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?

NO

Memory contents

Memory contains sensible data:

- cryptographic keys
- e.g. key to encrypted hard drive
- passwords
- cookies
- other authentication tokens
- sensible 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

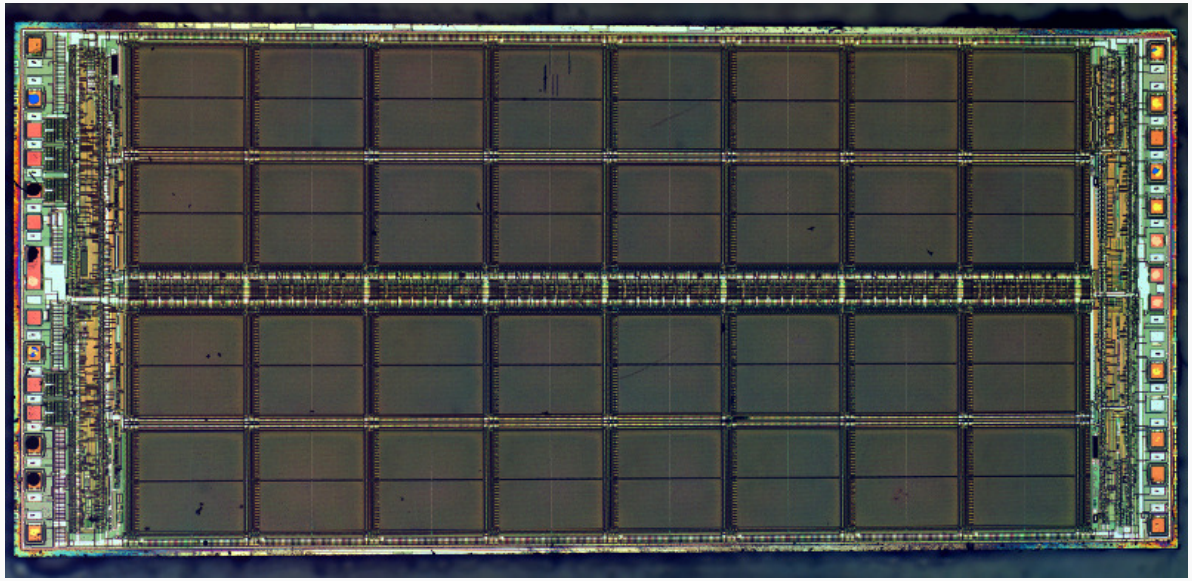
- *Cold Boot* $\rightarrow$ Boot after machine was powered off
  - Memory might lose contents
  - Always possible with physical access:
    Power switch, pull cable, remove battery
- *Warm Boot* $\rightarrow$ OS Reboot, Reset button
  - OS reboot cleans up secrets
  - Reset button not always available

