UNIVERSITÄT BONN

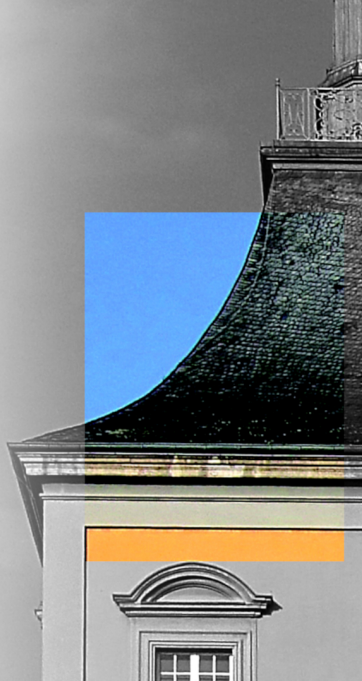
IT Security

Side Channels: Attacks and Defense

Dr. Jernej Tonejc

Bundesamt für Sicherheit in der Informationstechnik
Abteilung V - Verschlusssachensicherheit und Kryptographie

SCA | Universität Bonn | WS 2024/25
Gitversion: Unbekannt
Filename: ITSec-lecture-SCA



UNIVERSITÄT BONN

Lecture overview

- Definition of a side channel
- Types of side channels/attacks
- Countermeasures
- Examples
- Examples
- Examples

UNIVERSITÄT BONN

About Me

- PhD in Mathematics, USA
- Working with cryptography & IT-Security since 1998
- Cyber security @ Fraunhofer FKIE, 2014-2016
- At BSI[1] since 2016
  Information Assurance Technology and IT Management Division,
  Section KM 25 – IT Solution Systems for Classified I

[1] *Bundesamt für Sicherheit in der Informationstechnik/Federal office for information security*

UNIVERSITÄT BONN

BSI as an employer

Bundesamt für Sicherheit in der Informationstechnik

Personalgewinnung BSI

bewerbung@bsi.bund.de
Tel. +49 (0) 228 99 9582 6388
Bundesamt für Sicherheit in der Informationstechnik
Referat Z 8 – Personalgewinnung
Godesberger Allee 185-189
53175 Bonn

LinkedIn XING kununu

www.bsi.bund.de/karriere

www.bsi.bund.de/studierende

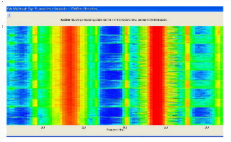
UNIVERSITÄT BONN

Outline

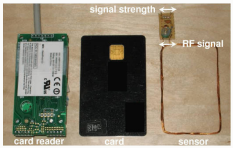
- What are Side Channels
- Attacks
- Countermeasures
- Turing Machine

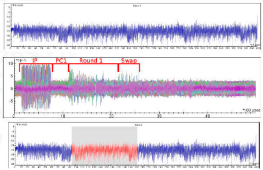
UNIVERSITÄT BONN

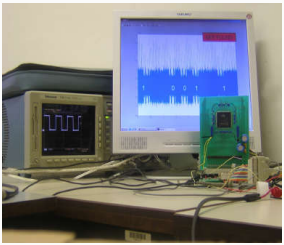
What are Side Channels



- Based on (non-intentional) physical information
- Can be inherent or induced
- Can enable new kinds of attacks







UNIVERSITÄT BONN

Side Channels vs. Covert Channels

Side channels ⇒ Interception/Wiretapping

The goal is to obtain the internal information about the system.
The attacker is often passive.

Covert channels ⇒ Communication

The goal is to exfiltrate the information.
They require an active attacker.

A side channel can be used as a building block for a covert channel.

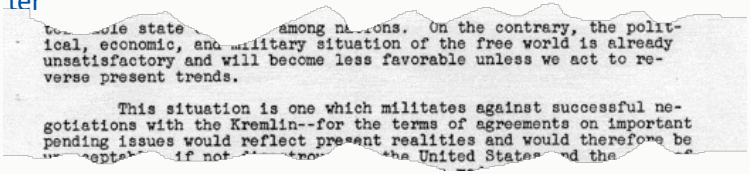
UNIVERSITÄT BONN

Types of Side Channels

- Timing (Kocher 1996)
- Power (KJJ 1999)
- Electromagnetic radiation (UCL &Gemplus 2001)
- Temperature (Naccache 2009)
- Light (Kuhn 2002)
- Sound (Shamir & Tromer 2004)
- Photonic emissions (TU Berlin 2012)

Some Unusual Side Channels

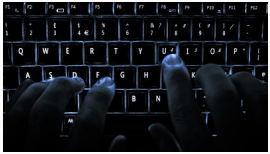
- Keyboard clicks can be distinguished by a cell phone's microphone [2]
- In former East Germany, a page with all possible characters was typed by each typewriter that was produced to trace them later



...ole state ... among na...ons. On the contrary, the political, economic, and military situation of the free world is already unsatisfactory and will become less favorable unless we act to reverse present trends.

This situation is one which militates against successful negotiations with the Kremlin--for the terms of agreements on important pending issues would reflect present realities and would therefore be ...eptab... if not ... ...tro... ...the United States ...nd the ...

- YOUR fingerprints



Source: Wikipedia

Source: Wikipedia

UNIVERSITÄT BONN

Types of Attacks

- Active vs. **passive**
  - Exploit abnormal behavior
  - Insertion of signals/glitches
  - Normal operation
  - Reading hidden signals
- Invasive vs. non-invasive
- Side-channel attacks are usually passive and non-invasive

UNIVERSITÄT BONN

Why it Works

Leakage is exploitable due to

- dependency on sequences of instructions executed
- dependency on data being processed
- other physical effects
- ability to work on one small part at a time

UNIVERSITÄT BONN

Levels of Analysis

- Simple: just one measurement
- Differential: multiple measurements, correlate
- Higher order: different samples
- Combining several side-channels
- Combining with theoretical cryptanalysis

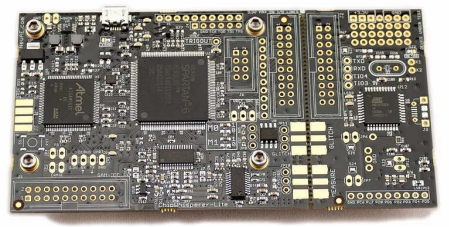
UNIVERSITÄT BONN

Tools

- Digital Storage Oscilloscope (DSO)
- EMF sensors and probes
- Focused Ion Beam machines
- ChipWhisperer
- …

ChipWhisperer Nano, ∼50 EUR

ChipWhisperer Lite, ∼250 EUR



UNIVERSITÄT BONN

Countermeasures

- TEMPEST[1]
  - NSA specification & NATO certification
  - Methods of shielding against spying
  - Zone model
  - Filtering
  - Specifics are classified

