TEL AVIV UNIVERSITY

Information Security – Theory vs. Reality

0368-4474, Winter 2015-2016

Lecture 5:
Side channels: memory, taxonomy

Lecturer:
Eran Tromer

More architectural side channels + Example of a non-cryptographic attack

TENEX directory password validation, inside a system call:

```
check_password(char* given_pass) {
   …
   for (i=0; i<=strlen(correct_pass); i++)
      if (correct_pass[i] != given_pass[i]) {
            sleep (3);
            return EACCESS; // access denied
      }
   return 0;
}
```

Attack each byte at a turn, by placing `given_pass` on a page boundary.

- Timing due to page fault
- Timing due to TLB miss
- Crash due to page fault
- Leftover page status after page fault

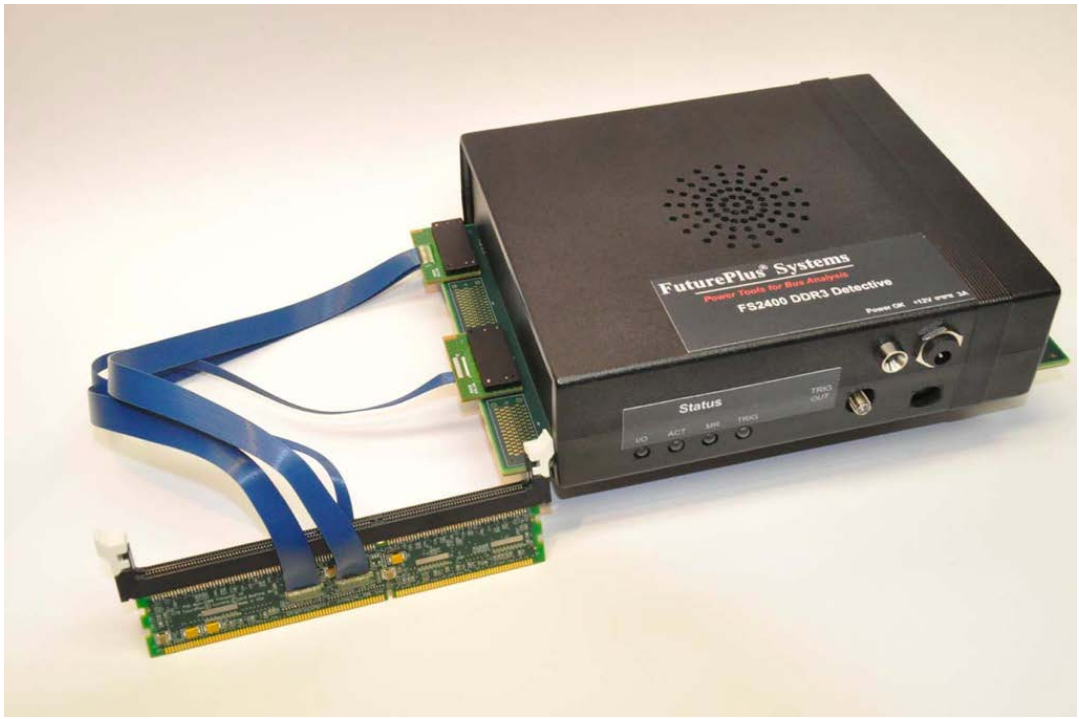
Information leakage from memory and storage

