The Cold Boot Attack and other Hot Stuff

by Pol Hölzmer

IT-S NOW

IT-S NOW

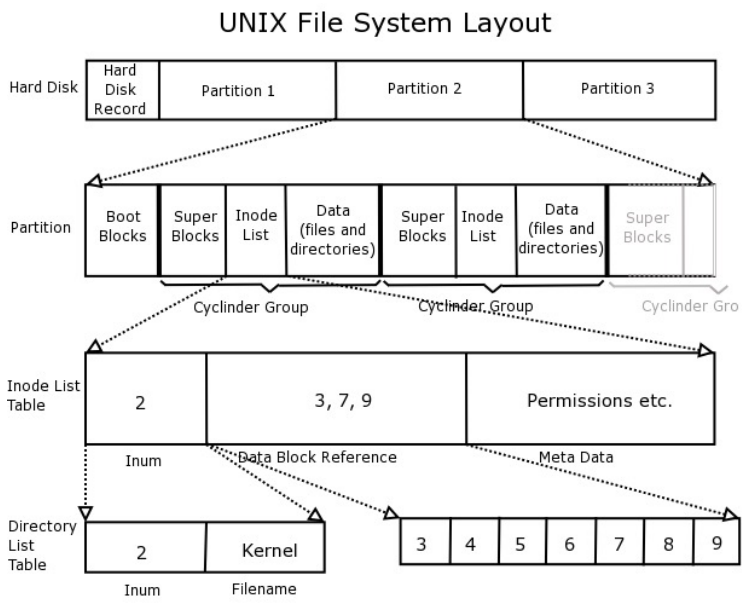
```
try:
        while audience.listen():
                speacker. inform()
                audience.learn()

        audience.act()

except ExpectationsMissed:
        print("Mission failed!")
```

Data Recovery
Background

- Raw {Disk, File} {Viewer, Editor}



- File Signatures (exerpt)

Hex signature	ISO 8859-1	Extension
FF D8 FF E0	ÿØÿà	jpg
4D 5A	MZ	exe sys dll
5A 4D	ZM	exe
50 4B 03 04 50 4B 05 06 (empty archive) 50 4B 07 08 (spanned archive)	PK^ᵉₓ^ᵉ₀_ₜ PK^ᵉ₀^ᴬ₀_ₓ PK^ᵉ₀_ᴸ^ᴮ₀	zip apk docx pptx xlsx
7F 45 4C 46	^ᴮ₀ELF	
89 50 4E 47 0D 0A 1A 0A	‰PNG^ᶜ₀ ^ᴬ₀^ᴳ₀^ᴬ₀	png
25 50 44 46 2D	%PDF-	pdf
D0 CF 11 E0 A1 B1 1A E1	ÐÏ^ᴮ₀à¡±^ᴳ₀á	doc xls ppt msi

Data Recovery

(EoL, Re-Buy)

Live Demo

Disk Encryption

Why? What?

Disk Encryption
What? Why?

Component
Software / Hardware

Operation
Read / Write

Target
Securing physical access

Process
encrypts / decrypts data on-the-fly

Devices
block device, disk partition or directory

Disk Encryption
Advantages

Why?

- Data **always** stored **encrypted**
- Data **only** readable for **trusted users**
- Plausible **Deniability**

What?

- **Notebooks** / Computer
- Smartphones / Tablets
- NAS / Server
- **External storage** devices

When?

Prevent Unauthorized access when:

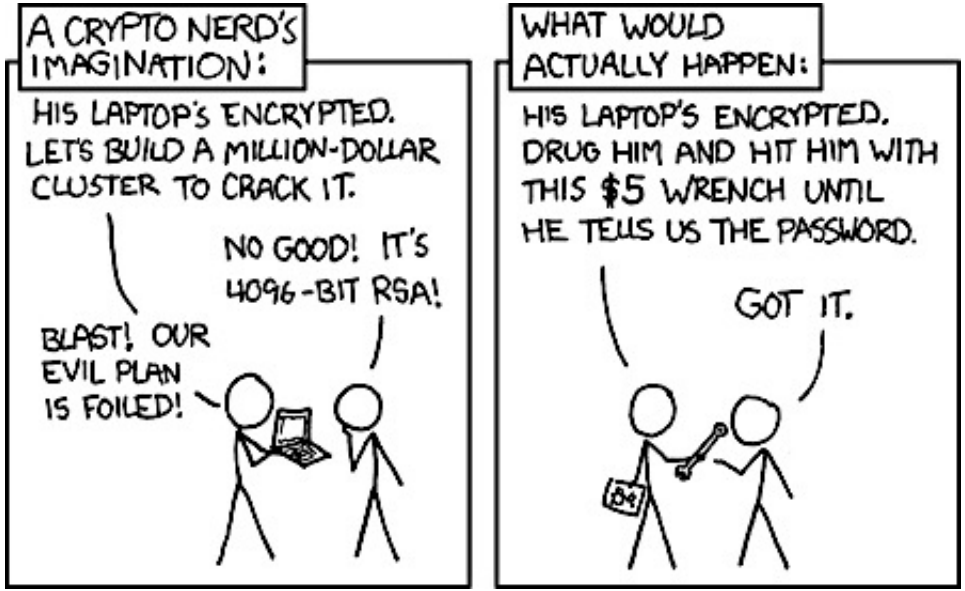
- Lost / Stolen / Public space
- Repair shops / End-of-life

