NTNU | Kunnskap for en bedre verden

SIDE-CHANNEL ATTACKS 4
- Real World Examples and Practicality

TTM4205 - Lecture 10

From theory to practice

REAL-WORLD EXAMPLES

What we have seen

- Timing / Power Analysis
  - Constant-time implementations
  - Masking
- **Will now** look at famous, real-world examples and countermeasures
  - Some attacks on TLS
  - Spectre and Meltdown

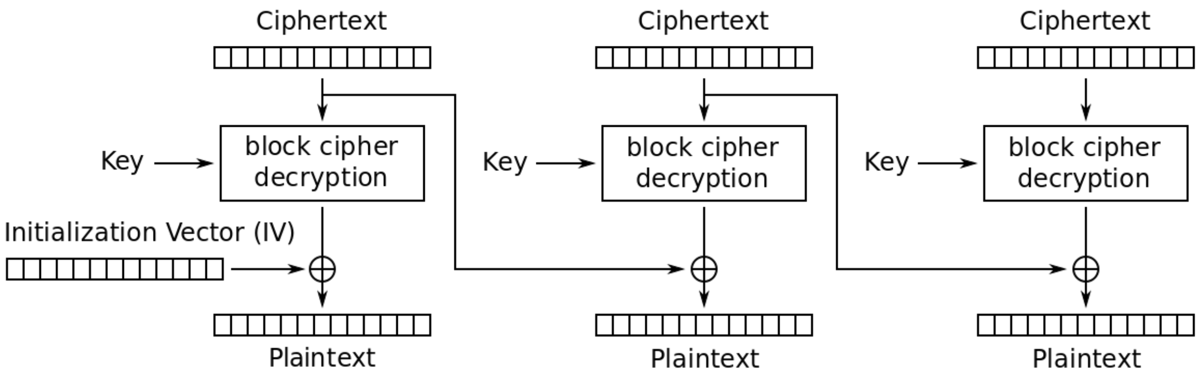
Side-Channel Attacks on TLS

- CBC-padding oracles:
  - Lucky Thirteen.
  - POODLE.

- Heartbleed.

CBC Padding Oracle

CBC mode decryption:



Cipher Block Chaining (CBC) mode decryption

PKCS#7

```
xx xx xx xx xx xx xx 01
xx xx xx xx xx xx 02 02
xx xx xx xx xx 03 03 03
xx xx xx xx 04 04 04 04
```

... etc

Oracle: returns whether padding was correct

Question: How to h4ck??

Lucky Thirteen (2013)

- CBC padding oracle attack published in 2002.
  - TLS mitigation: Don't return whether or not padding was correct.
- **Timing** became the new oracle.
  - Hard to mitigate - Lucky thirteen exploits this.
- **TLS 1.3 mitigation - Don't allow CBC**

Serge Vaudenay - Security Flaws Induced by CBC Padding

POODLE (2014)

- POODLE
  - Padding Oracle on Downgraded Legacy Encryption

- Was already mentioned in earlier lecture
  - Downgrades, then uses CBC padding oracle

SEE ALSO

- Bleichenbachers million message attack, exploiting padding oracles in RSA (1998)
    - (2018) ROBOT - Return Of Bleichenbacher's Oracle Threat

https://robotattack.org/

Heartbleed (2012)

- Vulnerability affecting OpenSSL.
- Vulnerability in the implementation of the "Heartbeat" protocol.
- Software bug that enabled **buffer over-read**
  - Reading from memory you should not be allowed.
- **Patch:** Make sure the attacker does not request more data than what makes sense.

Spectre and Meltdown (2018)

- Powerful, generic attack, affecting virtually all processors.
- **Mitigation: Swap out CPU unit.**
- "Band aids" slowed down the processing speeds by 5-30% (!)
    - Somewhat mitigates the effect, but the only "proper solution" was get a new processor.

https://www.cloudflare.com/learning/security/threats/meltdown-spectre/

Speculative Execution

- Like Heartbleed, can access and read data you are not meant too.
  - Unlike Heartbleed, not caused by a software bug.
- Relies on **speculative execution.**
- Earlier in the course: Compiler-optimisations may introduce side-channels
  - Speculative execution is the extreme version of this - processors will do operations before it is known whether it is needed.