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

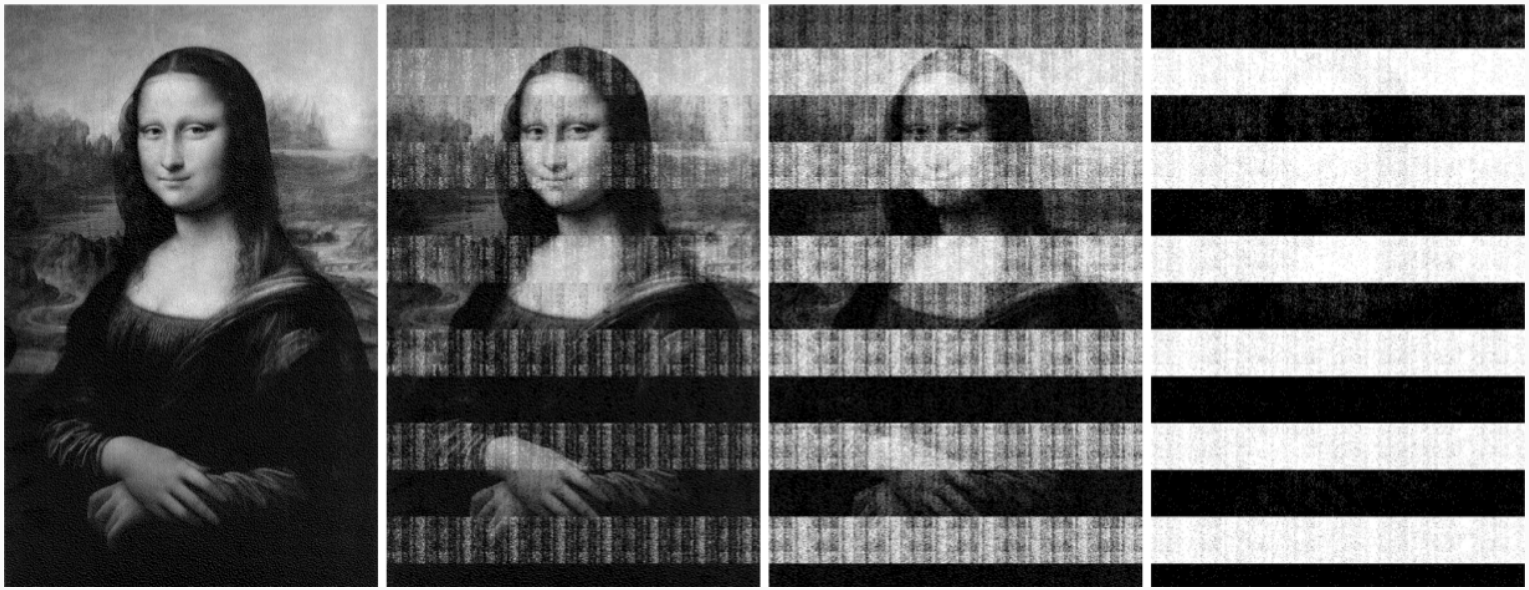


Figure 1: Image in memory without cooling after 5s, 30s, 60s, 5min[1]

Fixing memory corruption

- Errors are predictable
- Secrets' structure might help reconstruct
- AES: key schedule
- RSA, as shown by Coppersmith and others
- 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

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[1]
- Use hard disks with integrated encryption

[1] Power-On-Self-Test

Summary

- Your memory contains lots of sensible 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