NATO SDIP-27 Level A,B,C

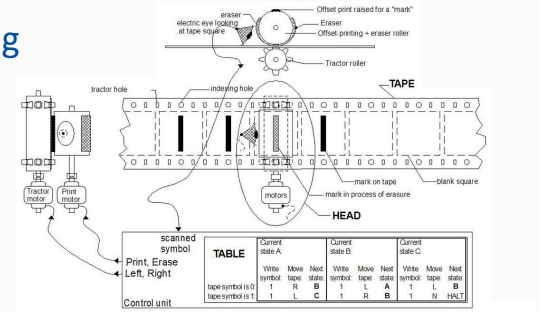
Zone 0, Zone 1, Zone 2, Zone 3

- Masking, hiding
- Time/execution randomization
- Noise generation

[1] Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions

Turing Machine

- A mathematical model of computing
  - A tape with cells
  - A head for reading & writing
  - A state register
  - Table of instructions
- In practice: need to read, write and move around



A fanciful mechanical Turing machine's TAPE and HEAD. The TABLE instructions might be on another "read only" tape, or perhaps on punch-cards. Usually a "finite state machine" is the model for the TABLE.

Source: Wikipedia CC BY-SA 3.0

Church-Turing thesis

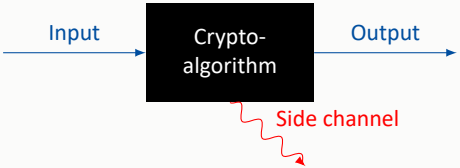
A function on natural numbers is computable by a human following an algorithm, if and only if it is computable by a Turing machine.

UNIVERSITÄT BONN

Outline

Side Channels on the Outside

- Treat the system as a closed box

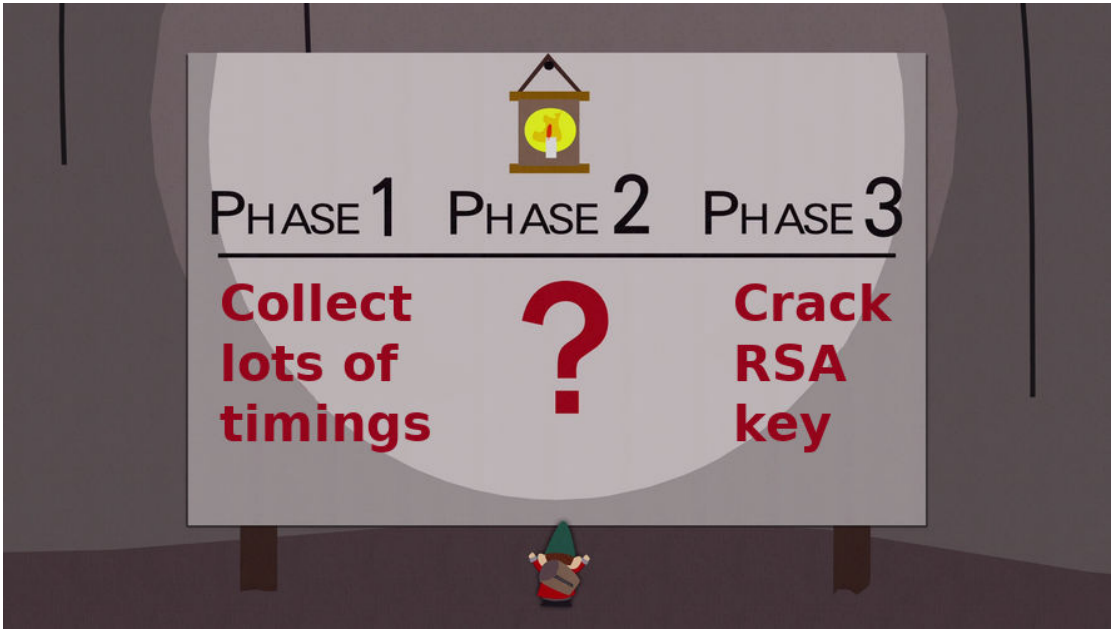


- We can observe:
  - Time
  - Power consumption
  - Radiation
  - . . .
- Passive attack

UNIVERSITÄT BONN

Measuring Timing Variations

- The duration depends on secret data
- Conditions:
  - Can correlate correct guesses with observed timings
  - Can work one bit/one byte at a time
- Averaging over several measurements to reduce the noise


PHASE 1
PHASE 2
PHASE 3
Collect lots of timings
?
Crack RSA key

RSA

- Public key (n, e), secret key (p, q, d)
- $n = p \cdot q$, $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$, n has $k+1$ bits
- To sign a message m, compute

$$m^d \bmod n,$$

using e.g. Square-and-Multiply (simplified):

Set $y \leftarrow 1, s \leftarrow m$
For bits $d_0, d_1, \ldots, d_k$ **of** d:
  If $d_i = 1$:
    $y \leftarrow y \cdot s \bmod n$
  $s \leftarrow s^2 \bmod n$
Return y

or

Set $y \leftarrow 1$
For bits $d_k, d_{k-1}, \ldots, d_0$ **of** d:
  $y \leftarrow y^2 \bmod n$
  If $d_i = 1$:
    $y \leftarrow y \cdot m \bmod n$
Return y

RSA

- Public key (n, e), secret key (p, q, d)
- $n = p \cdot q$, $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$, n has $k+1$ bits
- To sign a message m, compute

$$m^d \bmod n,$$

using e.g. Square-and-Multiply (simplified):

Set $y \leftarrow 1, s \leftarrow m$
For bits $d_0, d_1, \ldots, d_k$ **of** d:
  If $d_i = 1$:
    $y \leftarrow y \cdot s \bmod n$
  $s \leftarrow s^2 \bmod n$
Return y

or

Set $y \leftarrow 1$
For bits $d_k, d_{k-1}, \ldots, d_0$ **of** d:
  $y \leftarrow y^2 \bmod n$
  If $d_i = 1$:
    $y \leftarrow y \cdot m \bmod n$
Return y

Data-dependent execution!

UNIVERSITÄT BONN

Timing Attack

- Each signature takes time $T = e + \sum_{i=0}^{k} t_i$
- Guess the first b bits of d
- Predict the time given the guess and subtract from T
- Compute variance of the difference over all samples:
  - We obtain $\mathrm{Var}(e) + (k - b)\,\mathrm{Var}(t)$ for correct guess
  - We obtain $\mathrm{Var}(e) + (k + b - 2c)\,\mathrm{Var}(t)$ if only first $c < b$ bits correct
- Correct guesses decrease the variance
- Similar attacks on other public-key schemes

UNIVERSITÄT BONN

Square-and-Multiply (simplified)

- Execution-time independent implementation

Set $y \leftarrow 1$
For bits $d_k, d_{k-1}, \ldots, d_0$ **of** d:
    $y \leftarrow y^2 \bmod n$, $z \leftarrow y$
    If $d_i = 1$:
        $y \leftarrow y \cdot m \bmod n$
    Else:
        $z \leftarrow z \cdot m \bmod n$
Return y

- Is this safe?

