2550 Intro to cybersecurity

L19 (part 2): Cold Boot attack

abhi shelat/Ran Cohen

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.

Usenix 2008

Protecting data in stolen computers

- Basic protection: password-based login (OS level)
- Attacker can:
  - – remove the hard drive
  - – plug it into its computer
  - – reboot

LOG-IN
Username:
Password:

Stolen computer

Attacker’s computer

Protecting data in stolen computers

- Basic protection: password-based login (OS level)
- Industry best practice: disk encryption

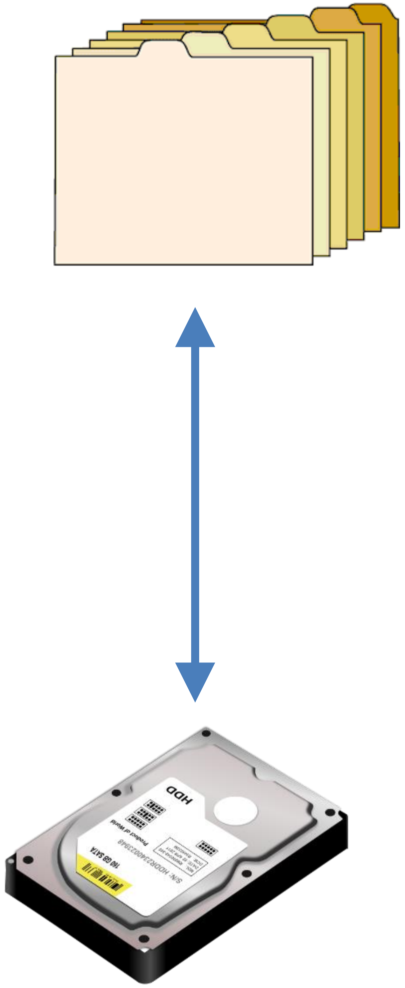
Stolen computer

Attacker’s computer

Disk Encryption Solutions

FileVault (Apple OS/X)