Disk Encryption
Disadvantages

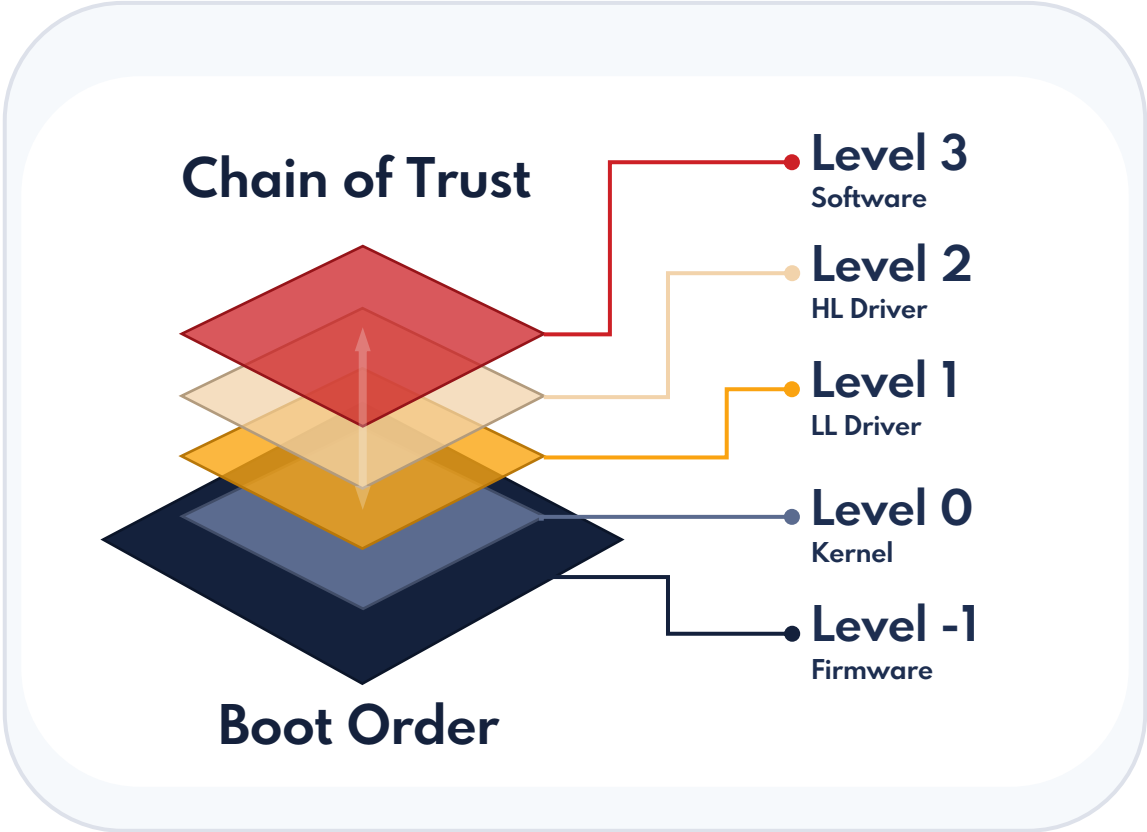
- The process slows data **access time**
- Lost / Destroyed keys also **destroy data**
  - Recovery mechanisms
- **Swap**, Bootloader, /tmp, /var

Disk Encryption
Vulnerabilities

- Break into **unlocked encrypted system**
- **Rubber-hose cryptanalysis** (Folter)
- **Coercion** (Nötigung)
- **Key extraction**



IT-S NOW


Chain of Trust
Level 3
Software
Level 2
HL Driver
Level 1
LL Driver
Level 0
Kernel
Level -1
Firmware
Boot Order

Disk Encryption Methods
Common Features

- **Cryptographic container** that needs to be "unlocked" and mounted to access data
- **Passphrase** and/or **Keyfile** needs to be supplied by the user
- Actual **encryption key** can be derived from user key
  - " is stored in **RAM**
  - " is stored in in the **kernel keyring**

Separated their **layer of operation**.

Disk Encryption Methods
Stacked Filesystem Encryption

Layer that stacks **on top of** the **existing filesystem**

- Files are written to an **encryption-enabled folder**
- Special stacked pseudo-filesystem
- Encryption / Decryption on-the-fly
- **Underlying filesystem** writes to disk
- Files are stored together with **unencrypted files**

Disk Encryption Methods
Full Disk Encryption (FDE)

Operates **below** the **filesystem layer**

- Makes sure that **everything written** is encrypted
- looks like a large blob of **random data**
- **no way** of **determining filesystem** and **data** it contains
- **Mounting** the protected container

IT-S NOW

Comparison	Full Disk Encryption	Stacked FS Encryption
Encrypts	Whole **block devices**	**Files**
Container for encrypted data	Disk / **partition** / virtual	**Directory** in existing FS
Relation to **filesystem**	**Below**	**Above**
File **metadata** encryption	✓	
Whole hard **drive** encryption	✓	
Swap space encryption	✓	
Dynamic **space allocation**		✓
Protect existing filesystems		✓
Offline file-based **backups**		✓

Disk Encryption Methods
Desktop Implementations

- macOS: **HFS+** (FDE), **APFS** (FDE / SFS) (FileVault / Data Protection)
- Windows: **BitLocker** (FDE)
- Linux:

	dm-crypt	VeraCrypt	eCryptfs	EncFS
Enc. stype	block device	block device	stacked FS	stacked FS
Encryption	kernelspace	kernelspace	kernelspace	Userspace
Note	de-facto standard for block device encryption on Linux; very flexible	maintained fork of TrueCrypt	slightly faster than EncFS; individual encrypted files portable between systems	easiest one to use; supports non-root administration
Supported ciphers	Every cipher the kernel Crypto API offers	AES, Twofish, Serpernt, Camellia, Kuznyechik	AES, Blowfish, Twofish...	AES, Blowfish, Twofish, and any other ciphers available on the system

Disk Encryption Methods
Mobile Implementations

- **File-Based Encryption (FBE)**: Different keys for different files.

- iOS / iPadOS: Data Protection
  - file-based encryption
  - Secure Enclave

- Android:
  - Version =< 9: full-disk encryption (dm-crypt)
  - Version => 10: file-based encryption
  - Version 10-12: full-disk encryption*

* only for devices that upgraded from a lower Android version

Disk Encryption Methods
Summary

Who to defend against?

