Side-channel attacks

Daniel Bosk

Department of Information Systems and Technology
Mid Sweden University, Sundsvall.

6th April 2020

1. Introduction
   - What are side-channels?
2. Timing attacks
   - Doing arithmetic
   - Typing pattern and guessing passwords
   - Summary
3. Emission attacks
   - Emissions from electronic systems
   - Exploiting acoustic emissions
   - Exploiting voltage
   - Exploiting electromagnetic emissions
4. Summary

What are side-channels?

Definition (Side Channel)

- Unintended channel emitting information.
- Due to physical implementation flaws and not theoretical weaknesses or forcing attempts.

What are side-channels?

- There are various categories, *e.g.*,
  - timing attacks,
  - acoustic attacks,
  - electromagnetic attacks,
  - . . .

1 Introduction
- What are side-channels?

2 Timing attacks
- Doing arithmetic
- Typing pattern and guessing passwords
- Summary

3 Emission attacks
- Emissions from electronic systems
- Exploiting acoustic emissions
- Exploiting voltage
- Exploiting electromagnetic emissions

4 Summary

Example

- Use the standard algorithms for addition and multiplication (using the binary number system).
- Give any number to an algorithm A.
- A will multiply your number by a secret value x.
- Can you tell the difference between $x = 3$ or $x = 7$?

Doing arithmetic

- Assume that we give the number 25 as our challenge to A.
- Looking at the numbers we have we see that $3_{10} = 11_2$, $7_{10} = 111_2$ and $25_{10} = 11001_2$
- Assume each step in the algorithm takes one time unit.
- Then 11001×11 will take 17 time units:
    - 5 time units for multiplying the last 1 in 11 with each digit in 11001,
    - another 5 time units for the next digit in 11,
    - we have an additional 1 time unit for shifting the second result one step,
    - finally, we get 6 time units for adding the numbers.
- 11001×111 will take 24 time units:
    - 5 time units for each digit, hence 15 in total,
    - we have two shifts, thus 2 time units more,
    - finally we have 7 time units for adding.

Note

- The first multiplication takes 17 time units to perform, the second takes 24 time units.
- This is one example of why *constant-time operations* are desirable.

Exercise

- Can we see the difference between $x = 2_{10} = 10_2$ and $x = 3_{10} = 11_2$?

Note

- The first multiplication takes 17 time units to perform, the second takes 24 time units.
- This is one example of why *constant-time operations* are desirable.

Exercise

- Can we see the difference between $x = 2_{10} = 10_2$ and $x = 3_{10} = 11_2$?

Example (SSH password guessing)

- Song, Wagner and Tian [SWT01] showed a timing attack on passwords sent over encrypted SSH sessions.
- As each keystroke in the password is sent in a separate package, the attacker can observe the delay between keystrokes.
- They found that this gave a factor 50 advantage for guessing the password.

Note

- Analytics scripts on many websites send key-presses to the server as you type.
- That's exactly the same situation.

Summary

- We can measure the time for different operations.
- Depending on the operations and times they take, we can figure out something about the operands.

1. Introduction
   - What are side-channels?
2. Timing attacks
   - Doing arithmetic
   - Typing pattern and guessing passwords
   - Summary
3. Emission attacks
   - Emissions from electronic systems
   - Exploiting acoustic emissions
   - Exploiting voltage
   - Exploiting electromagnetic emissions
4. Summary

Emissions from electronic systems

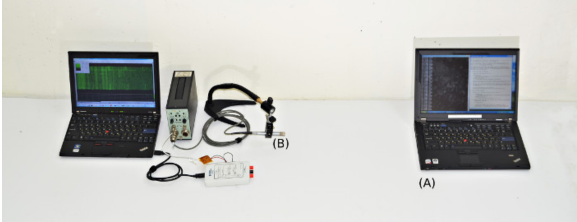
- Electronic systems emit signals just by running.
- Remember induction and similar properties from physics class.
- *E.g.*, electromagnetic emissions or acoustic emissions from vibrations.

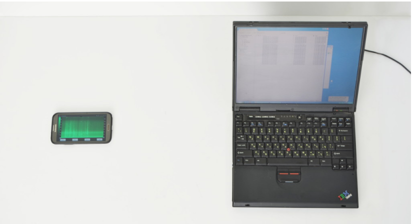
Exploiting acoustic emissions

- Some authors[1] showed an attack to extract a 4096-bit RSA private key from a laptop PC (GnuPG implementation of RSA).
- Computers emit high-pitched noise during operation due to vibrations in some of their electronic components.
- This was used to derive the key used for decryption of some chosen ciphertexts within an hour!
- Their results show that this attack can be accomplished by placing a mobile phone (microphone) next to the target laptop.