Square-and-Multiply (simplified)

- Execution-time independent implementation

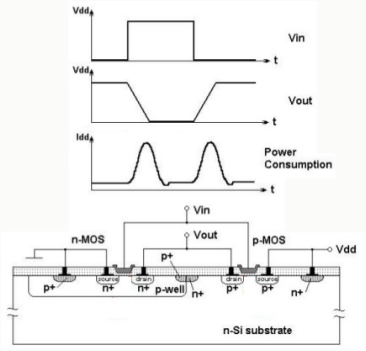
Set $y \leftarrow 1$
For bits $d_k, d_{k-1}, \ldots, d_0$ **of** d:
    $y \leftarrow y^2 \bmod n$, $z \leftarrow y$
    If $d_i = 1$:
        $y \leftarrow y \cdot m \bmod n$
    Else:
        $z \leftarrow z \cdot m \bmod n$
Return y

Caution:
Compiler optimization
may remove z!

- Is this safe? Seems to be...

Power Consumption of Circuits

- CMOS[1] circuits use current when switching
- More switching $\Rightarrow$ more current
- Operations correlate with current
- Measuring current reveals the operations



Source: S. Skorobogatov [7]

[1] Complementary Metal Oxide Semiconductor


Resistance is NOT futile

UNIVERSITÄT BONN

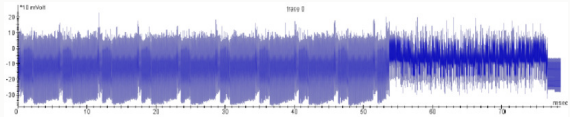
Types of Power Analysis

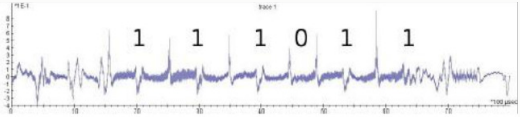
- Simple/Differential/Correlation Power Analysis (SPA/DPA/CPA)
- Template Attacks
- Stochastic Models
- Linear Regression Analysis
- Principal Component Analysis (PCA)
- . . .

UNIVERSITÄT BONN

Simple Power Analysis

- One or few measurements
- Search for repetitive patterns
- Data-independent but instruction-dependent
- See number of rounds, memory access, key



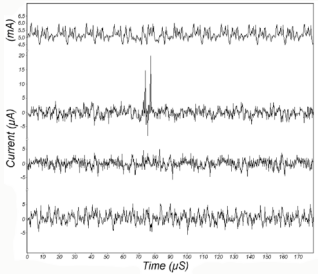


UNIVERSITÄT BONN

Differential Power Analysis

- Several thousand measurements
- Selection function: split the traces based on the predicted value of one cyphertext bit given the (sub)key guess
- Compare the difference of the averages of the two sets
- Correct (sub)key guess has higher difference

Try it yourself: https://dpacontest.telecom-paris.fr/home/

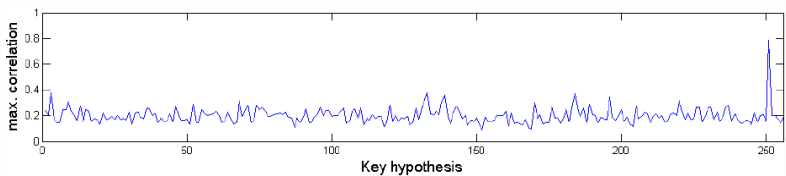


Source: [1]

UNIVERSITÄT BONN

Correlation Power Analysis

- Again several thousand measurements
- Model of the side channel vs. the real side channel
- Correlation based on key hypothesis
- Correct hypothesis has highest correlation



UNIVERSITÄT BONN

Padding Oracle Attacks

- CBC-mode[1] with PKCS7 padding:

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV \quad \text{(decryption)}$$

PKCS7-padding: last block has last n bytes equal to n

- Server reacts differently to different errors: bad padding vs. bad decryption
- First published in 2002 by Vaudenay
- Lucky Thirteen (2013), POODLE[2] (2014)

[1] Cipher-Block-Chaining

[2] Padding Oracle On Downgraded Legacy Encryption

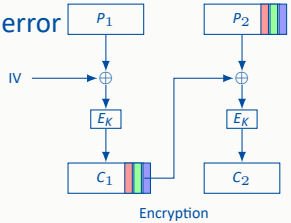
UNIVERSITÄT BONN

Example

- We encrypt two blocks, P_1, P_2, with 2 bytes of padding:

$$C_1 = E_K(P_1 \oplus IV), C_2 = E_K(P_2 \oplus C_1)$$

  where P_2 ends in `0x02,0x02`
- Modifying C_1 affects decryption of P_2: $P_2 = D_K(C_2) \oplus C_1$
- Change the last byte b_{-1} of C_1 as $b_{-1} \leftarrow b_{-1} \oplus z_{-1} \oplus 0x01$:
  - If the last byte of the original P_2 is z_{-1}, there is no padding error
  - Otherwise, there is a padding error
  - Try with all 256 possible values for z_{-1}
- Proceed by setting $b_{-1} \leftarrow b_{-1} \oplus z_{-1} \oplus 0x02$, $b_{-2} \leftarrow b_{-2} \oplus z_{-2} \oplus 0x02$ and guessing z_{-2}



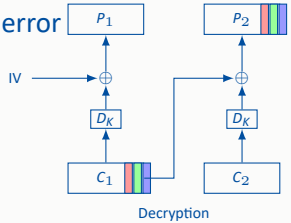
UNIVERSITÄT BONN

Example

- We encrypt two blocks, P_1, P_2, with 2 bytes of padding:

$$C_1 = E_K(P_1 \oplus IV), C_2 = E_K(P_2 \oplus C_1)$$

  where P_2 ends in `0x02,0x02`
- Modifying C_1 affects decryption of P_2: $P_2 = D_K(C_2) \oplus C_1$
- Change the last byte b_{-1} of C_1 as $b_{-1} \leftarrow b_{-1} \oplus z_{-1} \oplus 0x01$:
  - If the last byte of the original P_2 is z_{-1}, there is no padding error
  - Otherwise, there is a padding error
  - Try with all 256 possible values for z_{-1}
- Proceed by setting $b_{-1} \leftarrow b_{-1} \oplus z_{-1} \oplus 0x02$, $b_{-2} \leftarrow b_{-2} \oplus z_{-2} \oplus 0x02$ and guessing z_{-2}