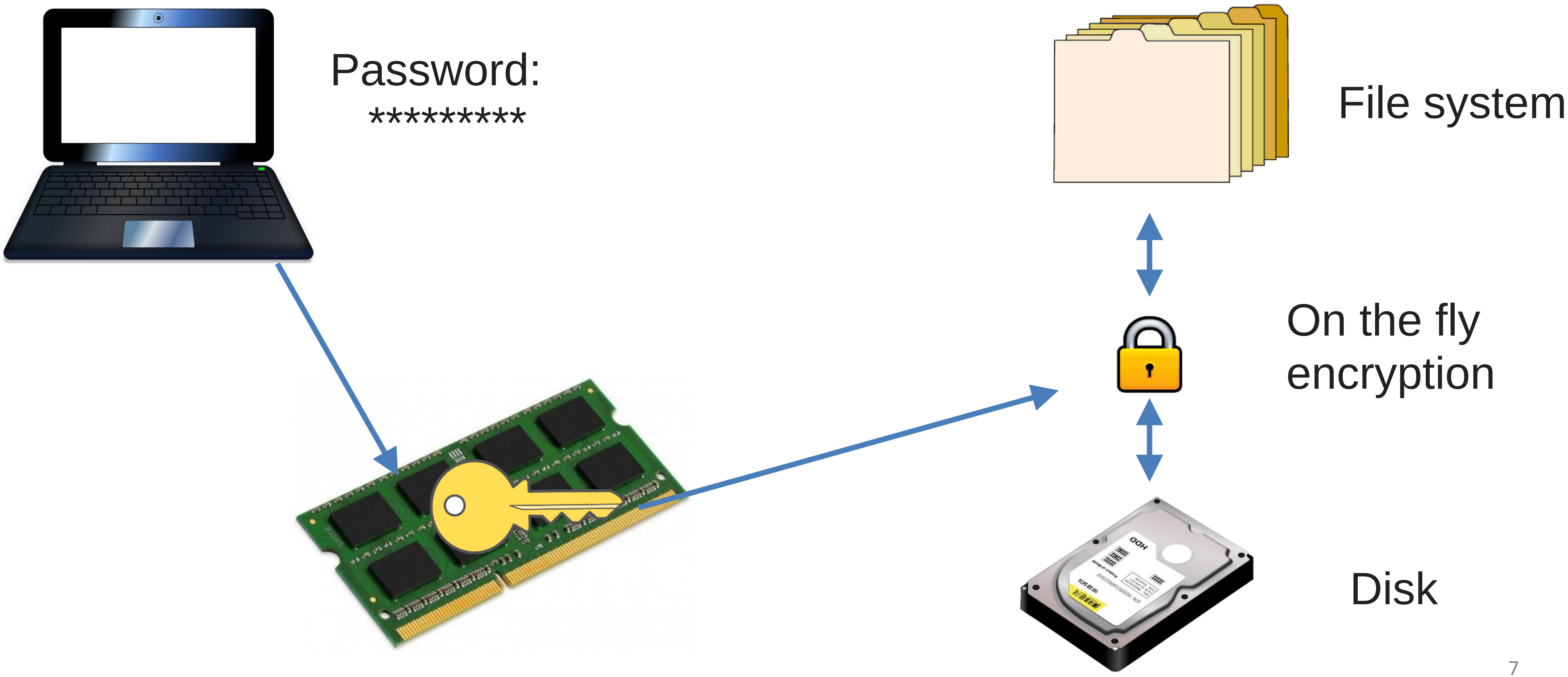
Full Disk Encryption



File system

Disk

Full Disk Encryption



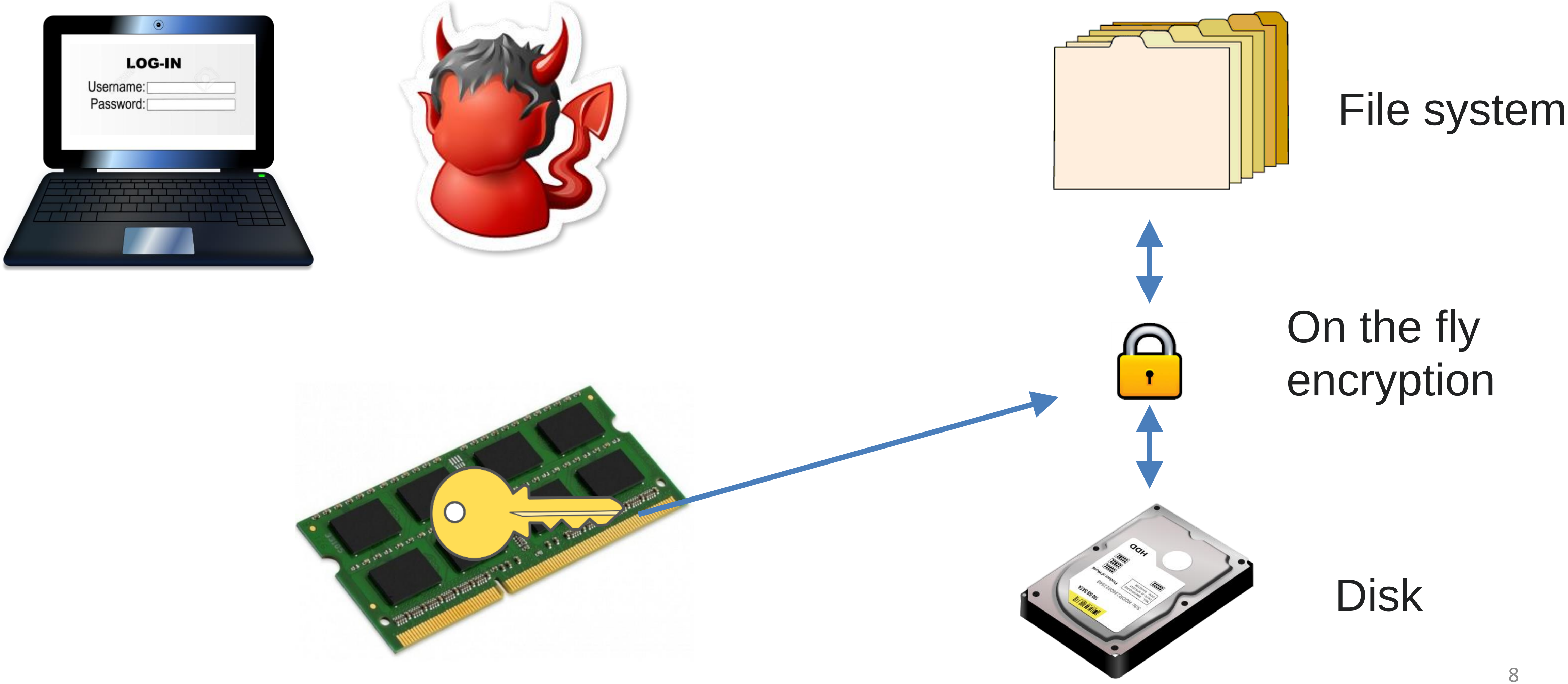
Password:
****

File system

On the fly
encryption

Disk

Full Disk Encryption



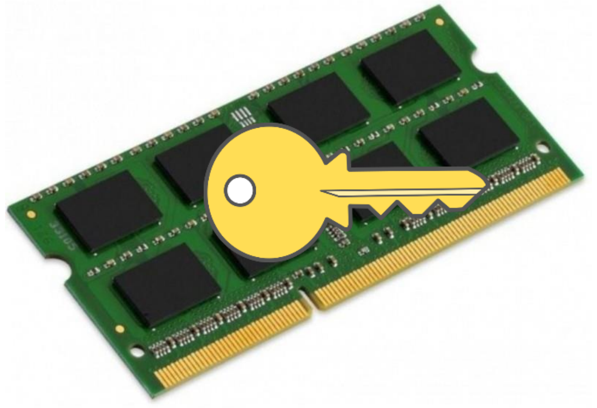
File system

