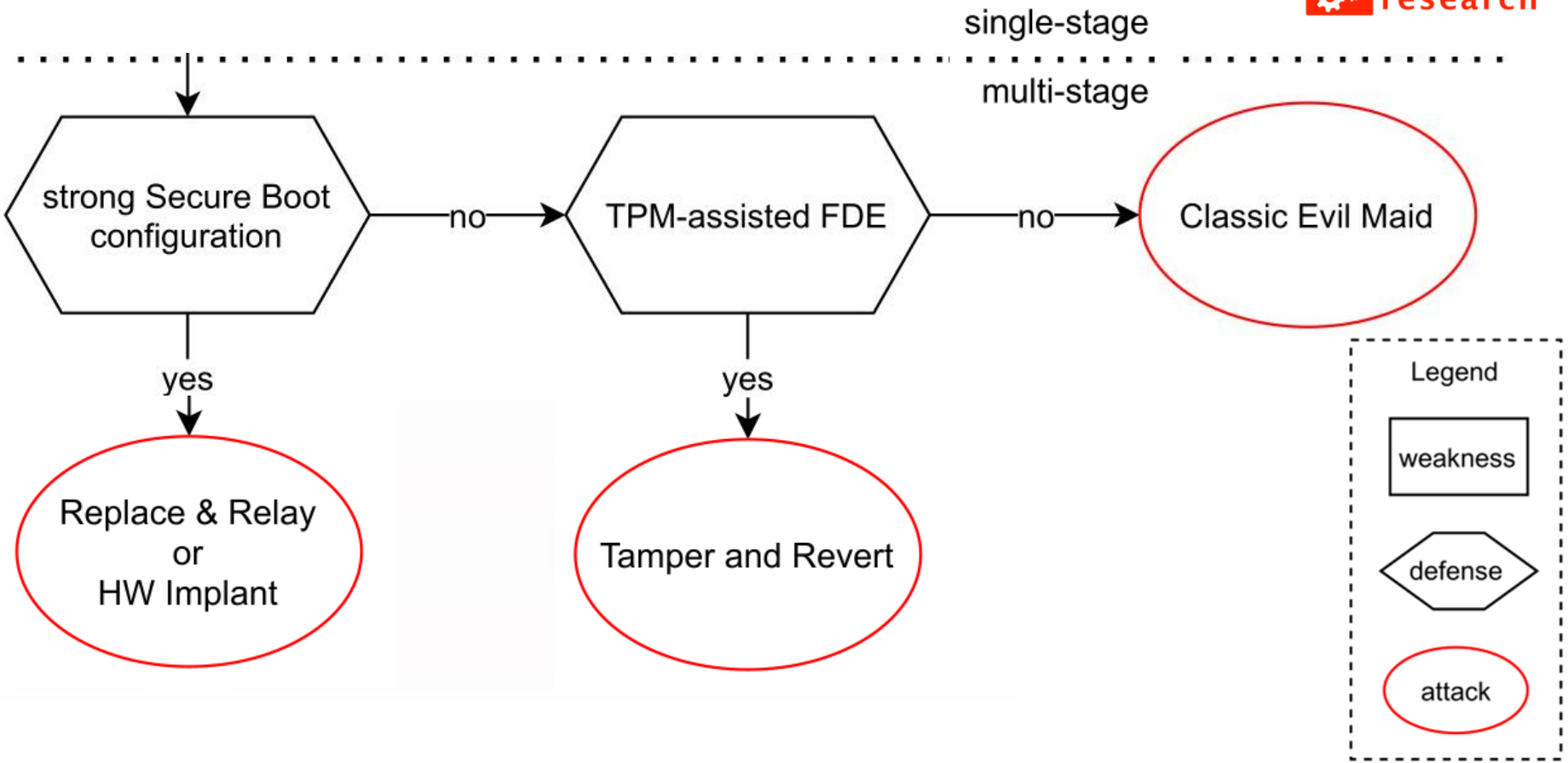
ref: [77], [78]

github.com/AonCyberLabs/EvilAbigail



ref: [80]


single-stage
multi-stage
strong Secure Boot configuration
no
TPM-assisted FDE
no
Classic Evil Maid
yes
yes
Tamper and Revert
Legend
weakness
defense
attack


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

We are hiring!

Was wir bieten:

- Wirklich spannende Projekte (nicht nur das übliche Web-, App-, AD-Testing)
- Fortbildung nach deiner Wunschspezialisierung
- Viel Spaß im Büro (Grillen, Events, Hunde, ...)
- Zw. €3800 und €5000 Bruttomonatsgehalt