UNIVERSITÄT BONN

Outline

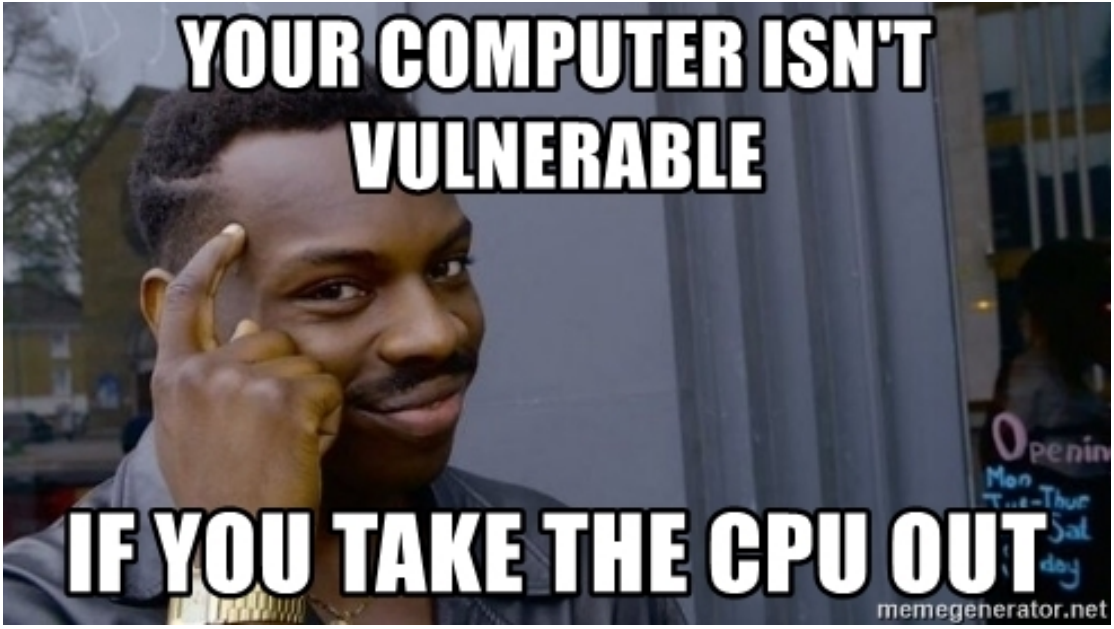
Introduction

Outside the box

Inside the box

- Rowhammer
- Flush and Reload
- Spectre and Meltdown

Watch and Listen Carefully


YOUR COMPUTER ISN'T VULNERABLE
IF YOU TAKE THE CPU OUT
memegenerator.net

UNIVERSITÄT BONN

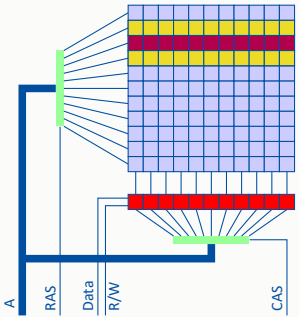
Actively Creating Side Channels

- Sometimes the channels are not there
- By manipulating the system, we create them
- We use the knowledge of
  - hardware
  - algorithm
  - implementation

UNIVERSITÄT BONN

Rowhammer

- Cells in DRAM need periodic refresh
- When reading, the original content is destroyed and must be copied back
- Due to high density,
  rapid access causes side effects:
  - Bits in adjacent rows can flip
  - Depends on the module
  - Unpredictable, but repeatable



UNIVERSITÄT BONN

How Flipping a Bit Helps

- Flipping the superuser or NX-bit in a pagetable:
  - Access to kernel pages from userspace
  - Memory pages can be made executable
  - Remove write protection
- Flipping a bit in ssh public key:
  - In .ssh/authorized_keys
  - New modulus can likely be factored
  - Compute the new private key and log in

UNIVERSITÄT BONN

How Flipping a Bit Helps

- Flipping the superuser or NX-bit in a pagetable:
  - Access to kernel pages from userspace
  - Memory pages can be made executable
  - Remove write protection
- Flipping a bit in ssh public key:
  - In .ssh/authorized_keys
  - New modulus can likely be factored
  - Compute the new private key and log in

All in RAM!

UNIVERSITÄT BONN

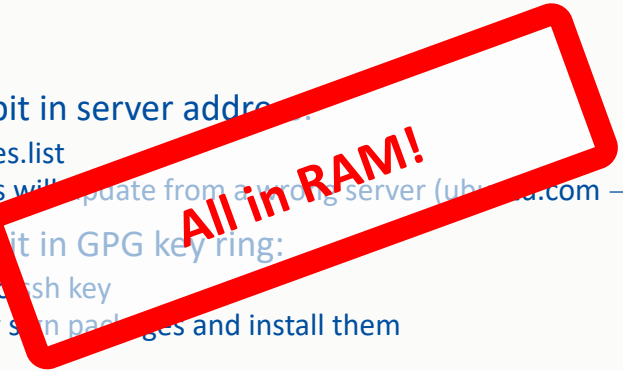
How Flipping a Bit Helps

- Flipping a bit in server address:
  - In sources.list
  - Packages will update from a wrong server (ubuntu.com $\rightarrow$ ufuntu.com)
- Flipping a bit in GPG key ring:
  - Similar to ssh key
  - Can now sign packages and install them

UNIVERSITÄT BONN

How Flipping a Bit Helps

- Flipping a bit in server addr[illegible]:
  - In sources.list
  - Packages will update from a wrong server (ubuntu.com → ufuntu.com)
- Flipping a bit in GPG key ring:
  - Similar to ssh key
  - Can now spoof packages and install them



UNIVERSITÄT BONN

Caching in Modern Computers

- Several types of memory:
  - In CPU (registers)
  - In CPU (cache)
  - RAM
  - Flash drives
  - Hard drives
  - Tapes/DVDs (backup)
- Access times vary greatly
- Speed increases the closer the data is to CPU

UNIVERSITÄT BONN

Caching in Modern Computers

- Several types of memory:
  - In CPU (registers)
  - In CPU (cache)
  - RAM

  Fast & Volatile

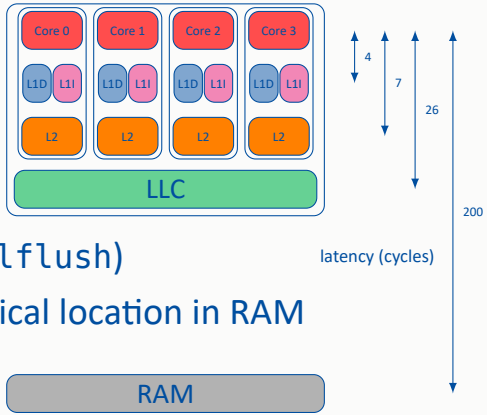
  - Flash drives
  - Hard drives
  - Tapes/DVDs (backup)