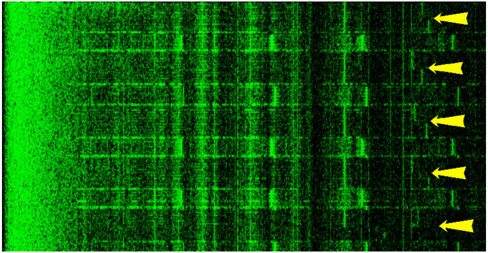
[1] Daniel Genkin, Adi Shamir and Eran Tromer. 'RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis'. In: *Advances in Cryptology – CRYPTO 2014*. Ed. by JuanA. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, pp. 444–461. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2_25. URL: http://dx.doi.org/10.1007/978-3-662-44371-2_25.

Exploiting acoustic emissions



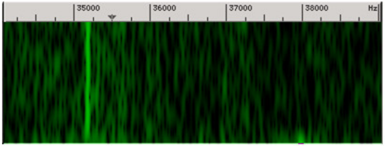


Exploiting acoustic emissions

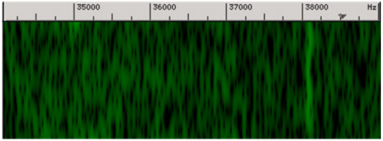


- The acoustic signals are picked up from components in the power supply.
- Individual CPU operations are too fast for a microphone to pick up.
- But long operations such as modular exponentiation (as in RSA) can create a characteristic acoustic spectral signature which can be detected using a microphone.

Exploiting acoustic emissions



Attacked bit is 0

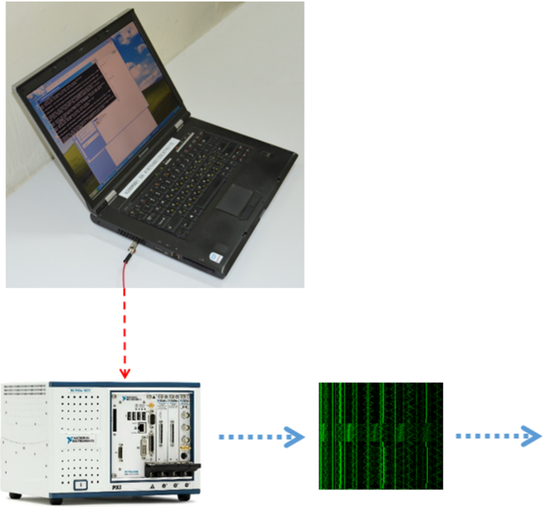


Attacked bit is 1

- The same authors[2] did the same thing again, but with variations in the ground–electric potential.

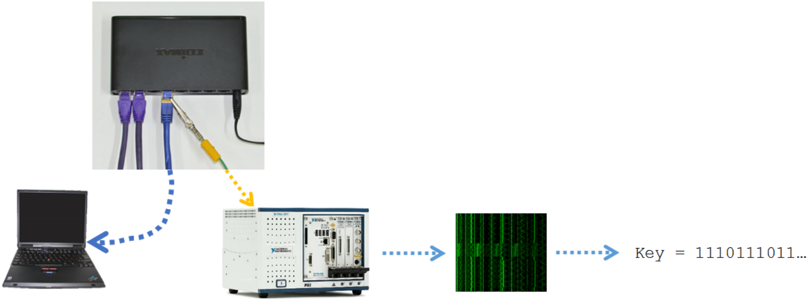
[2] Daniel Genkin, Itamar Pipman and Eran Tromer. 'Get your hands off my laptop: physical side-channel key-extraction attacks on PCs'. In: *Journal of Cryptographic Engineering* 5.2 (June 2015), pp. 95–112. ISSN: 2190-8516. DOI: 10.1007/s13389-015-0100-7.