- newbie hacker • professional crypto analyst

What do you want to encrypt?

- user data • system data • both

How should encrypted blocks access?

- Passphrase • key-file • both

When should encrypted parts be unlocked?

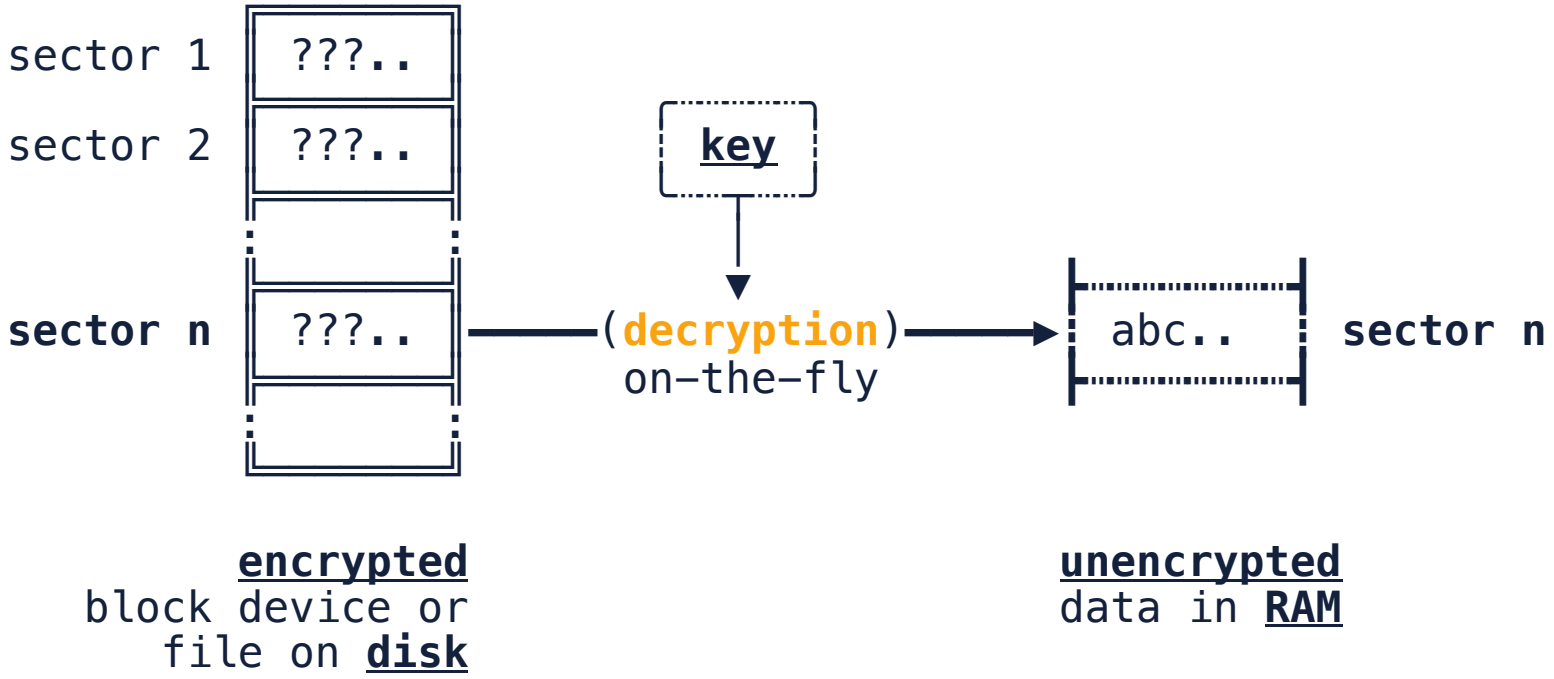
- before / during boot • at login • on demand

Cryptography

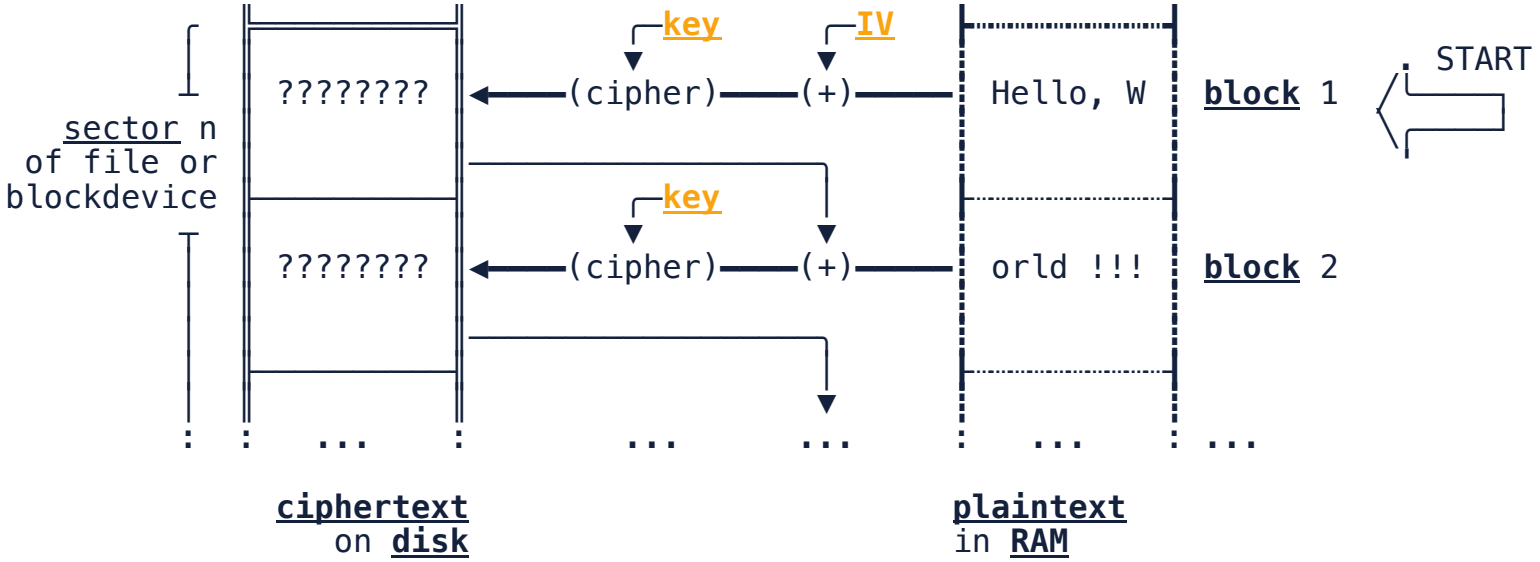
Briefly...