Bypassing memory/storage access controls

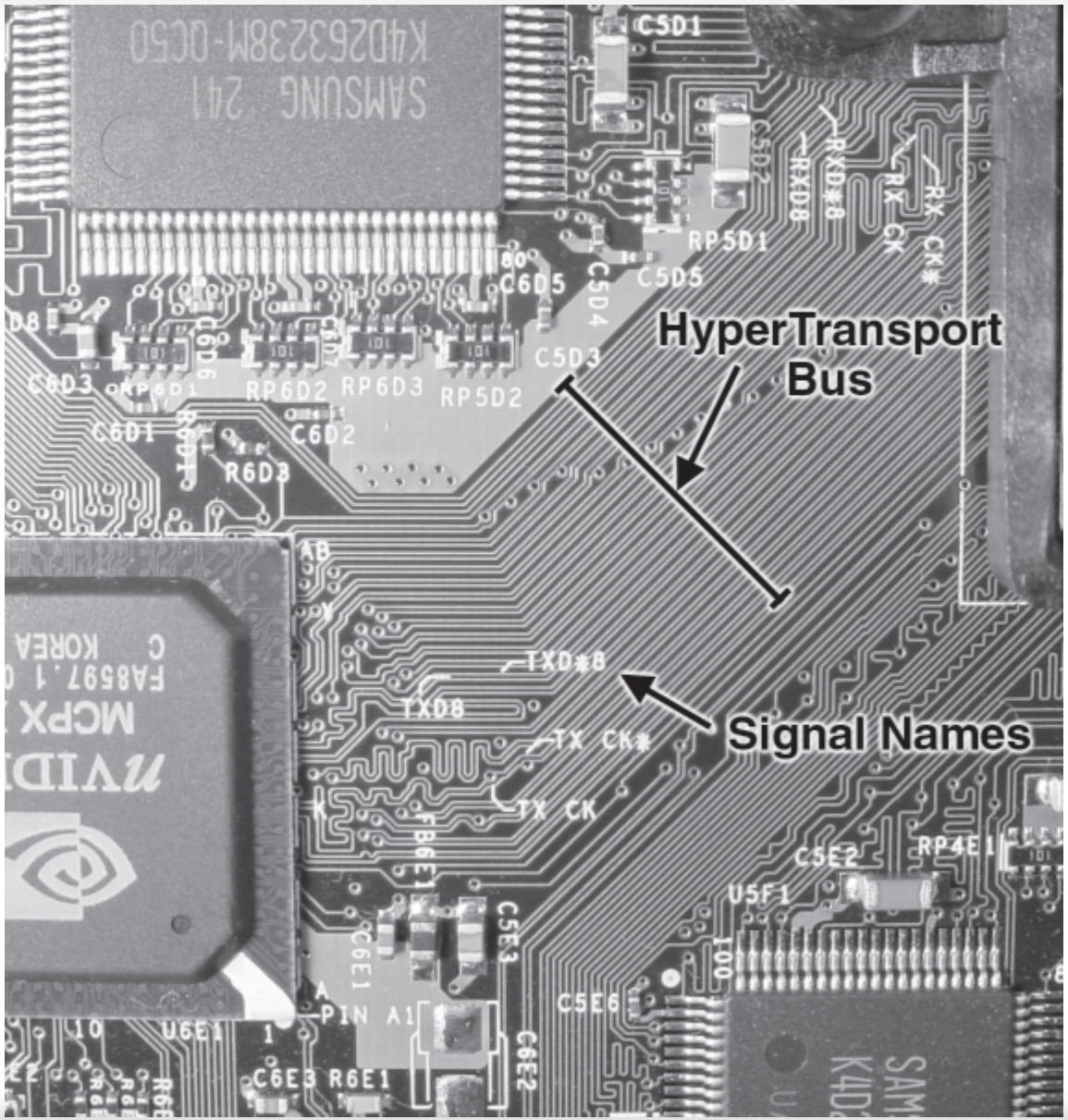
While system operates, DRAM is protected by CPU and OS. Can be circumvented by:

- Hardware snooping
- Data remanence:
  accessing residual data after
  - system shutdown
  - (attempted) logical erasure
  - (attempted) physical erasure