On the fly encryption

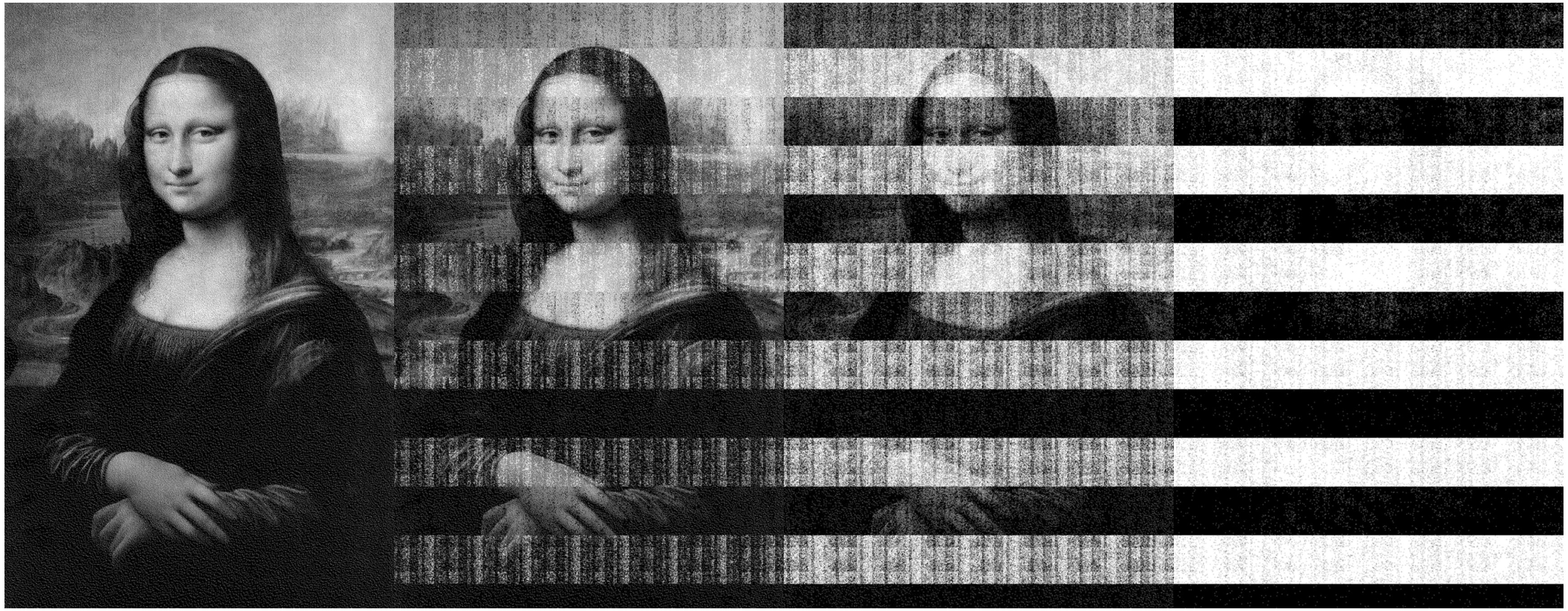
Disk

Common attack scenario

- Assumptions 1: secure encryption
- Assumptions 2: OS protects the key in RAM
- Attacker may try to reboot and intercept before OS loads
- Assumptions 3: RAM is volatile, key will be lost



