

# Cold Boot Attacks

---

Janosch Gräf <janosch.graef@cispa.saarland>

Cihan Biyikli <mail@cihan-biyikli.de>

May 17, 2017

Center for IT-Security, Privacy and Accountability

**What happens when you turn off your  
computer?**

**Data stays in memory**

## Memory contents

Memory contains sensitive data:

- cryptographic keys
- e.g. key for encrypted hard drive
- passwords
- cookies
- other authentication tokens
- sensitive files that were cached
- kernel data structures: e.g. connections that were open

# Attack

---

# Cold Boot Attack

1. Get physical access
2. Reset machine
3. Dump memory
4. Extract secrets
5. ...
6. PROFIT

# Cold Boot

- *Cold Boot* → Boot after machine was powered off
  - Memory might lose contents
  - Always possible with physical access:  
Power switch, pull cable, remove battery
- *Warm Boot* → OS Reboot, Reset button
  - OS reboot cleans up secrets
  - Reset button not always available

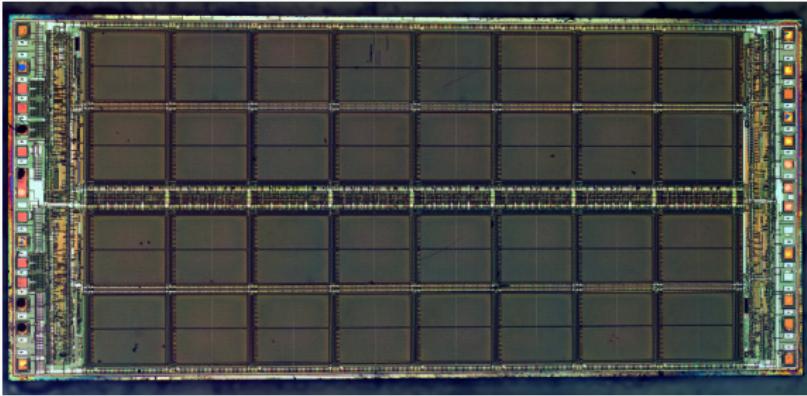
# Dumping memory

There are two good methods. Each with advantages and disadvantages:

1. Boot lightweight kernel (USB or PXE) that dumps memory.
2. Move memory to another machine, that is designed to dump memory.



# DRAM

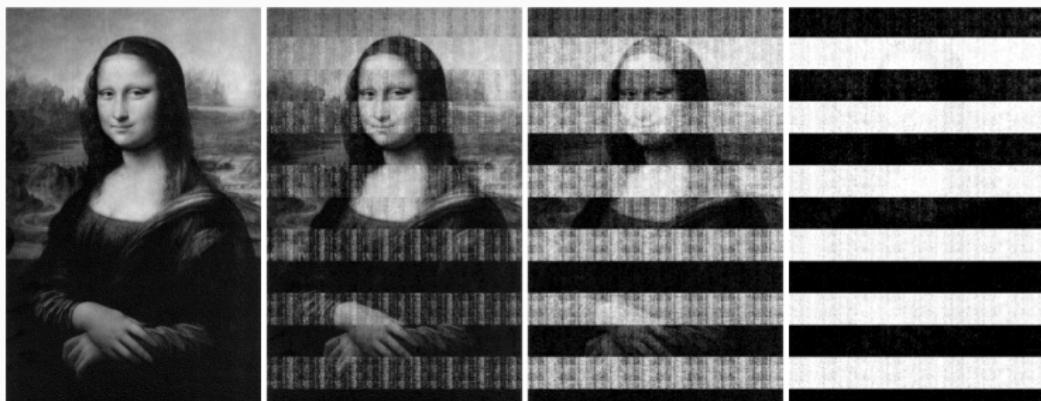


Source: <https://zeptobars.com/en/read/how-to-open-microchip-asic-what-inside>

- Modern computers use *Dynamic Random Access Memory*
- Cells that store a bit each.
- Cells consist of a transistor and a capacitor
- If not refreshed (while power is off), memory loses contents.
- Usual refresh period is  $64ms$ .

# Keeping memory intact

- Cooling slows down discharge of capacitors
- Data stays intact longer



**Figure 1:** Image in memory without cooling after 5s, 30s, 60s, 5min[1]

# Fixing memory corruption

- Errors are predictable
- Secrets' structure might help reconstruct
- AES: key schedule
- RSA: given the public key
- Plain text is constrained to ASCII
- Checksums (e.g. credit card number)

# Extracting useful information

- Properties of keys also help to find them.
- Kernel structures are relatively easy to find
- Give access to (buffered) files, processes, etc.
- Many formats have signatures