Exploiting voltage



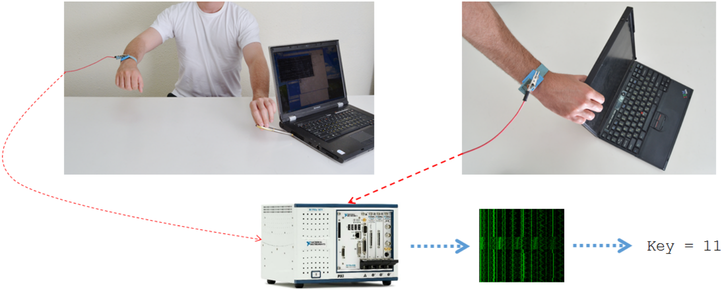
Key = 1110111011…

Exploiting voltage



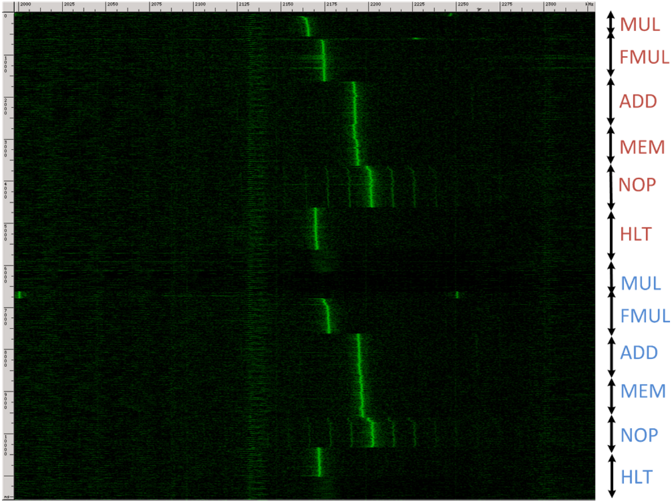
Key = 1110111011…

Exploiting voltage



Key = 1110111011...

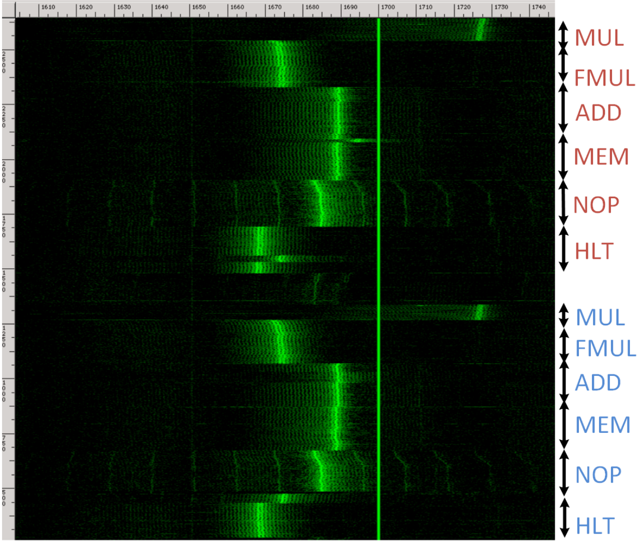
Exploiting voltage



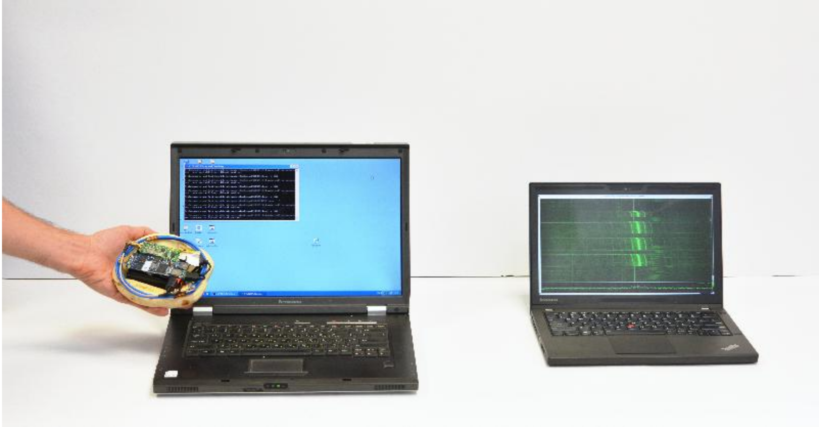
- And again[3], but with electromagnetic emissions.