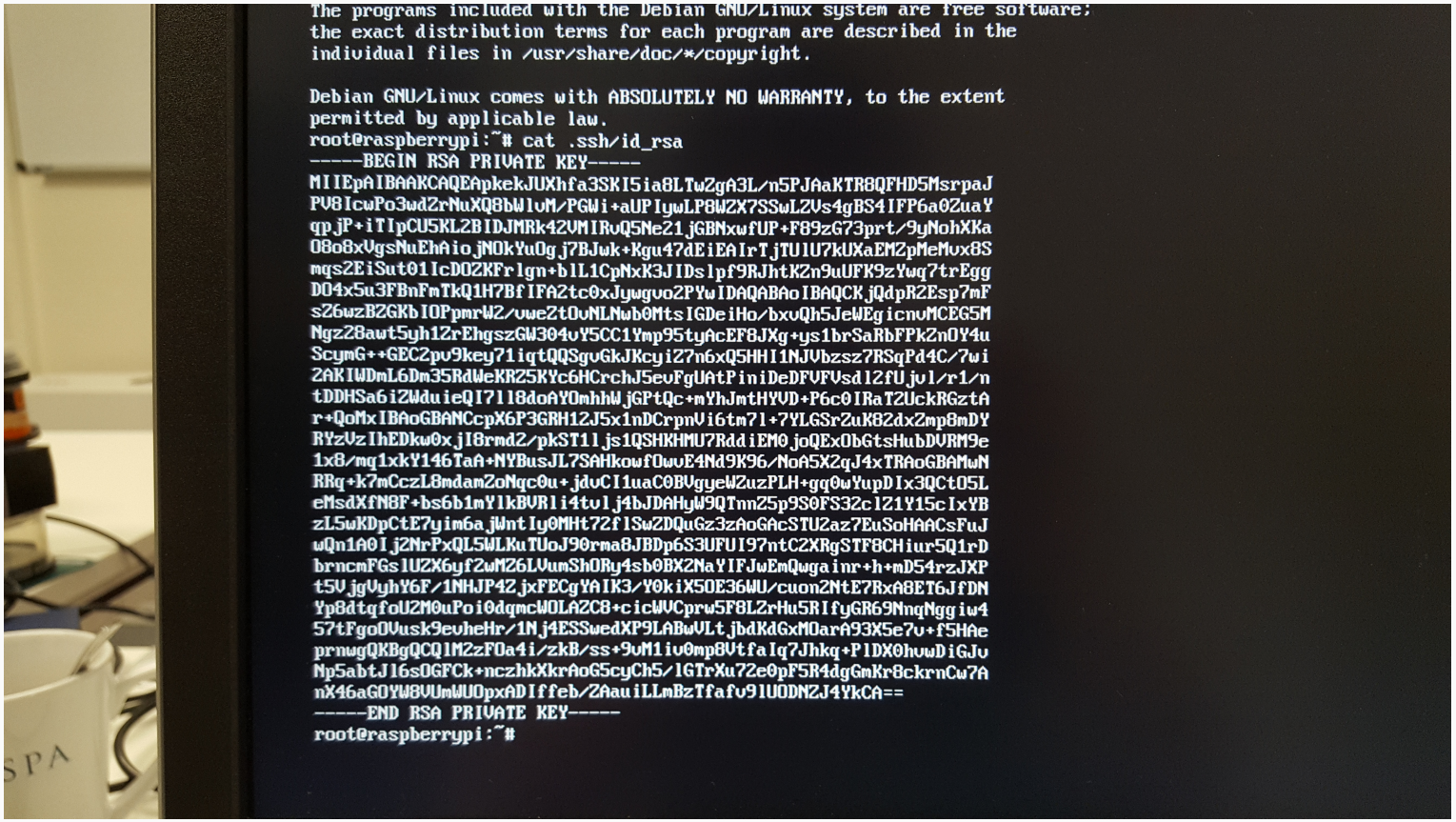


Figure 3: Loading secret into memory, by reading the file, its contents are loaded into the OS' file-system buffer.

Demo

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

Demo

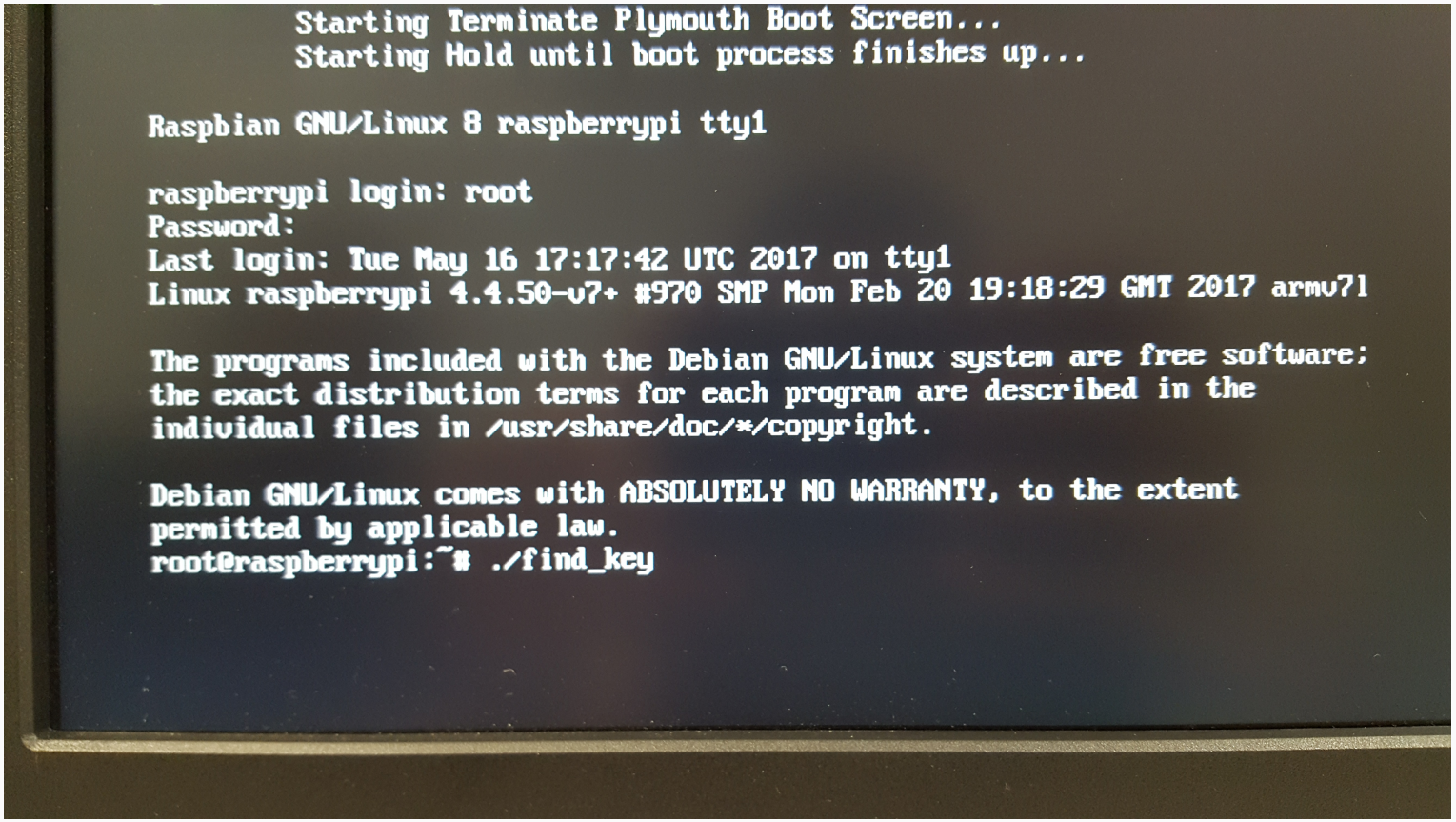


Figure 5: Searching the memory for the secret[2].