DRAM memory bus analyzers



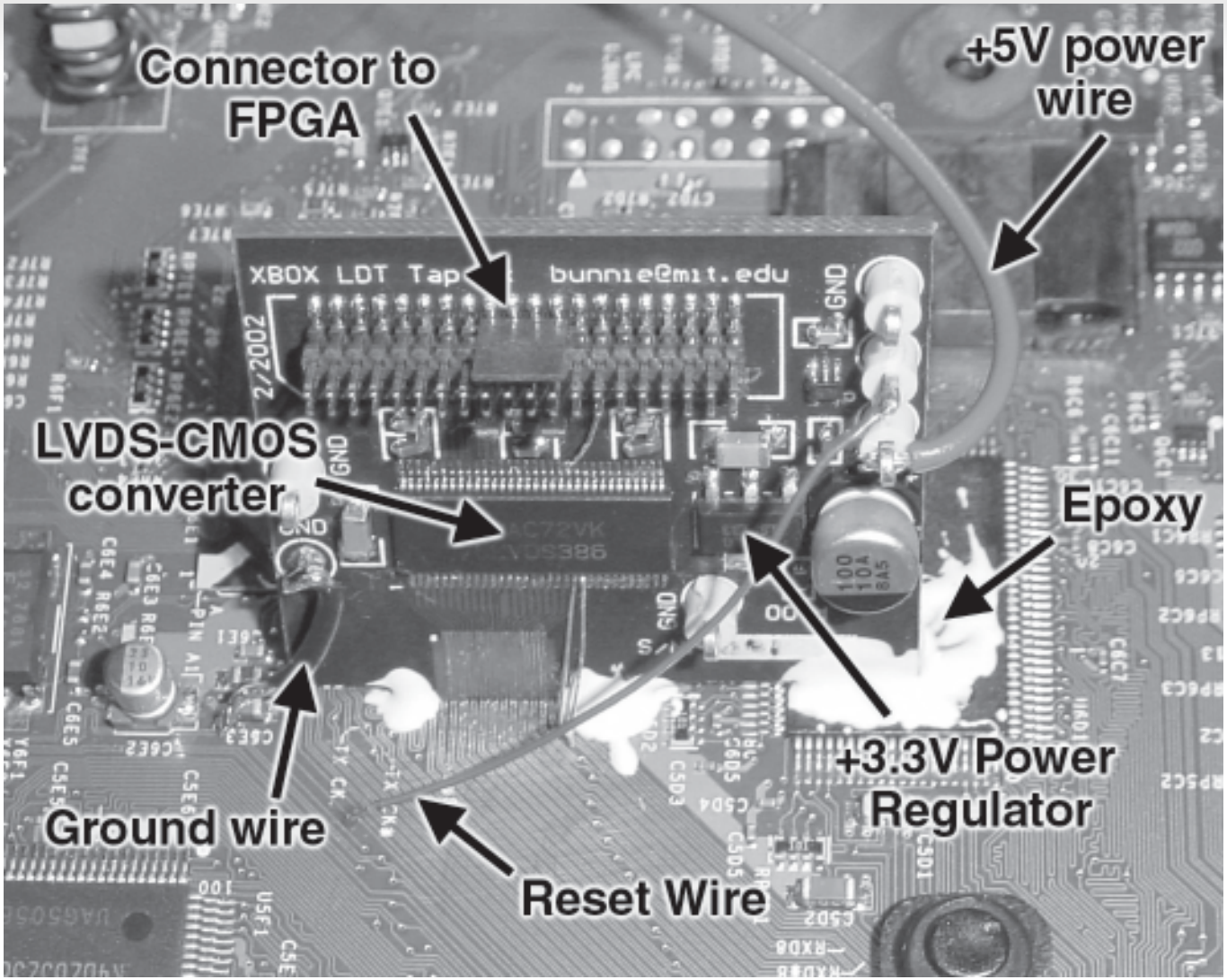
Tapping bus lines on printed circuit boards