Disk Encryption Concept

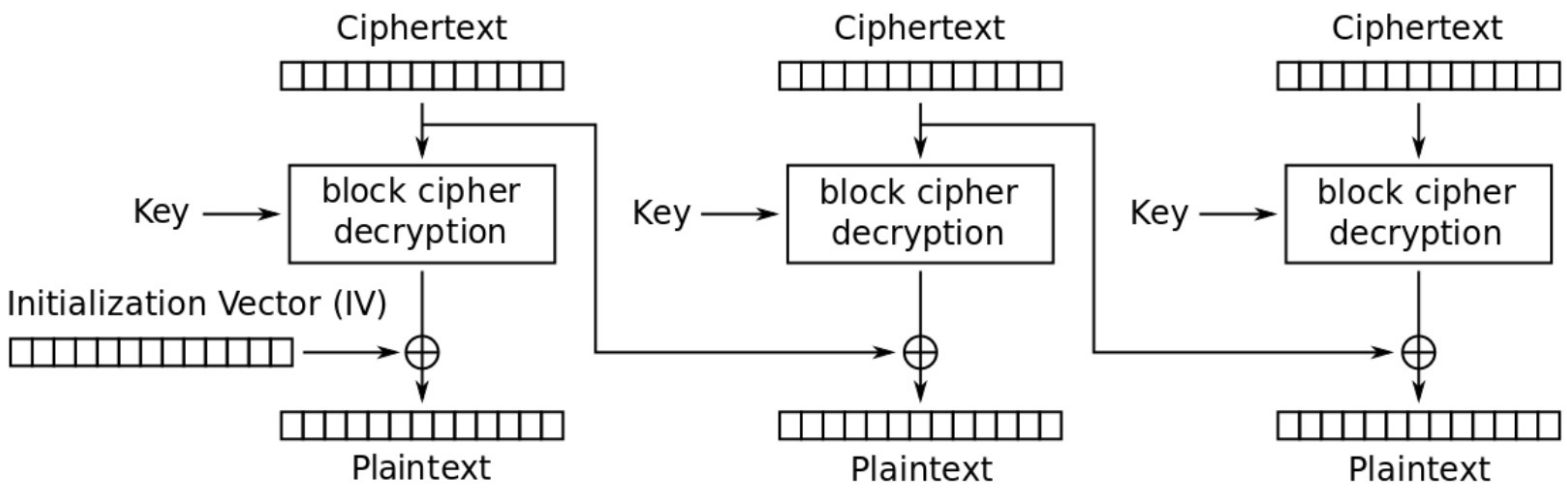
Basis Decryption Procedure



Disk Encryption Concept
Cipher Block Chaining (CBC) Mode



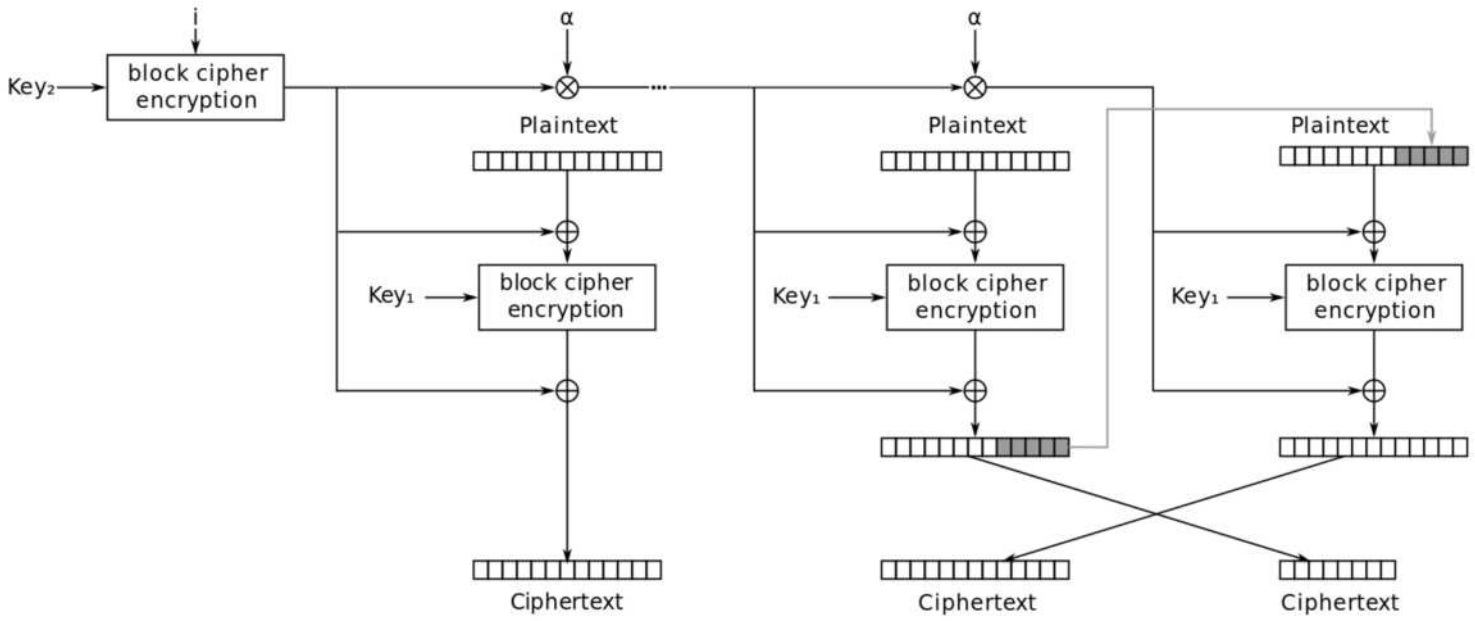
Disk Encryption Concept
Cipher Block Chaining (CBC) Mode



