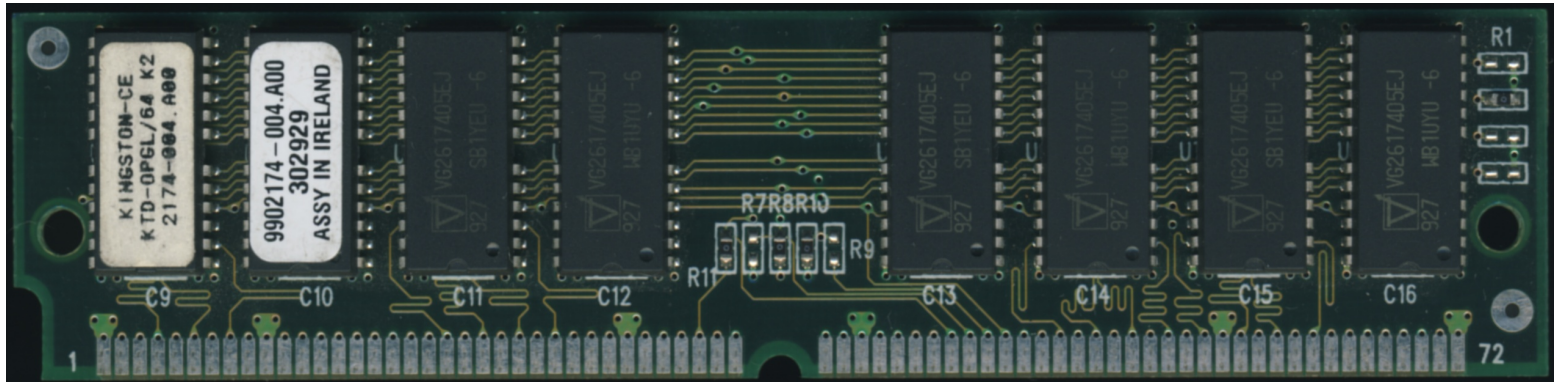
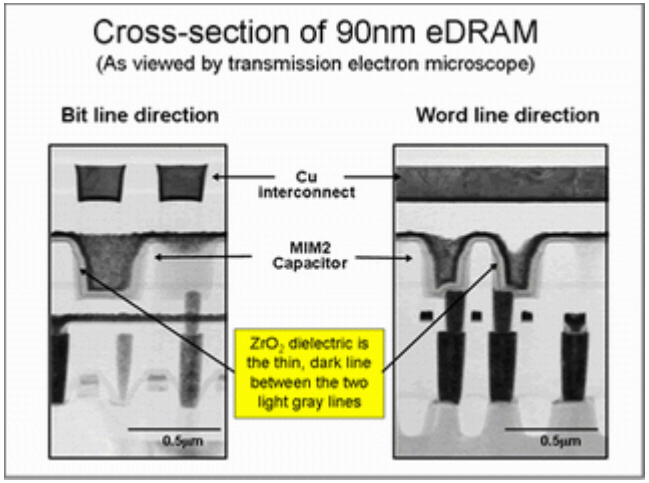
Cold Boot Attacks on Dynamic RAM

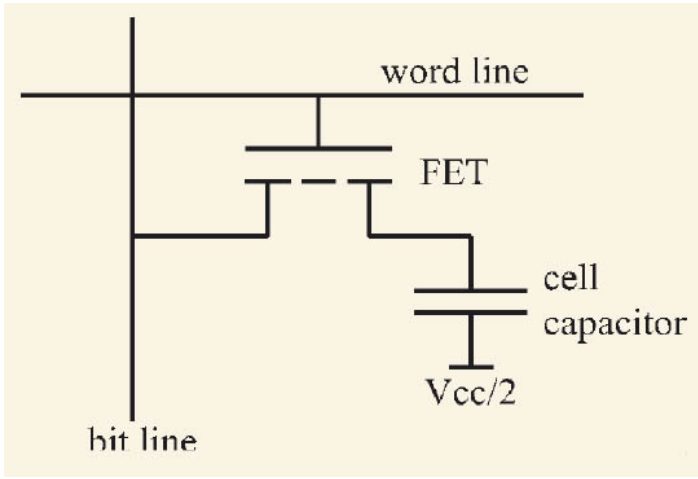


What's this about..