Post-Quantum Crypto

- New Crypto => New side-channel attacks.
- Lots of work required
  - Finding theoretical attacks.
  - New implementations in e.g. TLS -> New attacks
- Worth thinking about as a project
  - Smaller project in this course?
  - Bigger master project?

How practical are...

FAULT INJECTIONS?

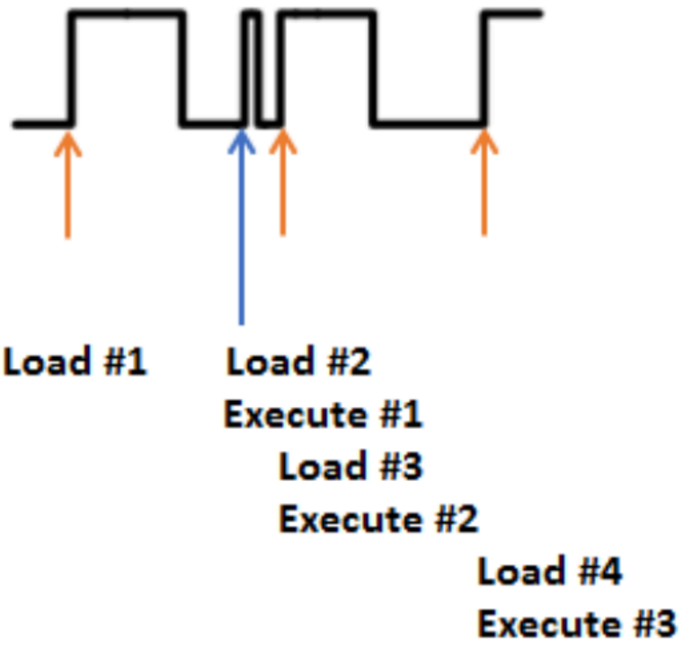
Overview

- We'll look at common fault injection methods, and some countermeasures

- Good resources (which most in this section is taken from):
  - Fault injection attacks on cryptographic devices
  - How Practical Are Fault Injection Attacks, Really?

Clock Glitching

- Part of lab exercises.
  - Skips instructions, based on irregular clocking.
- **Non-invasive**
- **Need control over chip's clock.**
- **$$: <2000 NOK**



Voltage Glitching

- Glitches by sudden burst or drop in voltage.
- **Non-invasive**
- **Inaccurate**
- **Need control over chip's power supply**
- **$$: Dirt cheap <500 NOK**

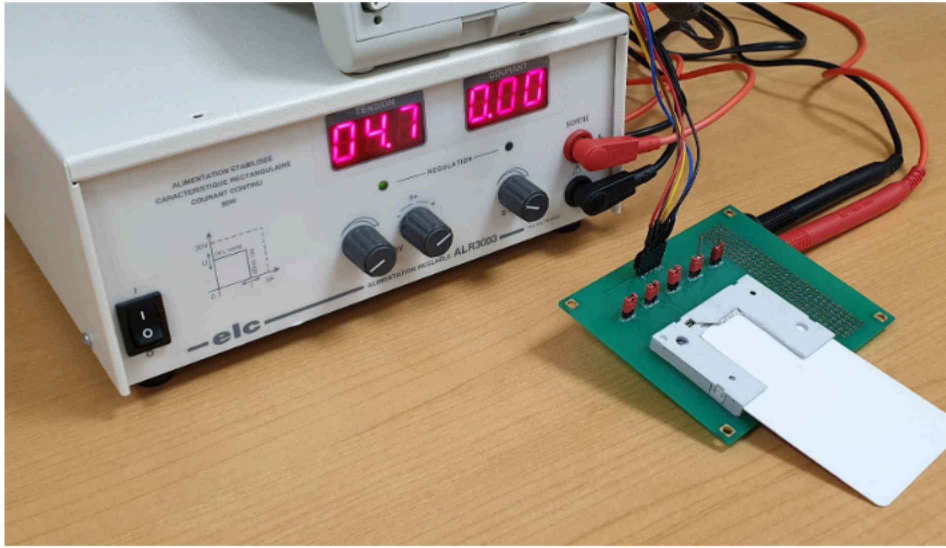
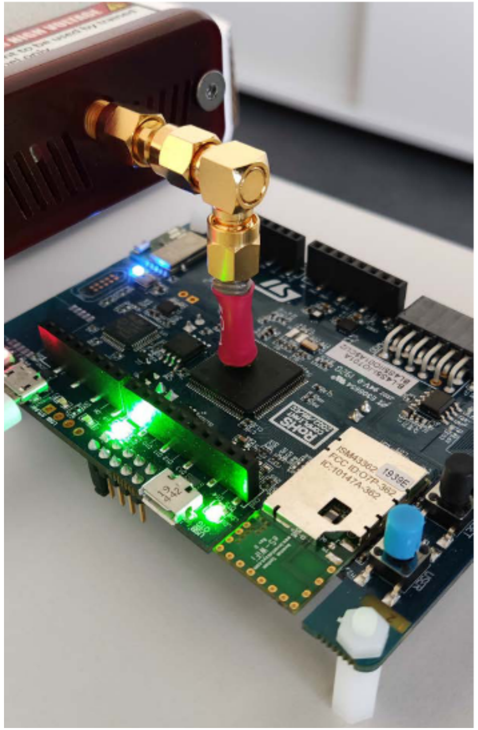