Cipher Block Chaining (CBC) mode decryption

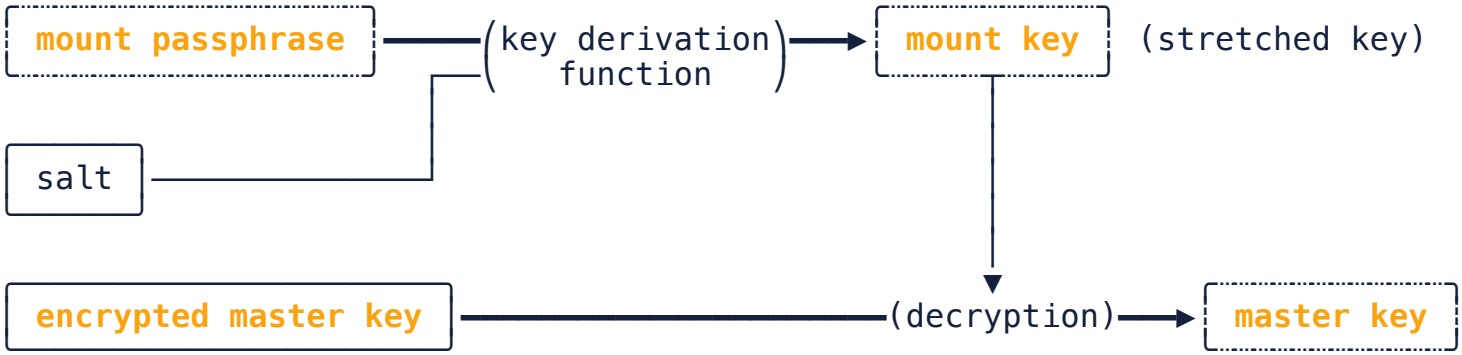
Disk Encryption Concept
XTS Mode

(XOR-encrypt-XOR(XEX)-based tweaked-codebook mode with ciphertext stealing)

