Week 1 Reading

Cold Boot

Stephen Beard
Team Member 2
Team Member 3

Summary

- DRAM cells hold state much longer than one might expect
- Authors show several ways to prolong this duration via cooling
- Authors show several ways to then access memory and extract sensitive data (like disk encryption keys)
- Mitigation is difficult

	Seconds w/o power	Error % at operating temp.	Error % at −50 °C
A	60	41	(no errors)
	300	50	0.000095
B	360	50	(no errors)
	600	50	0.000036
C	120	41	0.00105
	360	42	0.00144
D	40	50	0.025
	80	50	0.18

Table 2: Effect of cooling on error rates

Threat Model

- Attacker has physical access to a computer that is either on, slept, or recently turned off
- Sensitive data kept in memory in plain-text

Remanence Effects

- Decay rates across time for six different machines

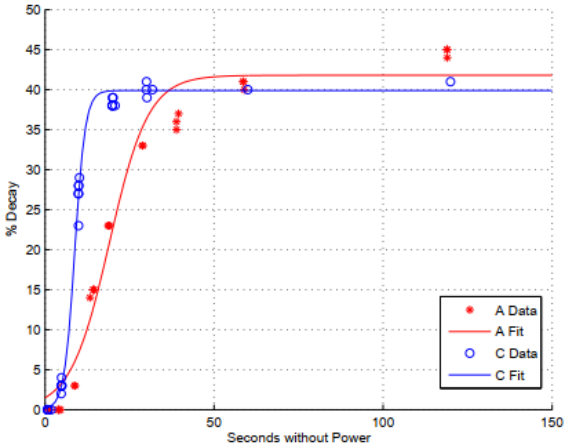


Figure 1: Machines A and C

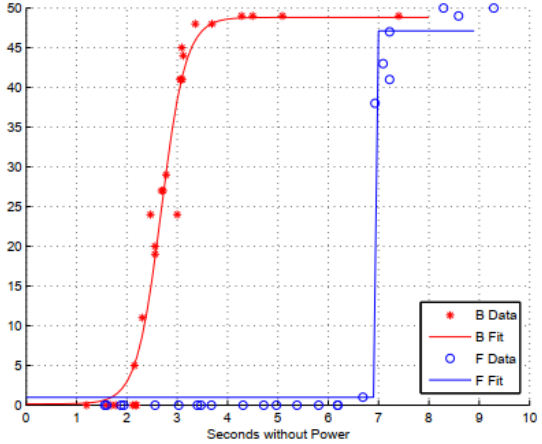


Figure 2: Machines B and F

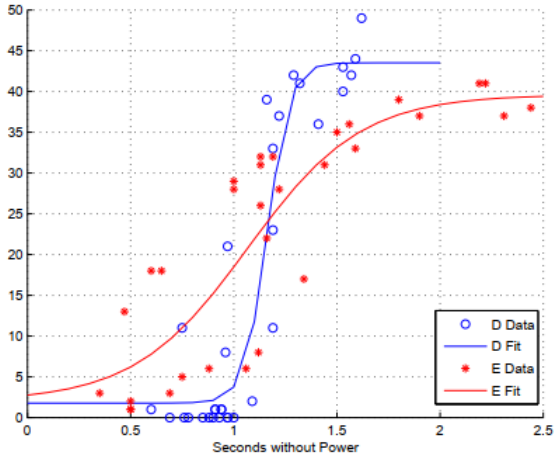
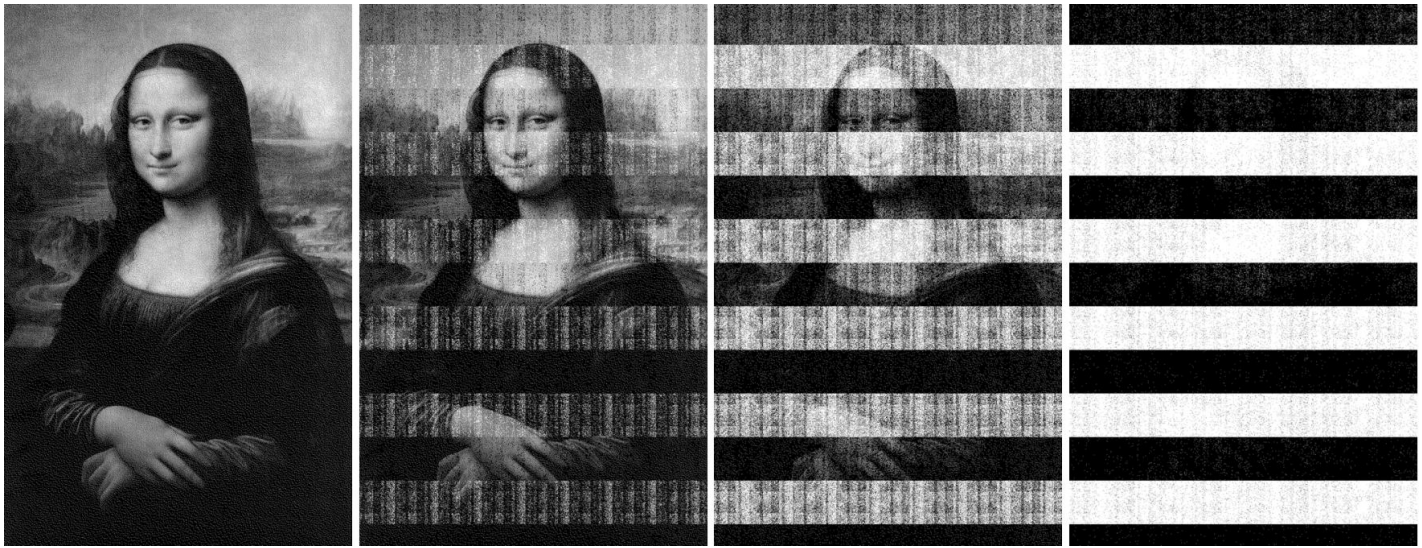


Figure 3: Machines D and E

Remanence Effects Visualized

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.



Imaging Residual Memory

- Three attack payload delivery modes
  - PXE Network Boot
  - USB Drive (including using an iPod)
  - EFI Boot Application
- Two Attack Vectors
  - Simple Reboot
  - Transfer DRAM modules
    - Bypasses any built-in protection (memory wiping)
- Cooling memory (with compressed air cans or liquid nitrogen) greatly extends the time cells hold their state

Key Reconstruction

- Authors discovered that even when memory decays, it decays in predictable patterns
- They developed several algorithms to model the decay, identify, and recover DES, AES, and RSA keys
- Key recovery then used to attack various disk encryption techniques
  - BitLocker (Windows)
  - FileVault (Apple)
  - TrueCrypt (open-source, OS agnostic)
  - Dm-crypt (Linux)
  - Loop-AES (Linux)

Countermeasures

- Scrubbing memory
- Limiting boot vectors
- Safely suspending a system
  - Flush sensitive data from memory on sleep, require key reentry
  - Only shutdown
- Avoiding Precomputation
- Key obfuscation
- Physical Defense
- Architectural Changes