- 1 Bit in Dynamic RAM

  ~=1 Transistor & 1 Capacitor

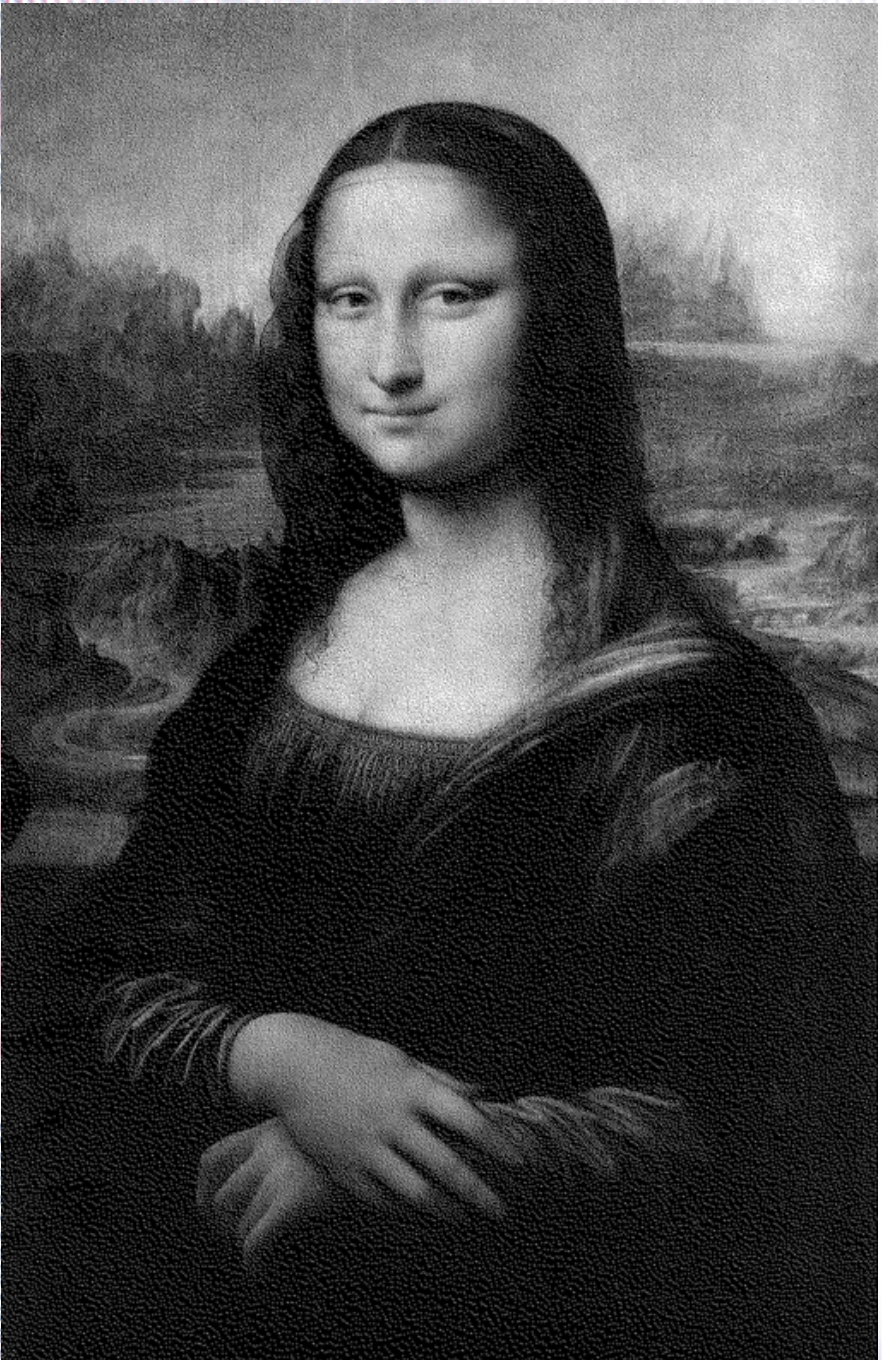