  Slow & Non-volatile
- Access times vary greatly
- Speed increases the closer the data is to CPU

UNIVERSITÄT BONN

Intel Cache Architecture

- Several levels: L0, L1, L2, LLC[1]
- Several types: TLB, LFB, BPU, BTB[2] …
- LLC is shared across cores
- Can flush (evict) LLC from userspace (`clflush`)
- Location in cache is related to the physical location in RAM

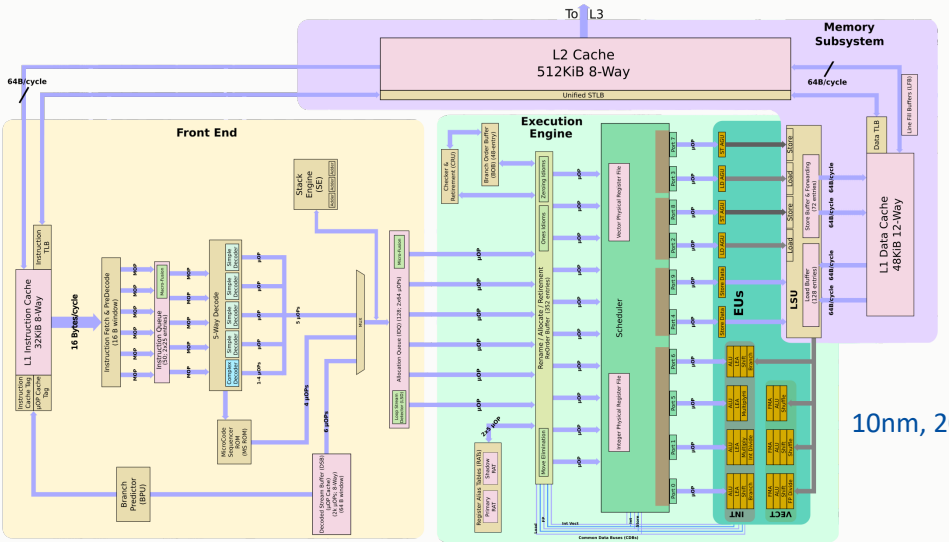


[1] Last-Level-Cache

[2] Translation Lookaside Buffer, Line Fill Buffer, Branch Prediction Unit, Branch Target Buffer

UNIVERSITÄT BONN

Intel Sunny Cove Block Diagram



UNIVERSITÄT BONN

Cache Timing Side Channel

- Computation speed depends on the location of the data
- In cache: fast. Not in cache: slow
- Two common techniques of measuring:
  - Flush+Reload: Evict relevant data and check for reload, or
  - Prime&Probe: Check if own data got evicted due to cache collision

UNIVERSITÄT BONN

Attacking with Flush+Reload

- Assumption: data-dependent code lies in different cache lines
- Focus on the library code
- Flush, wait and reload
- Shorter time indicates the victim loaded it already
- This is our side channel!

Flush+Reload attack on RSA

- Assume the If and Else branches lie in different cache lines:

Set $y \leftarrow 1$
For bits $d_k, d_{k-1} 1, \ldots, d_0$ **of** d:
    $y \leftarrow y^2 \bmod n, z \leftarrow y$
    If $d_i = 1$:
        $y \leftarrow y \cdot m \bmod n$
    Else:
        $z \leftarrow z \cdot m \bmod n$
Return y

Alignment determined by compiler and location in memory

- Depending on the bit value d_i, different cache lines get used

UNIVERSITÄT BONN

Speculative Execution

- Modern CPUs are superscalar: several execution units, long pipelines
- Conditional branches present an issue:
  branch target is unclear before the condition gets resolved
  - To increase speed, processor chooses the most likely branch instead of waiting
  - Correct choice speeds up the computation
  - Wrong choice causes a roll-back, but no loss otherwise: the processor would have to wait for the correct target anyway
- Similar problem with permissions check
- Problem: roll-back leaves cache polluted

UNIVERSITÄT BONN

A Library Example: Setup

- One central library
- Requests can also be made through the department's secretary
- The books arrive at the secretary's office the next day
- The secretary validates the request before giving out the book
- The books can be returned directly or to the secretary
- If a book is already at the secretary, no request is made to the library

UNIVERSITÄT BONN

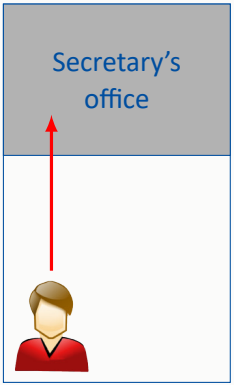
A Library Example: Goal

- We want to find out the grade of the student John Doe
- Grades are integers between 1 and 5
- The secretary has access to all the grades
- The secretary will only give out the requester's grade
- We get no answer if we ask directly

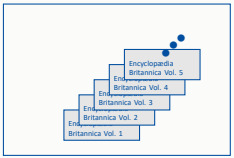
UNIVERSITÄT BONN

A Library Example: Attack

IT Department



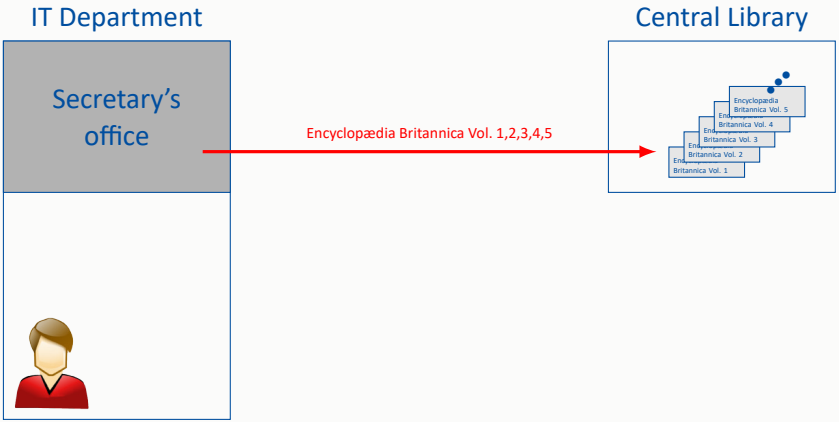
Central Library



1. "I want *Encyclopædia Britannica Vol. 1, 2, 3, 4, 5*"