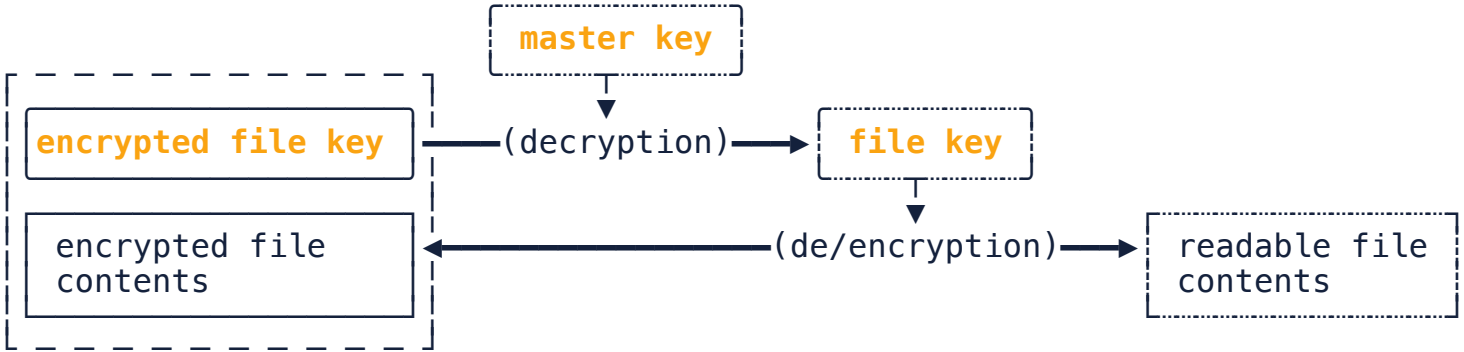


XEX with tweak and ciphertext stealing (XTS) mode encryption

Disk Encryption Methods
Cryptographic metadata



Disk Encryption Methods
Cryptographic metadata



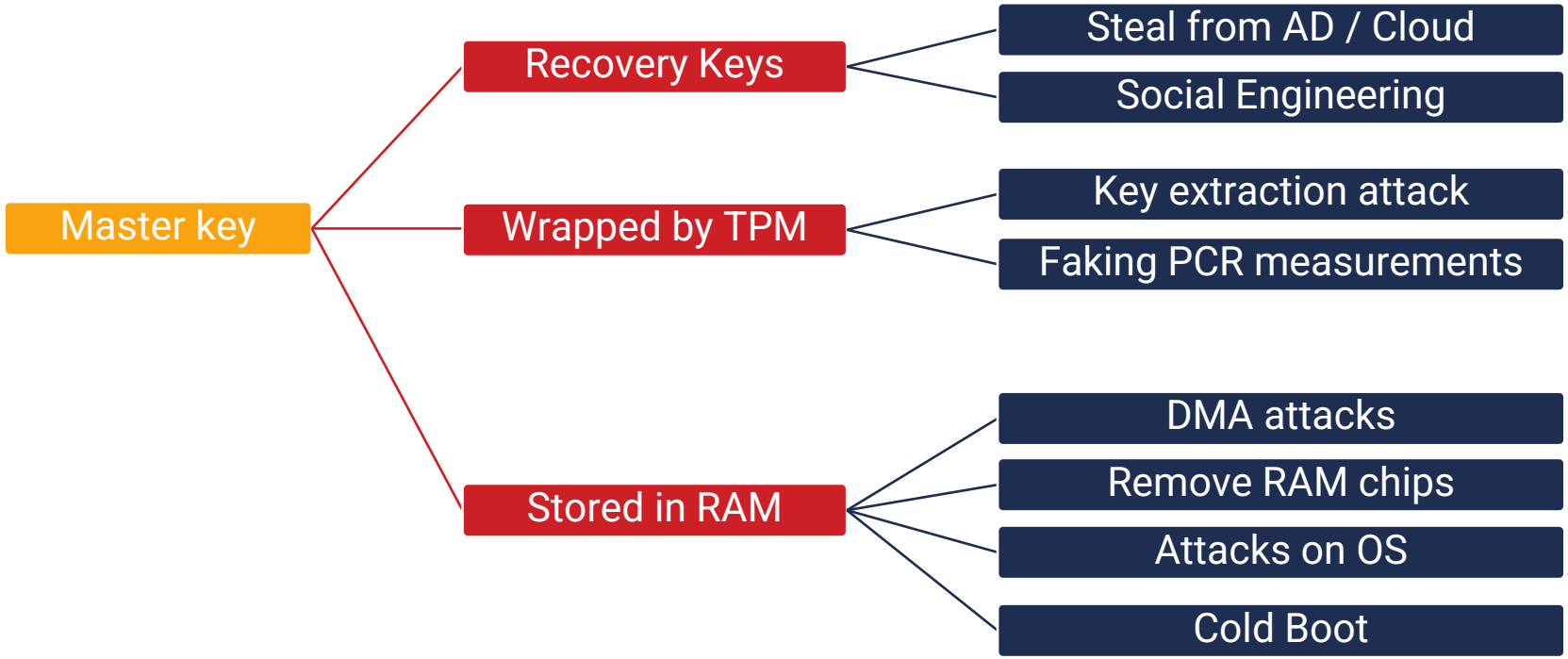
Attacks

on Full Disk Encrpytion

Disk Encryption
Naïve Approach: Brute-force Passphrase

```
>>> hashcat -h | grep FDE
   62XY | TrueCrypt                                          | Full-Disk Encryption (FDE)
     X  | 1 = PBKDF2-HMAC-RIPEMD160                         | Full-Disk Encryption (FDE)
     X  | 2 = PBKDF2-HMAC-SHA512                            | Full-Disk Encryption (FDE)
     X  | 3 = PBKDF2-HMAC-Whirlpool                         | Full-Disk Encryption (FDE)
     X  | 4 = PBKDF2-HMAC-RIPEMD160 + boot-mode             | Full-Disk Encryption (FDE)
      Y | 1 = XTS  512 bit pure AES                         | Full-Disk Encryption (FDE)
      Y | 1 = XTS  512 bit pure Serpent                     | Full-Disk Encryption (FDE)
      Y | 1 = XTS  512 bit pure Twofish                     | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit pure AES                         | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit pure Serpent                     | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit pure Twofish                     | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded AES-Twofish             | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded Serpent-AES             | Full-Disk Encryption (FDE)
      Y | 2 = XTS 1024 bit cascaded Twofish-Serpent         | Full-Disk Encryption (FDE)
      Y | 3 = XTS 1536 bit all                              | Full-Disk Encryption (FDE)
   8800 | Android FDE <= 4.3                                | Full-Disk Encryption (FDE)
  12900 | Samsung DEK (Android FDE)                         | Full-Disk Encryption (FDE)
  12200 | eCryptfs                                          | Full-Disk Encryption (FDE)
  137XY | VeraCrypt                                         | Full-Disk Encryption (FDE)
  14600 | LUKS                                              | Full-Disk Encryption (FDE)
  16700 | FileVault 2                                       | Full-Disk Encryption (FDE)
  18300 | Apple File System (APFS)                          | Full-Disk Encryption (FDE)
```

Disk Encryption
Attack Tree by F-Secure



Cold-Boot Attack

Lest We Remember (2008)

Princeton University

Cold-Boot Attack
Principle

1. Attacker gets **physical access**
2. Attacker performs **cold reboot**
3. **Boot** into minimal OS via **USB** or **PXE**
4. Dump encryption **keys** from **memory**

Cold-boot Attack
Statistics by Kensington

One laptop is stolen every 53 seconds.

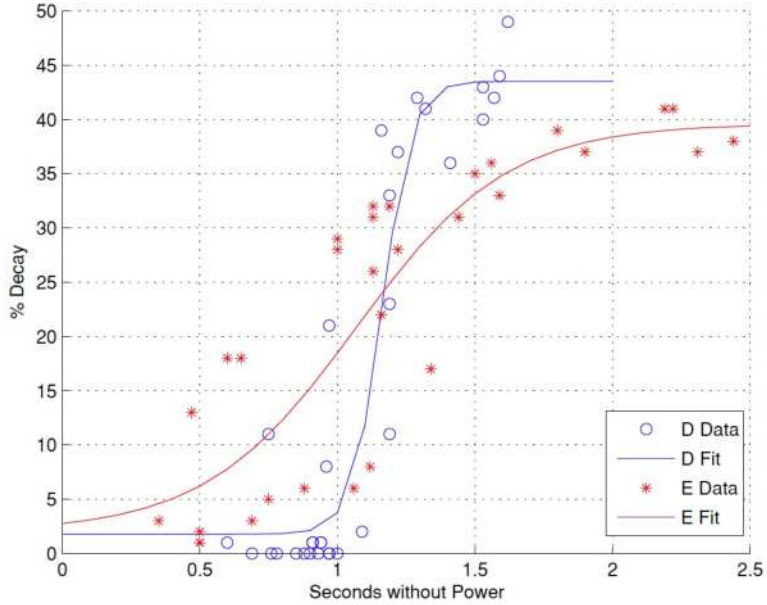
70 million smartphones are lost or stolen each year, with only 7 percent recovered.