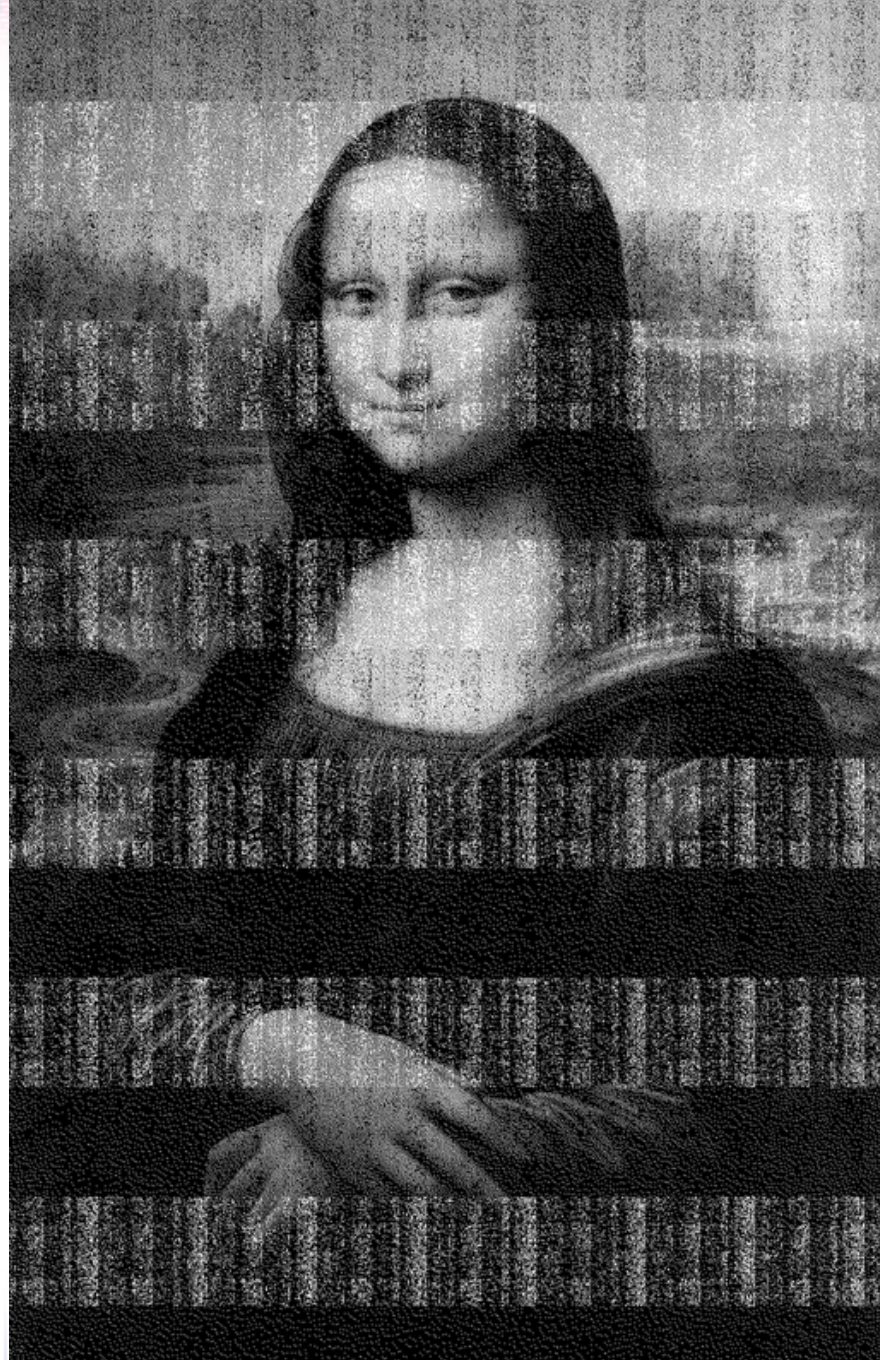
- Refreshing required

...?