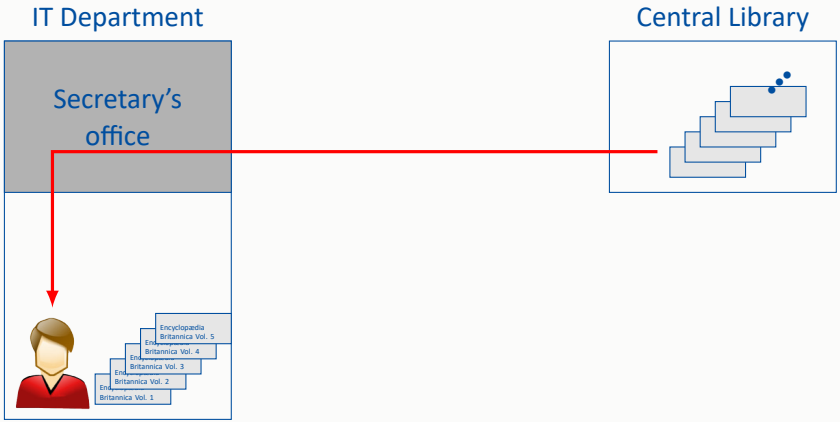
Day 1

A Library Example: Attack



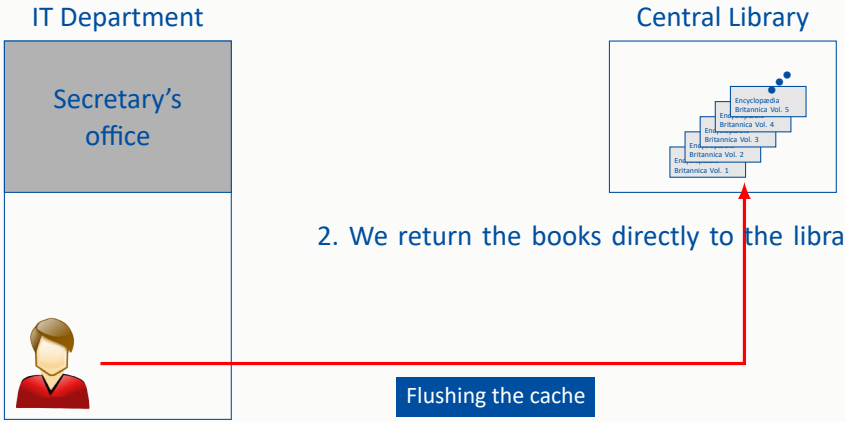
Day 1

A Library Example: Attack



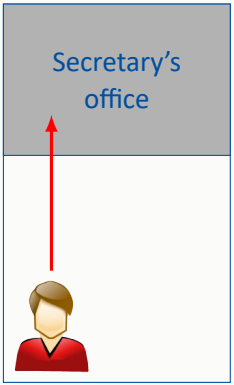
Day 2

A Library Example: Attack

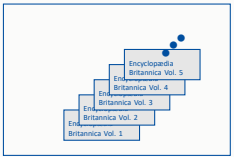


A Library Example: Attack

IT Department



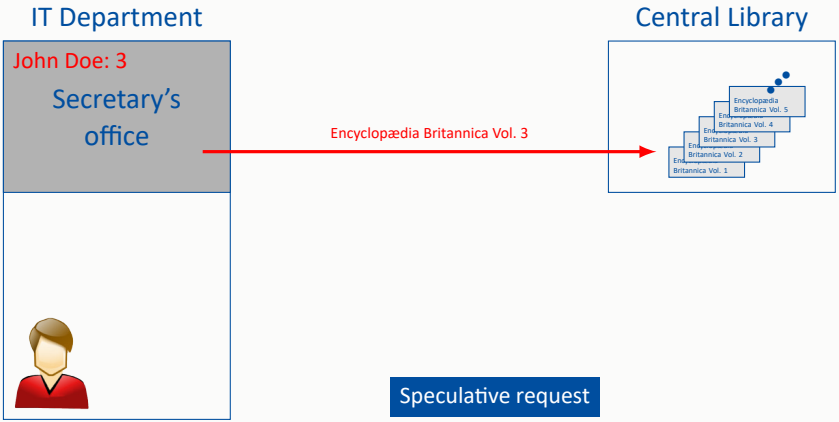
Central Library



3. "I want *Encyclopædia Britannica Vol. X, where X is John Doe's grade*"