Decay After Cutting Power



5 secs 30 secs 60 secs 5 mins

Capturing Residual Data

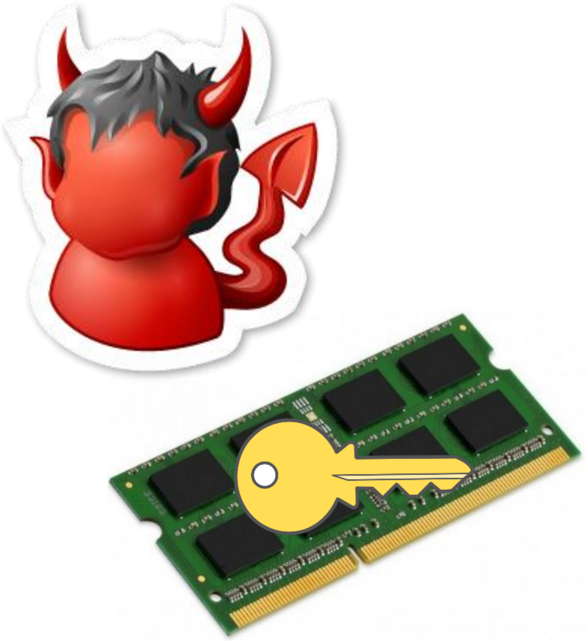
- After disconnecting power large part of RAM remain for a short time
- **Complication:** booting full OS overwrites large areas of RAM
- **Solution:** boot a small low-level program to dump out memory contents
  - PXE (Preboot eXecution Environment) dump (9 KB)
  - EFI (Extensible Firmware Interface) dump (10 KB)
  - USB dump (22 KB)

Basic Cold Boot Attack

Computer locked, disk encrypted, key in RAM

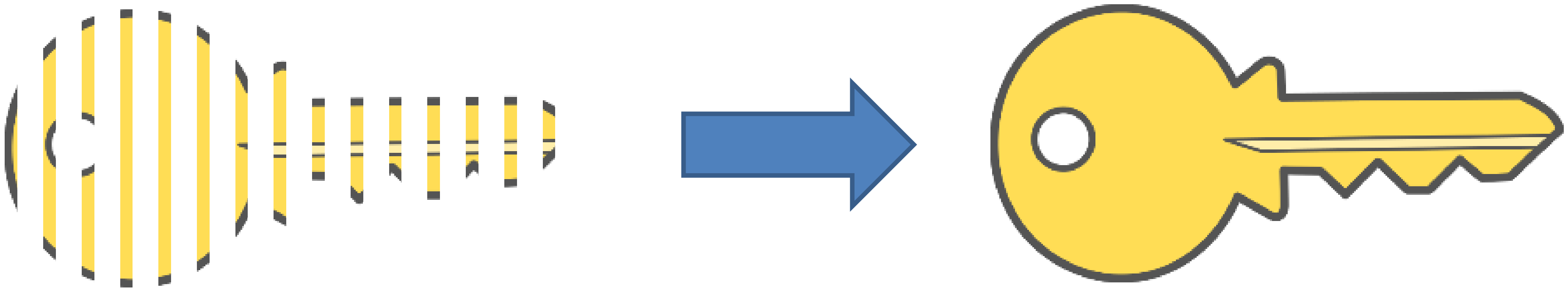
- Attacker can:
  - – Plug USB with memory dumping software
  - – Disconnect and reconnect the battery
  - – Analyze memory dump and extract key
  - – Decrypt the disk

Stolen computer



Recovering the key

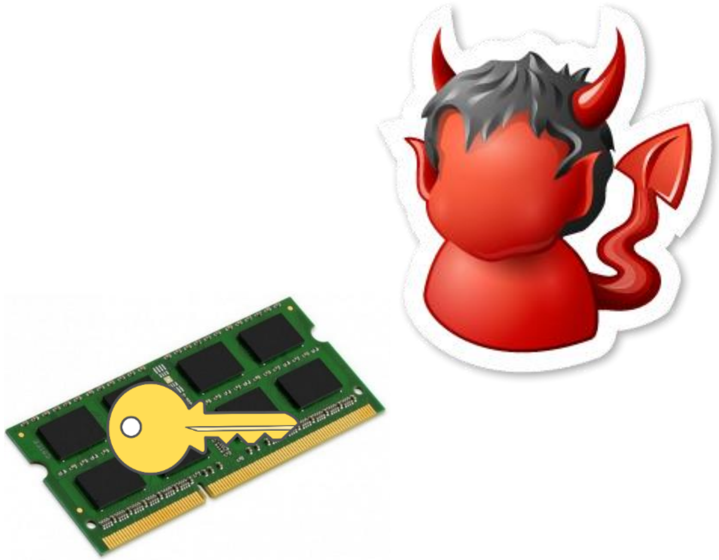
- The attack doesn’t recover the whole key
- For some encryption schemes this is sufficient to recover the key, e.g., AES and RSA
- Opened a new line of research “leakage-resilient cryptography”



What if BIOS Clears RAM?