Xbox HyperTransport bus traces

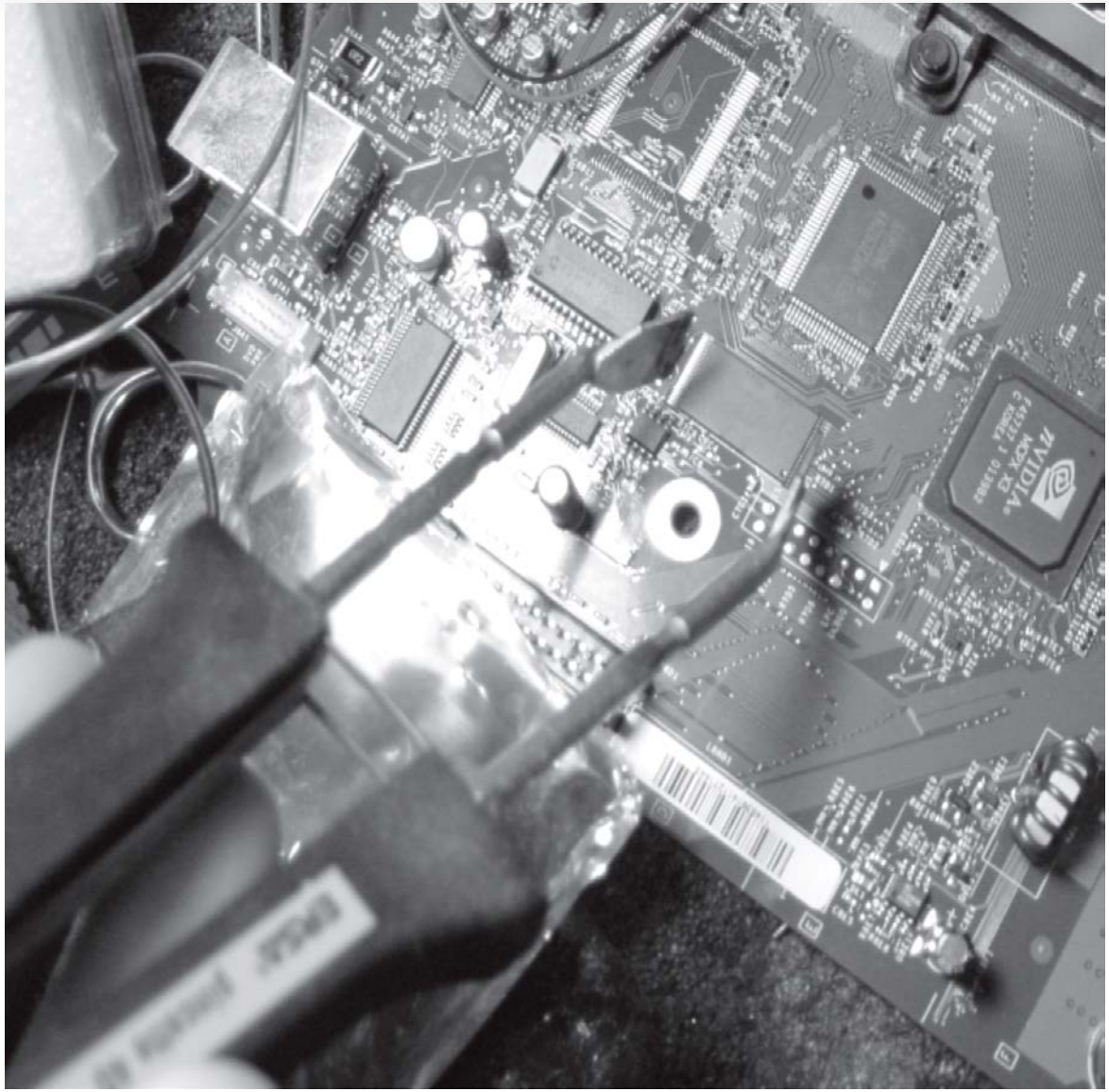
[Andrew “bunnie” Huang”, *Hacking the Xbox*]

Tapping bus lines on printed circuit boards (cont.)



HyperTransport tap board mounted on the Xbox motherboard. [Andrew “bunnie” Huang”, *Hacking the Xbox*]

Directly reading non-volatile memory chips (ROM, EPROM, EEPROM, flash)