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAAKCAQEAYP5htKbf4qBWbbDKwUrmxxuMqg3abwJQUSTR5pgeaq/fPfs1  
+j/N7eU4Y/YPmsuvsNrILlJMP+maLjA1BgHhL9mCvyT+E1hyEEKFMWXATvuBymMq  
FDL3U3741pYXop/jtcS+CgFWTeR5T54WWjtBBC4KpM42quMtf46zuXLjTUzzTsAl  
dL/9m4vgHpf3h3pyPQpykFZqBoyY+WjaKpx0ecj9p7l2Xquao474hb6owE/T1BKN  
U1jty5v4xvjEsjaHRafzV5Vph/zV8ZfumruPlLqcV/epJde6b8/gNoZJNXYZDUHz  
3BkbLIWPc/jeFn061kfnnvm7TzTLDcEYbTlETwIDAQABaoIBAGXNQ1unsfotT91b  
FDb24xCyCXsQbTSQrXGPSXpMTgunbKE0HfbUXk9CLF+k/55d0Gz5Qy8DDA/LGAaQ  
5oq4ZQBBYRHxDgNT3lT5bIBp6+P6IMOL7exKkBdVKmEpdVzdNWJ520fMDXl0xfagv  
4A5vuKyPTWDP+axwsFK1RB6H7EZ32w+wu0yJnDfgLt+K1NW6CGz+ExP3cG68qfF0  
lw78ZSJqq7Ti2ZjL/MqnIX6RW87LjL+wTldecWMAi7W44qSd4sT9sy6xP/eBUR2q  
kA+nfRqNzrsLoKoWkZC2mCc9d/1scf0kksbCasFzlzLm+0AvPX8yyS+U5jmjoGV3  
pKtuprECqYEAE9YqpUtemaGvUtGRnqcQN4cxv0JVp5Ho1ktVKsa0wp7bFamKS9A+6
```

# Mitigation

- Don't leave your computer alone!
- Shut down (or hibernate) if you leave it
- BIOS password, disable USB/PXE booting
- Glue or solder the RAM
- Use software that wipes sensitive data
- Enable destructive POST<sup>1</sup>
- Use hard disks with integrated encryption

---

<sup>1</sup>Power-On-Self-Test

## Summary

- Your memory contains lots of sensitive data
- Memory can stay intact when powered off
- Try to keep off-time short or cool memory
- Use USB, PXE or screwdriver to dump memory
- Errors are fixable