Day 2

A Library Example: Attack

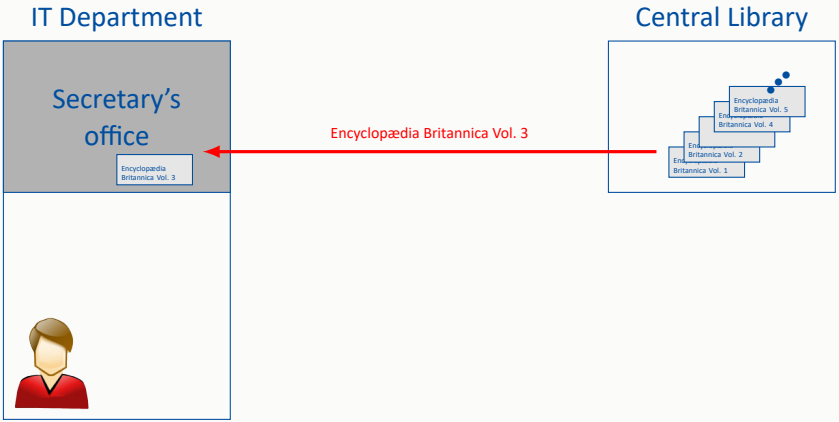


Speculative request

Day 2

UNIVERSITÄT BONN

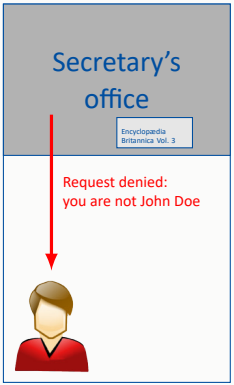
A Library Example: Attack



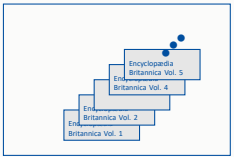
Day 3

A Library Example: Attack

IT Department



Central Library

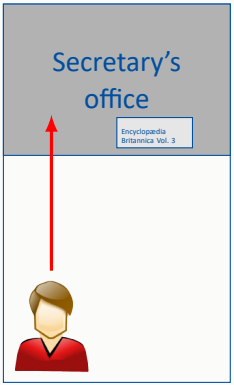


Permission check

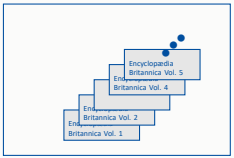
Day 3

A Library Example: Attack

IT Department



Central Library

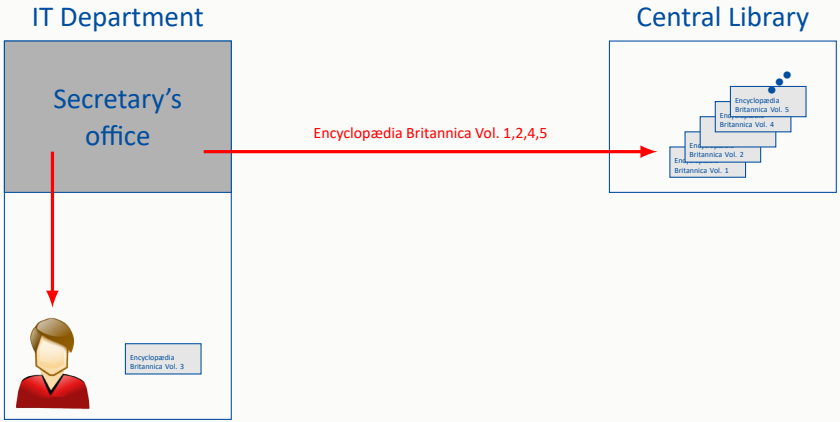


4. "I want *Encyclopædia Britannica Vol. 1, 2, 3, 4, 5*"

Reload

Day 3

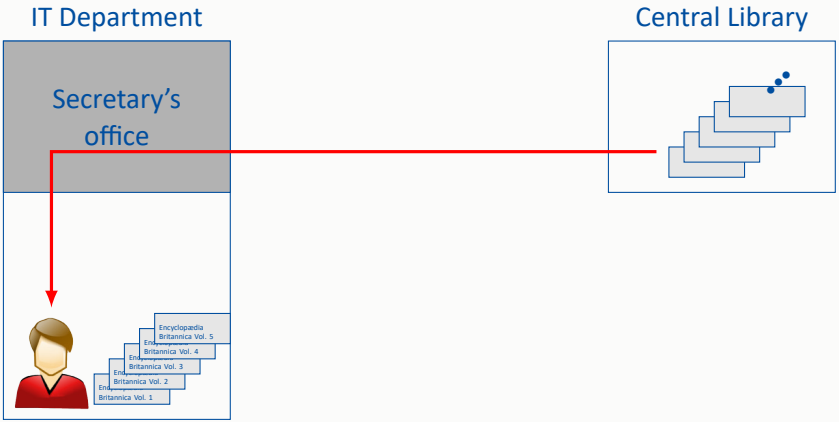
A Library Example: Attack



Day 3

UNIVERSITÄT BONN

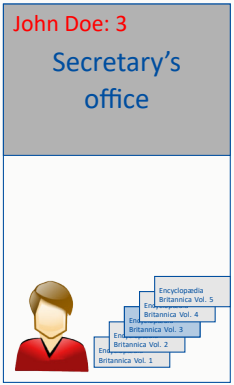
A Library Example: Attack



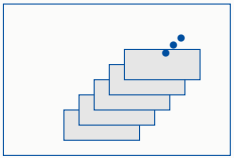
Day 4

A Library Example: Attack

IT Department



Central Library



The book that arrived first indicates the most likely grade

UNIVERSITÄT BONN

Outline

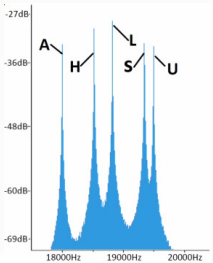
UNIVERSITÄT BONN

Exfiltrating Data, Linking Devices

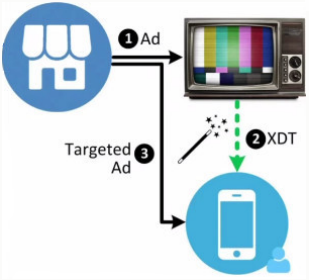
- Main goal of these attacks is getting data out
- Use of unexpected communication channels
- Mostly uses standard equipment

UNIVERSITÄT BONN

Cross-Device Tracking



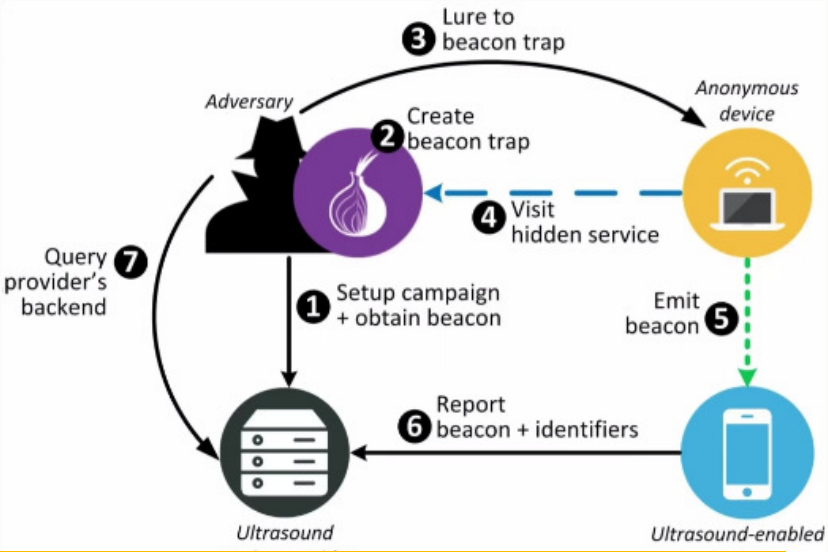
- SilverPush founded in 2012
- Embed inaudible sound in TV ads (ultrasound beacons)
- Apps on phones pick this up
  $\Rightarrow$ Cross-device user tracking
- Privacy issues voiced in 2015



Source: Talk at 33C3 [5]

UNIVERSITÄT BONN

Deanonymizing Tor Users



UNIVERSITÄT BONN

Escaping the Air-Gapped Machines

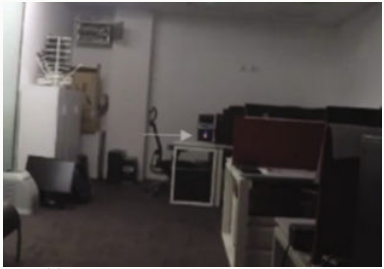
- Air-gapped: no direct connection to the world
- Need to bridge the gap to leak the data
- Infiltration doable[1], exfiltration a challenge
- Is it enough to see the machine?