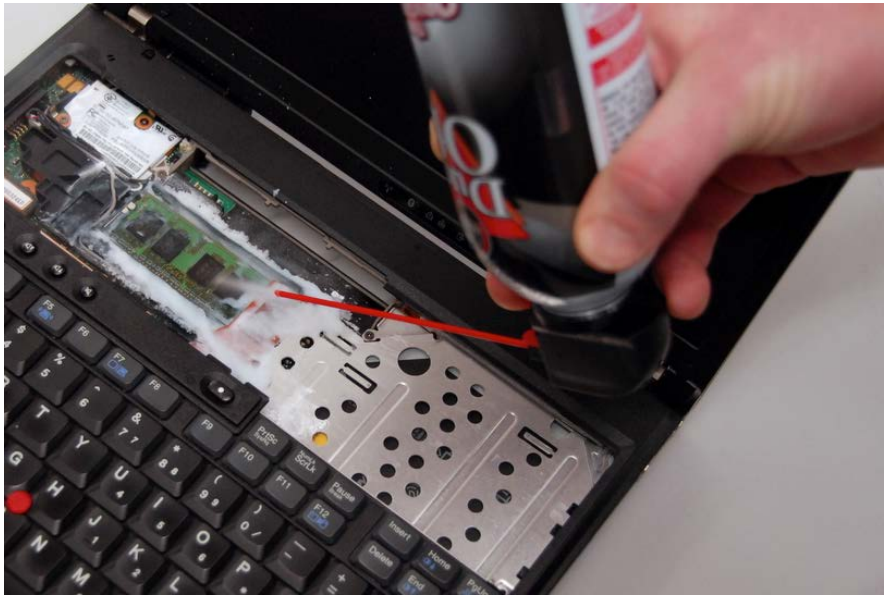


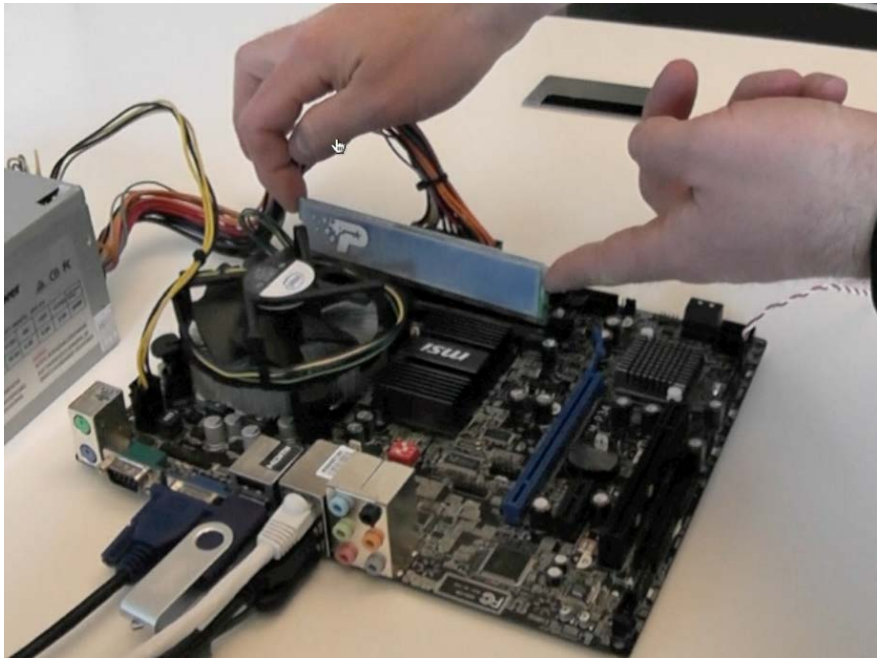
Removing the Xbox FLASH ROM with a tweezer-style soldering iron.
[Andrew “bunnie” Huang”, *Hacking the Xbox*]

DRAM data remanence (“cold boot” attack)

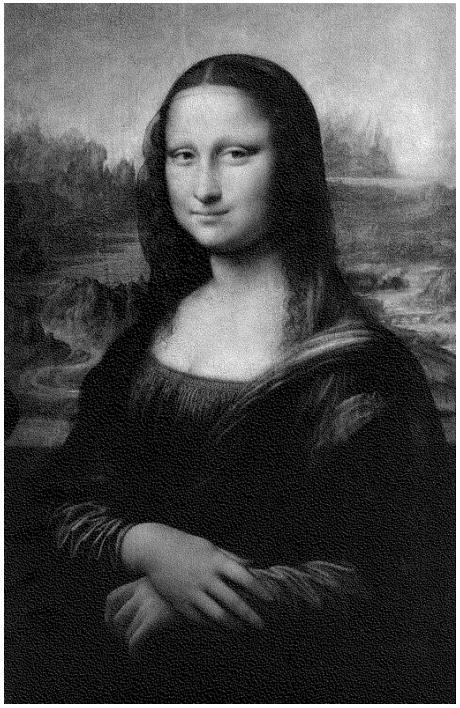
- Freeze the state of volatile DRAM and read it on a different machine
  - Cold boot attack (literally freeze)
  - Keep power using capacitor