80 percent of the cost of a lost laptop is from data breach. 52 percent of devices are stolen from the office/workplace, and 24 percent from conferences.

Cold-Boot Attack
Background

- **DRAM** characterizing remanence effects
- **Decay** at {Room (**seconds**), Reduced (**minutes**)} Temparature
- Error rate (Decayed Bits)
- Liquid Nitrogen

- **Cold** vs. **Hot** Reboot
- Memory wiping and footprint
- POST, ECC
- Key reconstruction



Cold-Boot Attack
Decay Pattern and Predictability

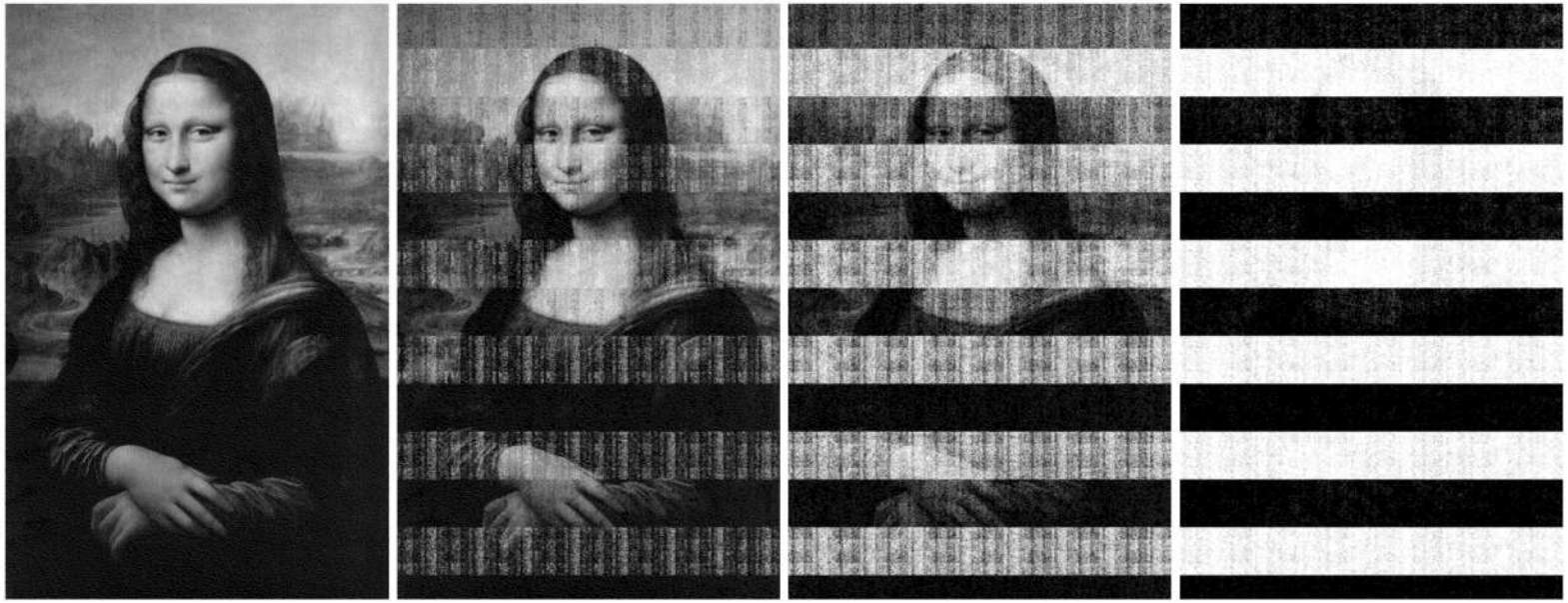


Figure 4: We loaded a bitmap image into memory on Machine A, then cut power for varying lengths of time. After 5 seconds (left), the image is indistinguishable from the original. It gradually becomes more degraded, as shown after 30 seconds, 60 seconds, and 5 minutes.

Cold-Boot Attack
Imaging Residual Memory

Imaging Tools

- PXE network boot
- **USB drives**
- EFI (Net)boot
- iPods

Imaging Attacks (and Problems)