[2]Using program *find_key*. Download link will be provided later.

Demo

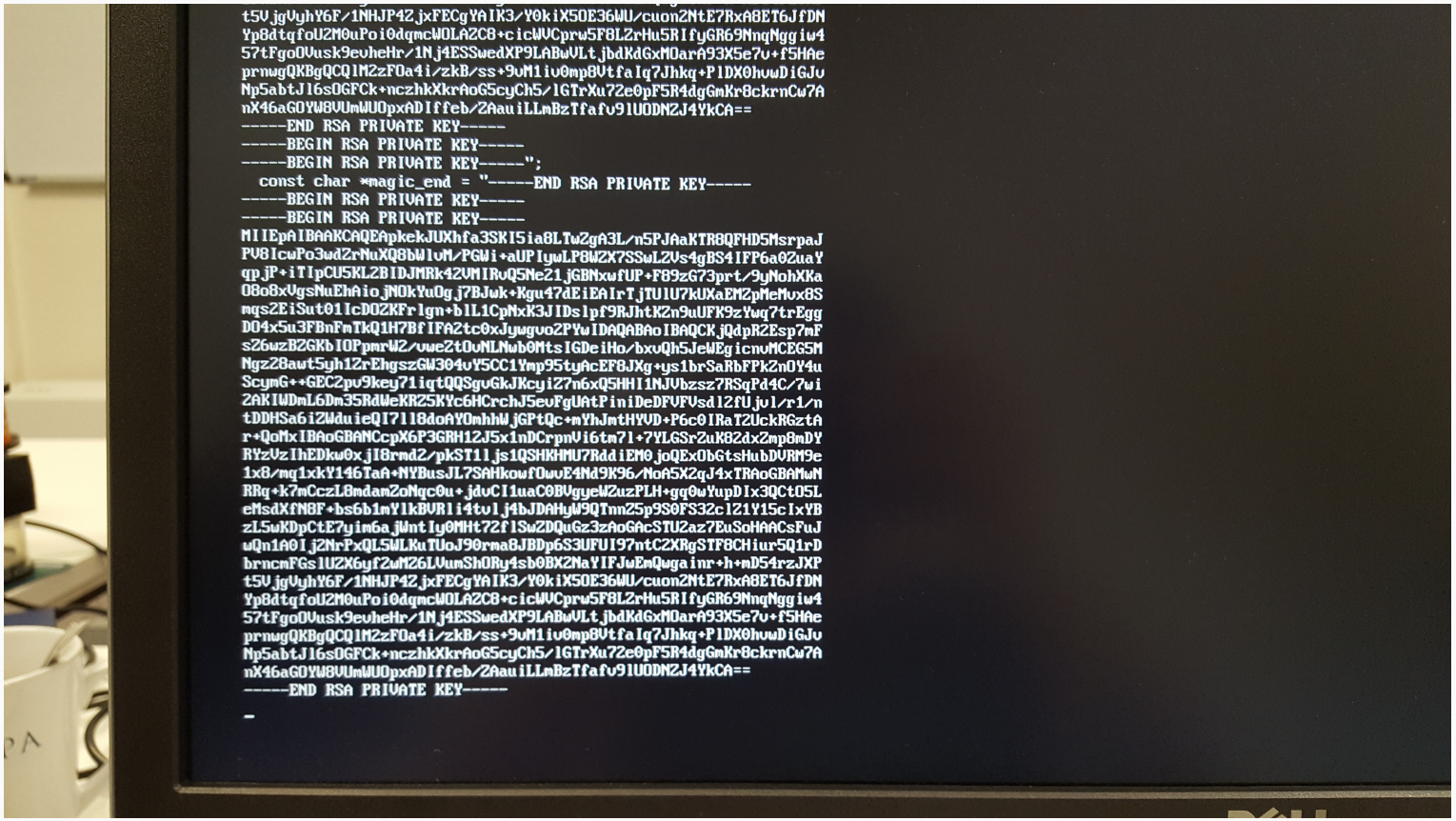


Figure 6: The key was successfully found. There might be some bit flips in the result.

Thank you!

Any questions?

Summary

- Your memory contains lots of sensible 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.