[Halderman et al., *Lest We Remember: Cold Boot Attacks on Encryption Keys*, 2008]

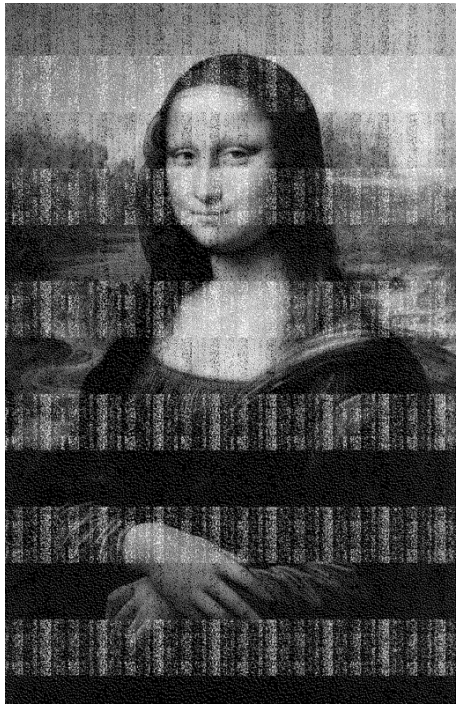




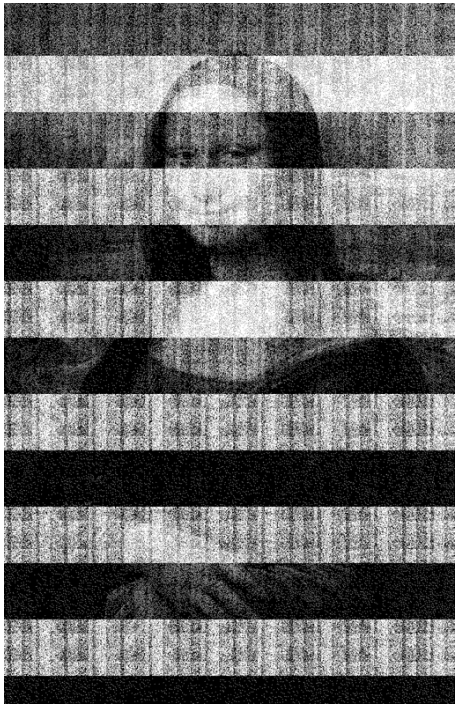
DRAM data remanence ("cold boot" attack), example of memory decay



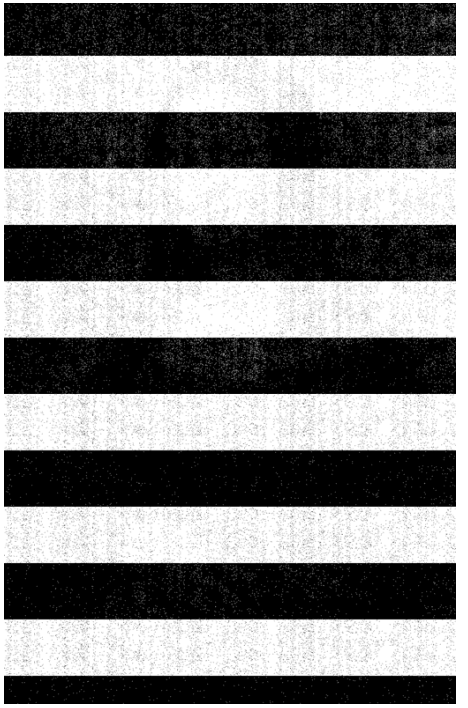
5 seconds



30 seconds



60 seconds



5 minutes

[Halderman et al., *Lest We Remember: Cold Boot Attacks on Encryption Keys*, 2008]