FIGURE 1. **An example of a voltage glitch on a smart card.**

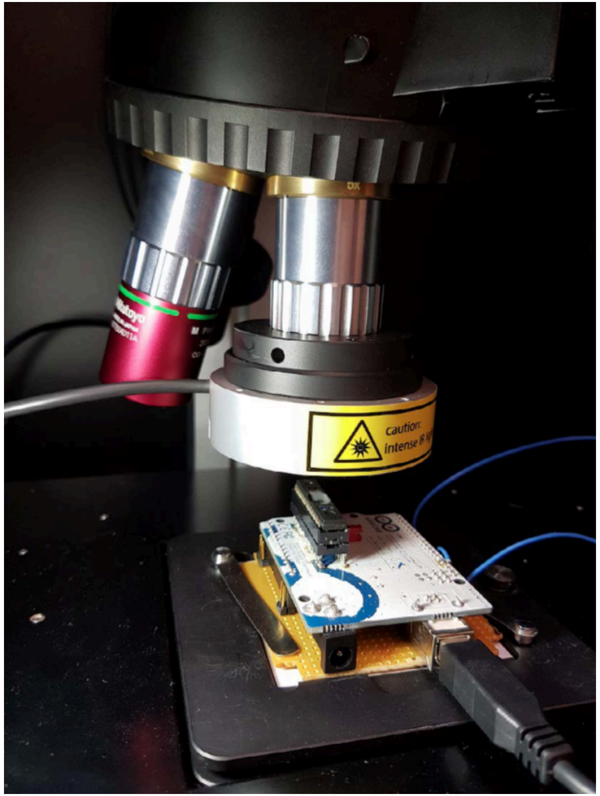
Electro-Magnetic Pulse

- Cause EM disturbance near device.
  - Focus more on bit flips/ resets and similar
- **Can be done from a "distance".**
- **Less reliable/accurate than lasers**
- **$$: 30.000 - 300.000 NOK**