## Demo Time!

---

# Demo



**Figure 2:** Our victim: A Raspberry Pi

# Demo



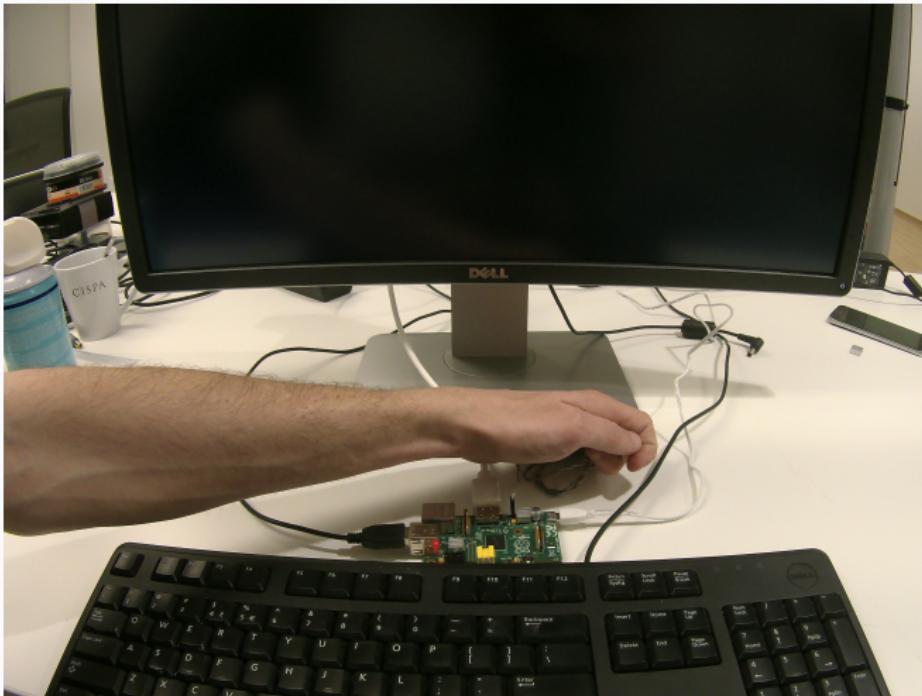
**Figure 3:** Loading secret into memory, by reading the file, its contents are loaded into the OS' file-system buffer.

# Demo



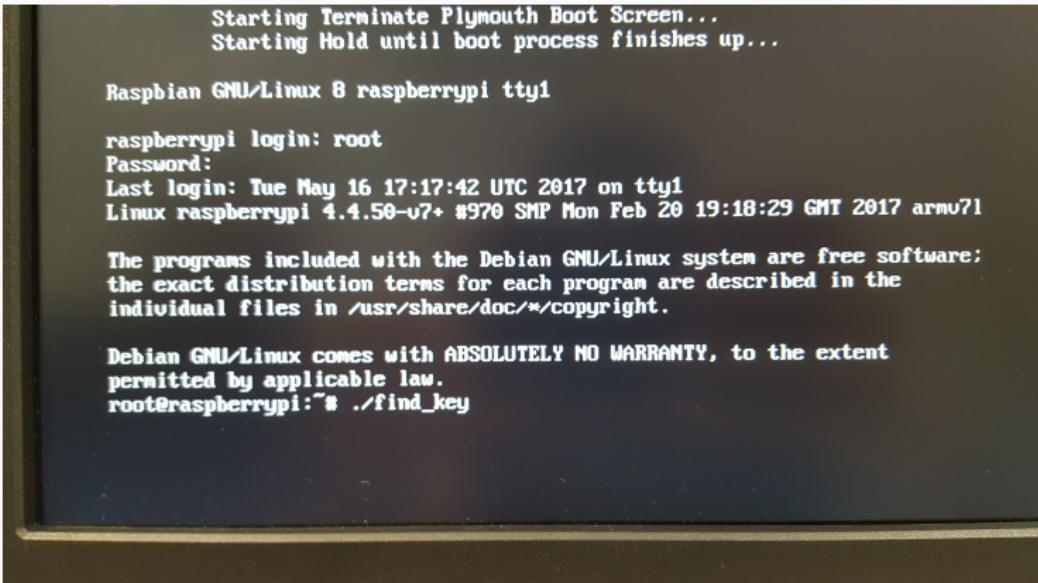
**Figure 4:** Cooling down memory with an inverted duster can.

# Demo



**Figure 5:** Power-cycling the Raspberry Pi

# Demo

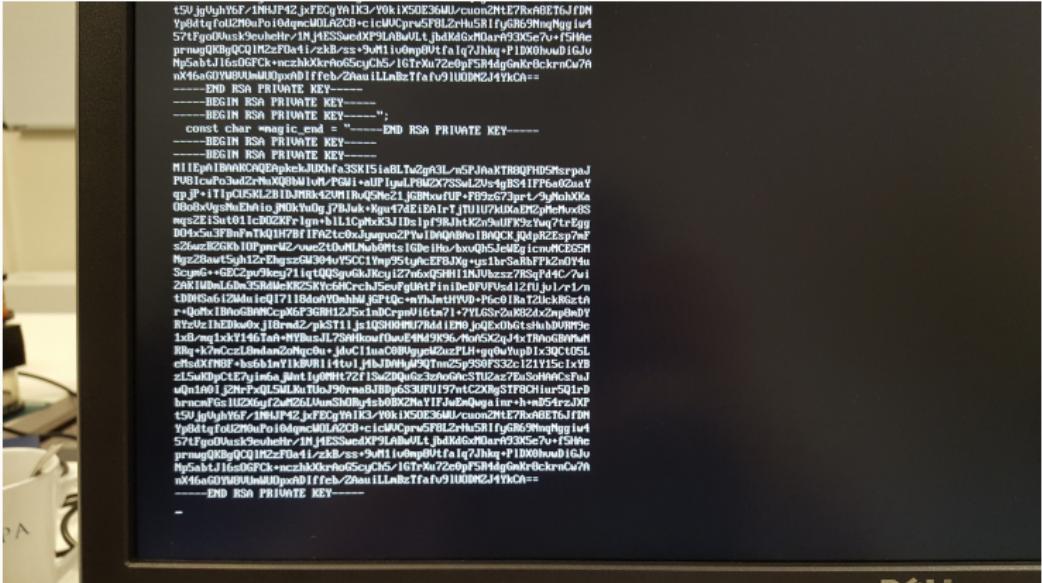


**Figure 6:** Searching the memory for the secret<sup>2</sup>.

---

<sup>2</sup>Using program *find\_key*. Download link will be provided later.

# Demo



**Figure 7:** The key was successfully found. There might be some bit flips in the result.

**Thank you!**  
**Any questions?**

## Summary

- Your memory contains lots of sensitive data
- Memory can stay intact when powered off
- Try to keep off-time short or cool memory
- Use USB, PXE or screwdriver to dump memory
- Errors are fixable

All slides and programs are available here:  
<https://github.com/jgraef/coldboot-attacks>



## Bibliography I

- [1] Halderman, J Alex and Schoen, Seth D and Heninger, Nadia and Clarkson, William and Paul, William and Calandrino, Joseph A and Feldman, Ariel J and Appelbaum, Jacob and Felten, Edward W *Lest we remember: cold-boot attacks on encryption keys*, Communications of the ACM, Vol. 52, 2009.