- Simple reboots
- **RAM transplantation**

Cold-Boot Attack

Live Demo

Data Acquisition
Law Enforcement / Forensics

Secure Data Destruction

Recyling Loopback

Secure Data Destruction
Evasion Techniques

Secure Data Destruction

Secret Service

Aus fünf Festplatten wurde Staub

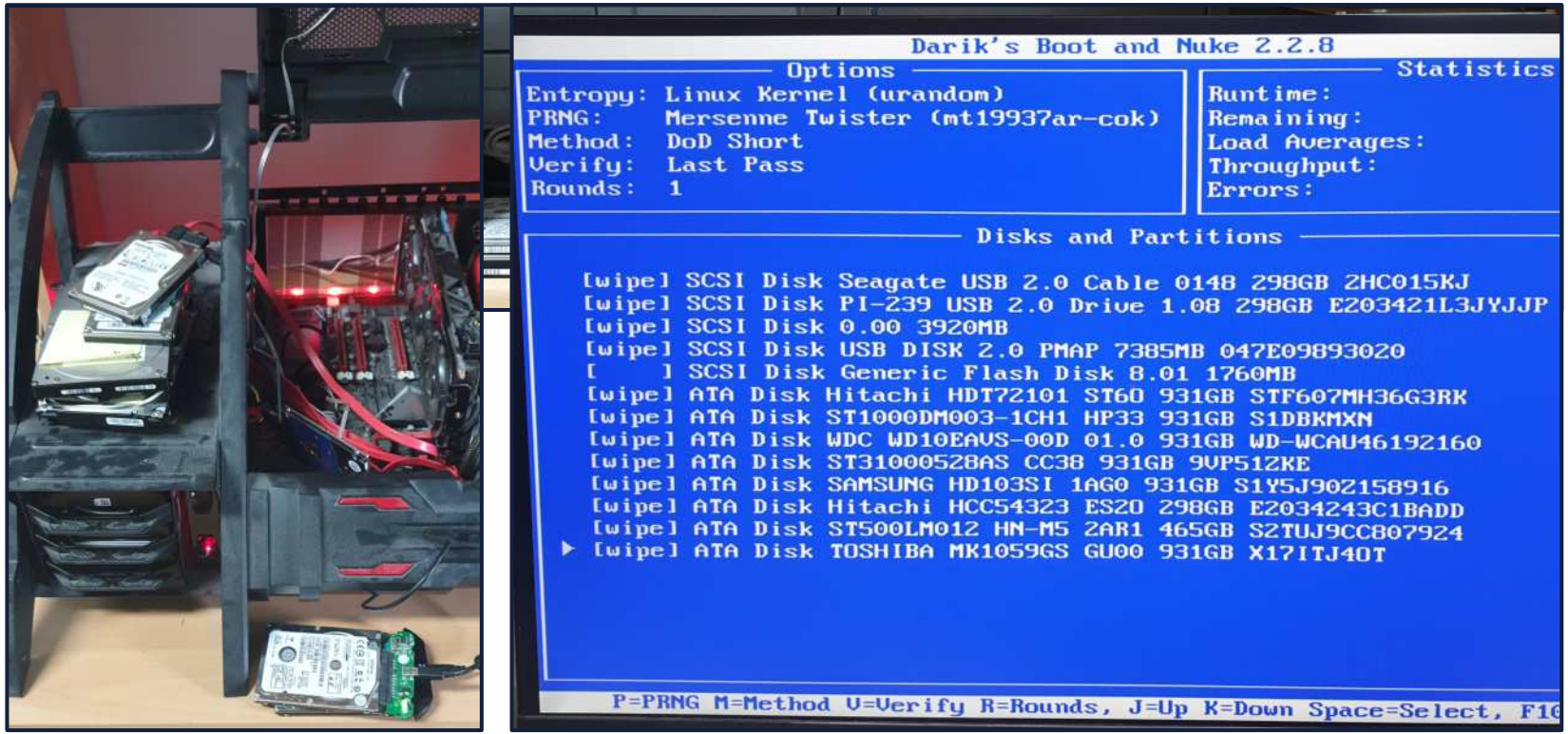
Ex-Kanzleramtsmitarbeiter schredderte und tauchte unter. Reisswolf-Chef überrascht.

Secure Data Destruction

Simple Procedure

Secure Data Destruction

Darik's Boot and Nuke (DBAN)



Learnings

- Local Data Protection:
  - **Full Disk Encryption** (Windows, MacOS, Linux, Android, IOS)
  - **Veracrypt** (External Devices, Plausible Deniability)
  - Hardware Encryption

- Secure (and sustainable) Data Destruction:
  - **DBAN** (Darik's Boot and Nuke)

Thank you for Listenting and Learning!
It's NOW the time to ACT!

powered by

wirtschafts agentur wien

FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

Sources

Content based on:
- https://citp.princeton.edu/our-work/memory/
- https://wiki.archlinux.org/index.php/Disk_encryption
- https://wiki.archlinux.org/index.php/FUSE
- https://www.youtube.com/watch?v=RqvPZnLkP70
- https://www.backblapple.com/en-us/HT204837
- https://jumpcloud.com/blog/what-is-full-disk-encryption-fde/
- https://www.slideshare.net/MSbluehat/bluehat-v18-an-icecold-boot-to-break-bit-locker
- https://www.slideshare.net/MSbluehat
- http://www.learnlinux.org.za/courses/build/fundamentals/fundamentals-all.html
- https://www.garykessler.net/library/file_sigs.html
- https://www.bleepingcomputer.com/news/security/cold-boot-attack-steals-passwords-in-under-two-minutes/
- https://blog.f-secure.com/cold-boot-attacks/
- https://www.brainkart.com/article/XTS-AES-Mode-For-Block-Oriented-Storage-Devices_8420/
- https://dban.org/
- https://source.android.com/security/encryption/full-disk
- https://source.android.com/security/encryption/file-based

Images taken from:
- Slide 3 (Left): https://www.learnlinux.org.za/courses/build/internals/ch08s04.html
- Slide 3 (Right): https://en.wikipedia.org/wiki/List_of_file_signatures
- Slide 9: https://xkcd.com/538/
- Slide 10: https://www.diva-portal.org/smash/get/diva2:830892/FULLTEXT01.pdf
- Slide 21: https://wn.wikipedia.org/wiki/Cipher_Block_Chaining_Mode
- Slide 22: https://en.wikipedia.org/wiki/Disk_encryption_theory#XTS
- Slide 35 (Left): https://wiebetech.com/downloads/556/HotPlug_LT_User_Manual_REV1.0.pdf
- Slide 35 (Right): https://www.logicube.com/
- Slide 37 (Right): https://www.youtube.com/watch?v=b8ghF63cL3g
- Slide 37 (Others): https://duckduckgo.com/?q=kiss+juncker+kurz&iax=images&ia=images
- Slide 38 (Left): https://epaper.vn.at/politik/2019/07/23/aus-fuenf-festplatten-wurde-staub.vn
- Slide 38 (Right): https://resisswolf.com