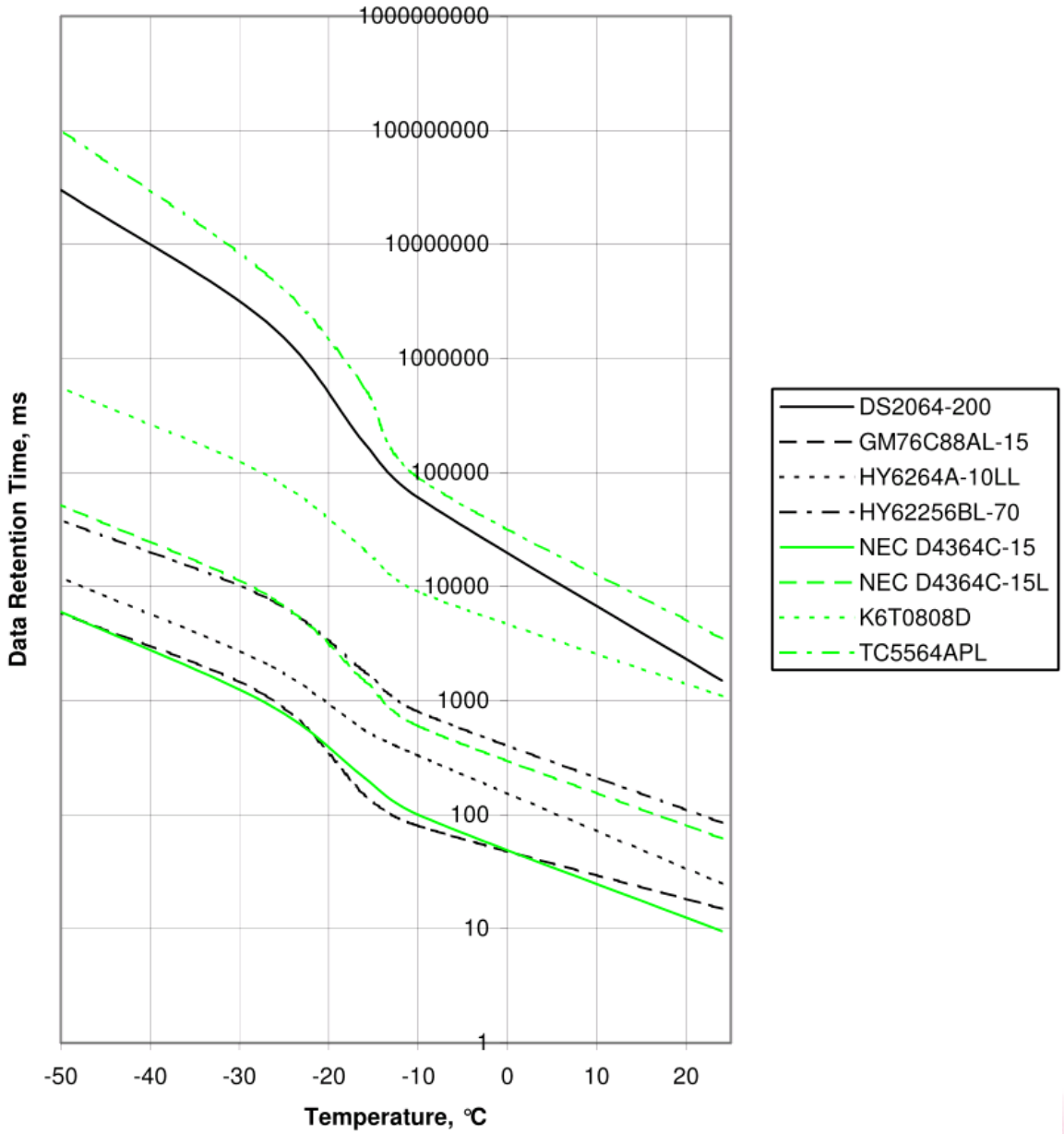
- Cryptographic programs keep passphrases and/or derived keys in Dynamic RAM
- Contrary to common belief, Dynamic RAM doesn't loose it's content quickly
- Common BIOS doesn't zero Dynamic RAM content anymore at bootup



5s 30s
after
power-off



SRAM Chips with Power Supply Pin Connected to GND



Physical effects and threat model

- Cooled memory modules keep content for weeks
- Threat model: Physical Memory Access
- Computer can be just shut down or running and locked
- Attack: Retrieval of Memory Modules or Rebooting into RAM extraction environment

Typical Scenarios

- Airport inspection of a notebook that was just shut down (GPG-Keys, VPN Passphrase, ...)
- Extraction of HDD/SDD encryption keys from a fully encrypted web server

..but they won't do that..?

- They already do.
- Federal and State Agencies routinely use RAM extraction from running and recently rebooted/shutdown systems
- Preferred modus operandi for extraction from running and locked systems: IEEE1394 and Thunderbolt DMA RAM content retrieval

So how does the extraction work?

- Stage 1: Reboot into minimal Kernel on USB device or Physical removal of Dynamic RAM modules
- Stage 2: Saving Dynamic RAM module state on permanent storage media
- Stage 3: Retrieve cryptographic keys by searching for known Data Structures of cryptographic software and/or Key Scheduling of symmetric ciphers

What can I do?

- Shutdown script that wipes memory (e.g. kexec of secure-delete package smem utility)
- Configure encryption software to wipe memory on unmount
- Avoid using system suspension – Use hibernation
- Disable key caching
- Off-Topic: Disable IEEE1394 and Thunderbolt

Sources

- http://citp.princeton.edu/memory
- Real Digital Forensics (Jones, Bejtlich, Rose / 2009)
- https://launchpad.net/ubuntu/+source/secure-delete
- Low temperature data remanence in static RAM (Skorobogatov / 2002)