SRAM data remanence

- Data remanence in SRAM
  - Low temperature data remanence is dangerous to tamper resistant devices which store keys and secret data in a battery backed-up SRAM
  - Long period of time data storage causes the data to be “burned-in” and likely to appear after power up; dangerous to secure devices which store keys at the same memory location for years
- Experimental example
  Eight SRAM samples were tested at different conditions
  - at room temperature the retention time varies from 0.1 to 10 sec
  - cooling down to −20ºC increases the retention time to 1…1000 sec, while at −50ºC the data retention time is 10 sec to 10 hours
  - grounding the power supply pin reduces the retention time

Data remanence: continued

Remanence in magnetic hard disk

- Residual bias in magnetic field
- Imperfect alignment of write head on track

→ using high-precision equipment, can peel current data layer and access prior data.

Aided by error-correcting codes.

Remanence at higher levels

- Memory cell
- Smart memory
  - Flash Translation Layer
  - Bad-sector handling
  - Hardware buffers
  - Battery-backed buffers
  - Hybrid disks (HDD+SSD)
- Filesystem (undelete an erased file)
- Application-level (backups, revisions)`

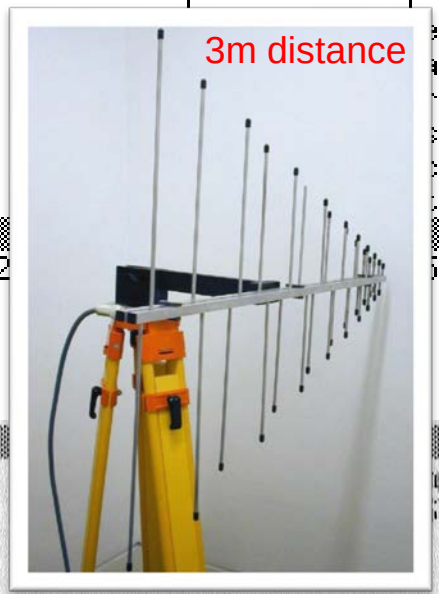
Taxonomy of side/covert channels

Side/covert channels: **physical**

- Electromagnetic
  (radiated emanations)
  - Computation
  - Peripherals
    CRT screen electron gun (van Eck), CRT/LCD screen cable, keyboards, printers
- Electric
  (conducted emanations)
  - Power
  - Ground
    (chassis, shields, cables, adjacent wall socket)
- Mechanical
  - Acoustic
    - Voltage regulators
    - Peripherals (keyboards, printers)
  - Vibrations
    - On-screen keyboards
- Thermal
  - Between cores
  - Between computers
- Optical
  - Status LEDs
  - CRT screens

Electromagnetic “van Eck” attack on analog CRT screen

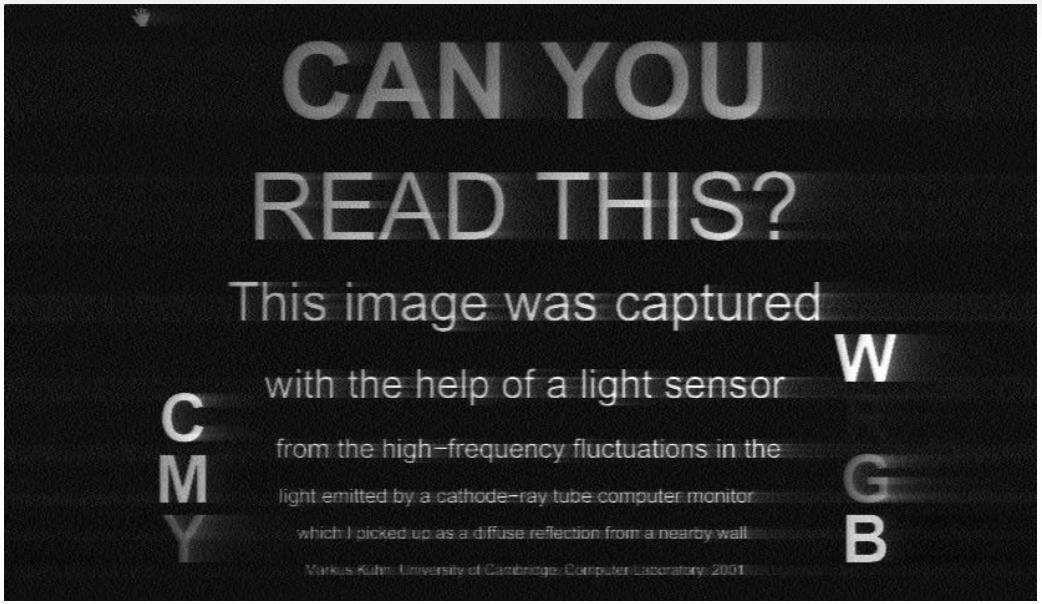
[Markus Kuhn, Compromising emanations: eavesdropping risks of computer displays, 2003]