[1] E.g., an infected USB-Stick

UNIVERSITÄT BONN

Blinking HD-LED

- Disk activity makes LED blink:
  - Duration corresponds to amount read
  - E.g. $<$4kB$\sim$0.18 ms, 5MB$\sim$32ms
- Low-privilege process can read data
- Simple camera can record 60 frames/sec
- Bitrates from 60 – 4000 bits/sec[2]
- Need to control the noise



Source: [6]

[2] with photodiode

UNIVERSITÄT BONN

(Un)expected Sources of Signals

- Data lanes within PC emit EMR[3]
- Need to find useful frequencies
- Example 1: DDR-RAM
- Example 2: Videocards

[3] Electromagnetic radiation

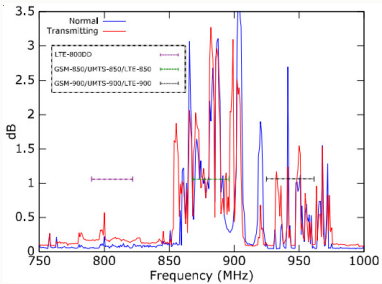
UNIVERSITÄT BONN

RAM Radio

- DDR-RAM
- LTE uses 800MHz carrier frequency
- Modified phone firmware[4] can decode signals
- Use MOVNTDQ[5] for RAM access
- Bitrates 2-100 bits/s

Standard Name	I/O bus clock (f_c)	EMR Range
DDR3-1600	800MHz	600MHz-1100MHz
DDR3-1866	933MHz	750MHz-1150MHz
DDR4-2133	1066MHz	750MHz-943MHz (fragmented) 1.04GHz-1.066GHz

Source: [8]



[4] Using e.g. OsmocomBB

[5] Move Double Quadword Non-Temporal; avoids cache

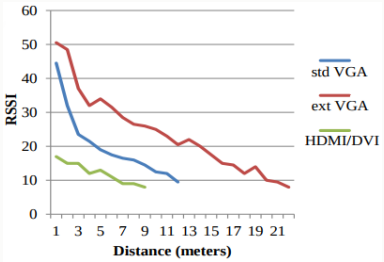
AirHopper

- Video cables cary signals

$$(H_{pixel} + H_{sync}) * (V_{pixel} + V_{sync}) * RR = PC^{6}$$

E.g. for 1440x900 we get 106.5 MHz

- Control signals even when monitor off
- Smartphones have FM receivers
- Patch code to ignore headphones
- Use modulation (A-FSK or DTMF[7])
- Effective range $\sim$7m, 80 bits/s



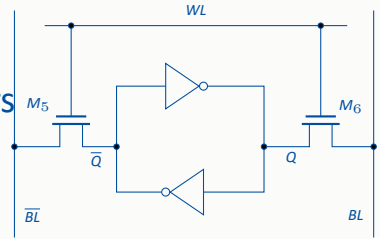
Source: [9]

[6] Utility like cvt can be used to compute the pixel clock (PC)

[7] Audio Frequency-Shift Keying, Dual-Tone Multiple Frequency

Photonic Emission Analysis

- Microprocessors are built out of lots of transistors
- Low-power embedded devices at μm scale
- Internal memory uses SRAM cells
  - Cell consists of 6 MOSFETs[8]
  - 4 are within two cross-coupled inverters
  - Access through *WL*, value in *BL*, $\overline{BL}$

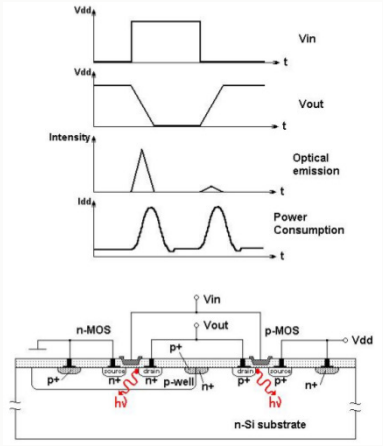


[8] Metal-Oxide-Semiconductor Field Effect Transistor

UNIVERSITÄT BONN

Transistor Operation

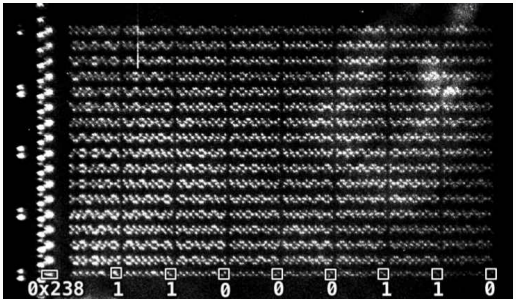
- Hot-carrier luminescence:
  Transistors emit photons when switching
- Can detect SRAM memory access
- How?
  - Picosecond imaging circuit analysis (PICA, expensive, 1,000,000+ EUR!)
  - Optical microscope + CCD (cheaper)
  - Issue: temporal vs. spatial resolution



Source: S. Skorobogatov [7]

UNIVERSITÄT BONN

Practical Example



From: J. Krämer, PhD Thesis "Why Cryptography Should Not Rely on Physical Attack Complexity"

Optical emission of AES S-Box, stored in SRAM of ATMega328P. 256 Bytes are stored in 32 cells of 8 bytes each. The emissions of the row drivers (left) are clearly visible.

Summary


SIDECHANNELS
SIDECHANNELS EVERYWHERE
LIGHTYEAR
imgflip.com

UNIVERSITÄT BONN

Summary

- What is a side channel
- What types of side channels exist
- Countermeasures
- Lots of examples

Take-away

Secure software development is not enough.

UNIVERSITÄT BONN

Lightning Survey

UNIVERSITÄT BONN

References

1 P. Kocher et al. Differential Power Analysis.
2 S. Yang. Researchers recover typed text using audio recording of keystrokes. http://www.berkeley.edu/news/media/releases/2005/09/14_key.shtml
3 B. Gras et al. Memory Deduplication: The Curse that Keeps on Giving. 33C3
4 Y. Yarom. FLUSH+RELOAD: a High Resolution, Low Noise, L3 Cache Side-Channel Attack.
5 V. Mavroudis, F. Maggi. Talking Behind Your Back. 33C3.
6 M. Guri et al. LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED, DIMVA 2017.
7 S. Skorobogatov. Using Optical Emission Analysis for Estimating Contribution to Power Analysis.
8 M. Guri et al. GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies. USENIX 2015.
9 M. Guri et al. AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies. MALCON 2014.
10 M. Lipp et al. Meltdown. ArXiV e-print 1801.01207
11 P. Kocher et al. Spectre Attacks: Exploiting Speculative Execution. ArXiV e-print 1801.01203
12 B. Nassi et al. Video-Based Cryptanalysis: Extracting Cryptographic Keys from Video Footage of a Device's Power LED. IACR e-print 2023.923.