- Can the attacker move the memory to its own computer where BIOS doesn’t clear RAM?
- Naively that would take too much time
- Solution: cool the memory card

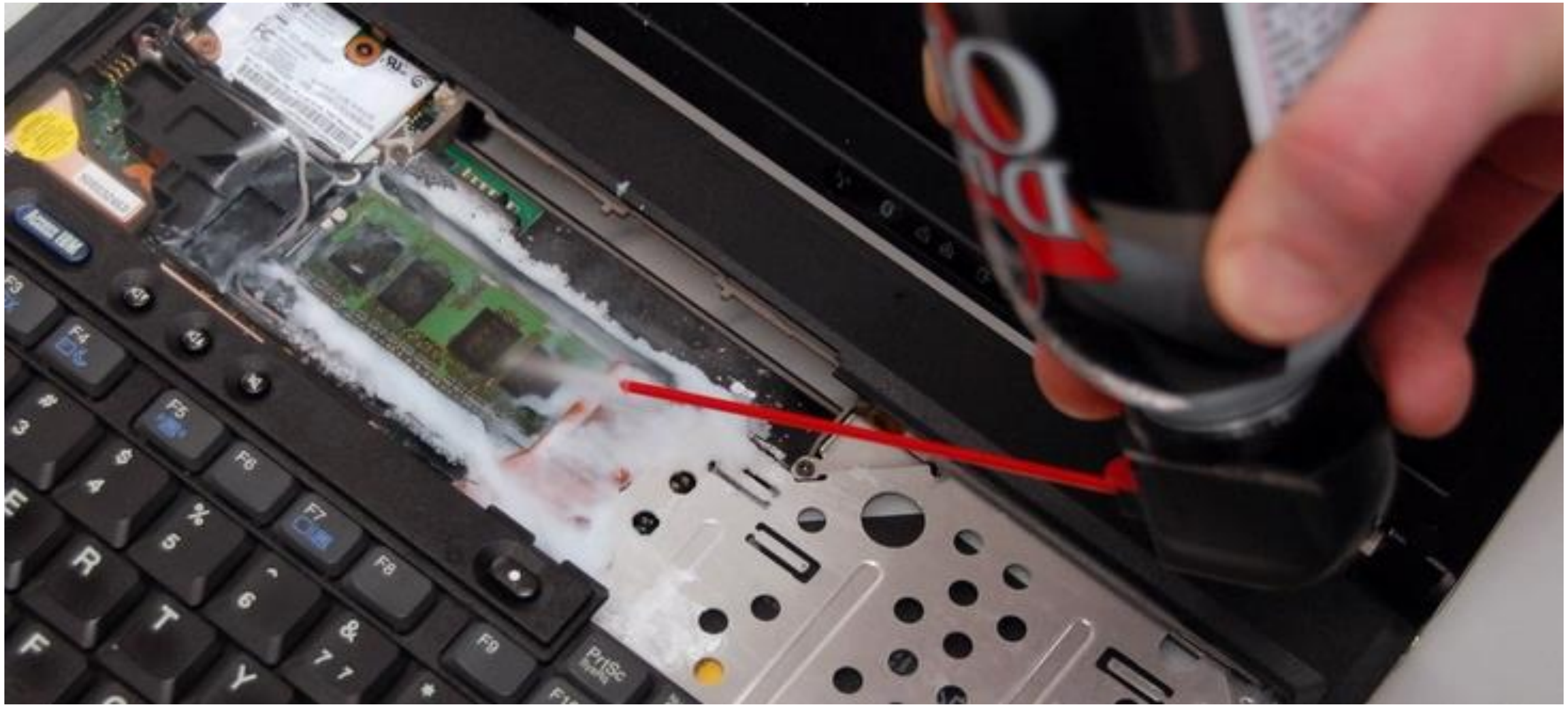
Stolen computer



Attacker’s computer

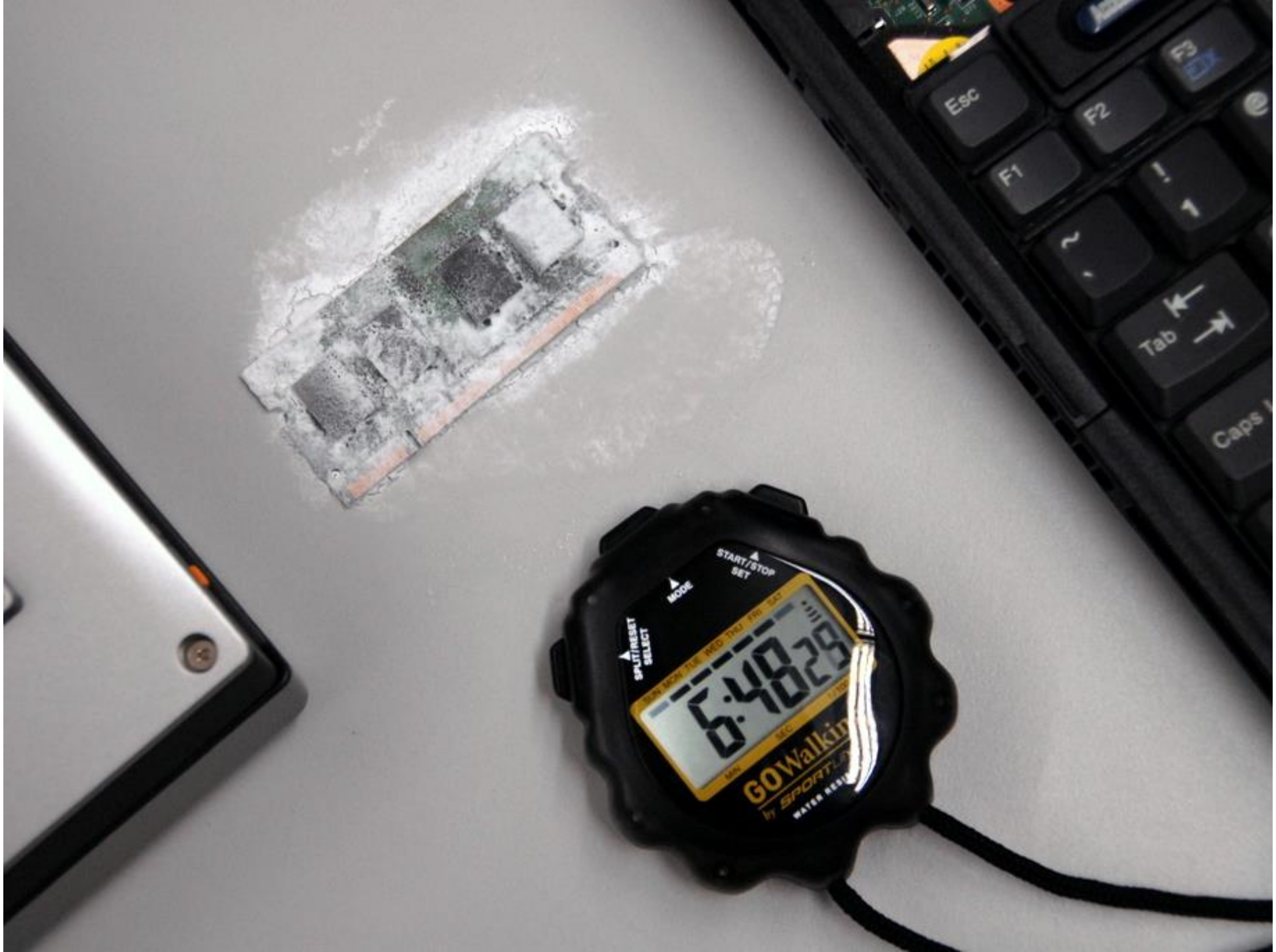
Slowing Decay by Cooling

Spray with upside-down multipurpose duster



-50°C

< 0.2% decay after **1 minute**


START/STOP
SET
MODE
SPLIT/RESET
SELECT
SUN MON TUE WED THU FRI SAT
6:48 29
MIN
SEC
GOWalkin
by SPORTLI
WATER RESIS
Esc
F1
F2
F3
Tab
Caps

Even Cooler

Liquid nitrogen -196°C

< 0.17% decay after **1 hour**

Not necessary in practice