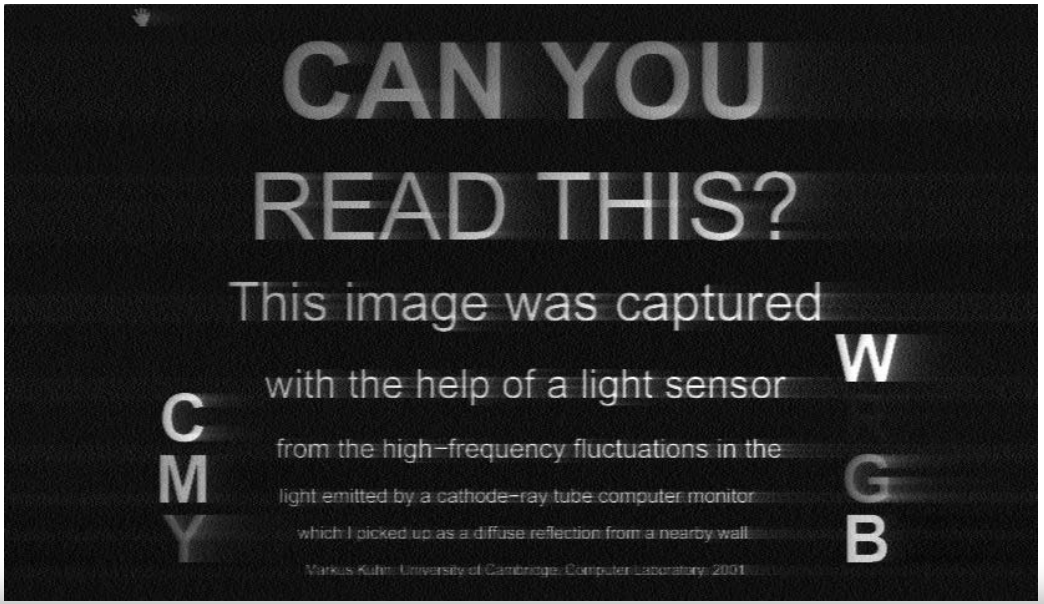


Reflected optical emanations from CRT

[Markus Kuhn, Compromising emanations: eavesdropping risks of computer displays, 2003]

CRT 1m from wall,
photodetector 1.5m from wall





Side/covert channels: **(micro)architecture**

- Data cache
- Instruction cache
- DRAM contention
- Branch predictor
- Functional units
  - ALU
- Paging mechanism
  - Page faults
  - Table Lookaside Buffer
- Memory prefetching
- Hard disks
  - Contention
  - Head movement

Side/covert channels: **OS / VMM / storage virtualization**

- Scheduler
  - Assists other attacks (e.g., temporal resolution for cache attack)
  - Directly exploitable
- Deduplication
  - Assists other attacks
  - Directly exploitable (example: cloud storage dedup)

Side/covert channels: **other**

- Data remanence
  - Hard disks magnetic remnants
  - DRAM/SRAM cells persistance
  - Block remapping
- Timing
  - Nominal computation
    - Optimizations
    - Contention and variable-time operations
  - Error handling

  Often can be done over a network.
- Communication (nominally or by other channels)
  - Data
  - Metadata
    - source, destination
    - flags
    - timing
    - size
      - after compression…
  - Protocol recognition
  - Deanonymization
    - Tor