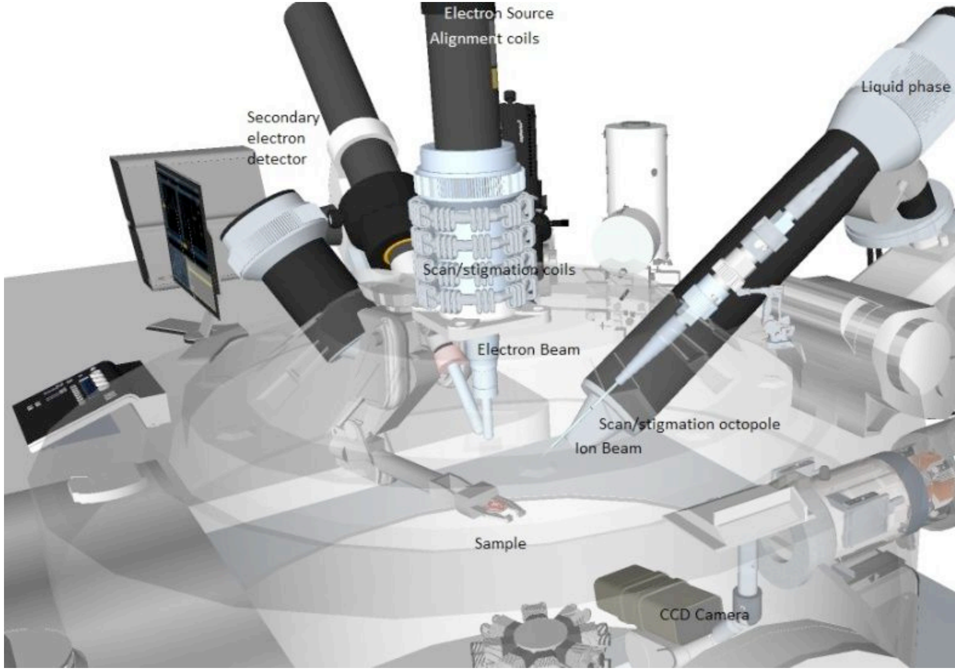
Shoot Lasers at it

- Shoot laser at the chip.
  - pew pew
- **Can target specific set of bits to flip.**
  - **Accuracy limit is he wavelength of the light being shot**
- **Semi-invasive.**
- **$$: ~500.000 NOK**



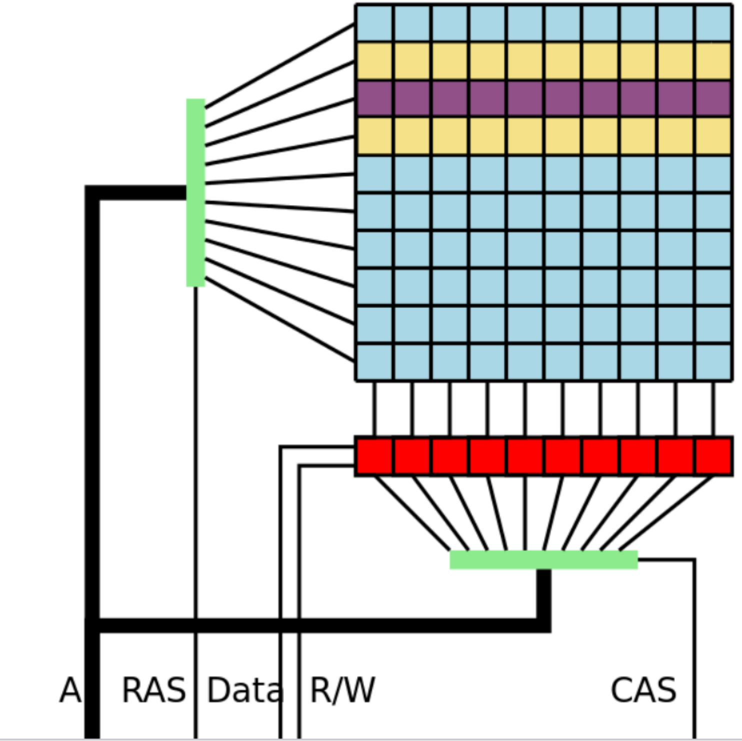
Shoot ~~Lasers~~ ions at it

- Shoot ionised particles instead of photons.
- **Probably the most accurate, powerful technique.**
- **Accuracy only limited by size of ion (i.e. an atom).**
- **$$: >10.000.000 NOK**



The Rowhammer attack

- DRAMs are so small that rapid changes in memory cells might affect neighbouring cells.
  - 2015: Actual exploit by Project Zero.
- **Can be done remotely**
- **Different "attack vector" than other techniques**
- **$$: Free**



Countermeasures

- **Any ideas?**

Countermeasures

- **Any ideas?**
- **Shielding:**
  - Make the chip physically inaccessible.

Countermeasures

- **Any ideas?**
- **Shielding:**
  - Make the chip physically inaccessible.
  - Overkill for most devices, but typical countermeasure for equipment used in e.g. military

Countermeasures

- **Any ideas?**
- **Sensors:**
  - Have sensors that notice tampering.
    - Glitching, Lasers, EMP etc...

Countermeasures

- **Any ideas?**
- **Error detection.**
  - Implement error detection in cryptographic operations.
  - E.g. compute things twice.
    - Based on assumption that injecting exactly the same fault twice is hard
    - Not necessarily true for lasers / ion beams.
  - Can also use error detecting codes.