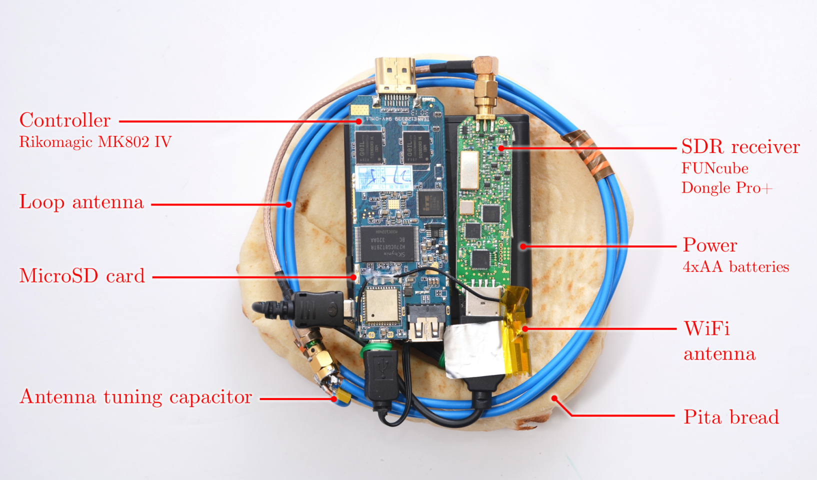
[3] Daniel Genkin et al. 'Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation'. In: *Cryptographic Hardware and Embedded Systems – CHES 2015*. Ed. by Tim Güneysu and Helena Handschuh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 207–228. ISBN: 978-3-662-48324-4.

Exploiting electromagnetic emissions



Exploiting electromagnetic emissions

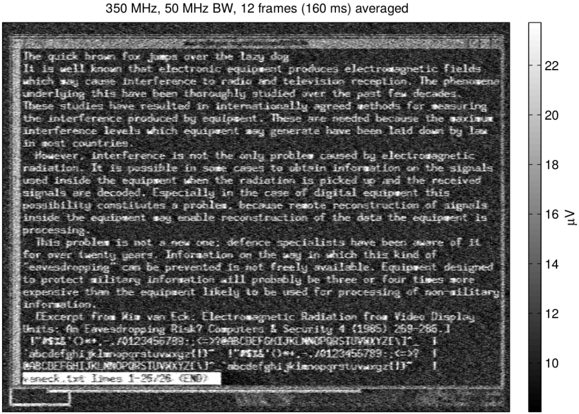



Controller
Rikomagic MK802 IV
Loop antenna
MicroSD card
Antenna tuning capacitor
SDR receiver
FUNcube
Dongle Pro+
Power
4xAA batteries
WiFi
antenna
Pita bread

Note

- There are also other parts emitting electromagnetic signals.
- *E.g.*, screens [Kuh04].

Exploiting electromagnetic emissions



350 MHz, 50 MHz BW, 12 frames (160 ms) averaged

```
The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic fields
which may cause interference to radio and television reception. The phenomena
underlying this have been thoroughly studied over the past few decades.
These studies have resulted in internationally agreed methods for measuring
the interference produced by equipment. These are needed because the maximum
interference levels which equipment may generate have been laid down by law
in most countries.
  However, interference is not the only problem caused by electromagnetic
radiation. It is possible in some cases to obtain information on the signals
used inside the equipment when the radiation is picked up and the received
signals are decoded. Especially in the case of digital equipment this
possibility constitutes a problem, because remote reconstruction of signals
inside the equipment may enable reconstruction of the data the equipment is
processing.
  This problem is not a new one; defence specialists have been aware of it
for over twenty years. Information on the way in which this kind of
"eavesdropping" can be prevented is not freely available. Equipment designed
to protect military information will probably be three or four times more
expensive than the equipment likely to be used for processing of non-military
information.
  [Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_  |
`abcdefghijklmnopqrstuvwxyz{|}~  !"#$%&'()*+,-./0123456789:;<=>?  |
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~   |
vaneck.txt lines 1-26/26 (END)
```

Fig. 3. Text signal received from a 440CDX laptop at 10 m distance through two intermediate offices (3 plasterboard walls).

1 Introduction
- What are side-channels?

2 Timing attacks
- Doing arithmetic
- Typing pattern and guessing passwords
- Summary

3 Emission attacks
- Emissions from electronic systems
- Exploiting acoustic emissions
- Exploiting voltage
- Exploiting electromagnetic emissions

4 Summary

- We can measure something during the operations.
- From these measurements we can infer things about operands *etc*.

[Gen+15] Daniel Genkin, Lev Pachmanov, Itamar Pipman and Eran Tromer. 'Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation'. In: *Cryptographic Hardware and Embedded Systems – CHES 2015*. Ed. by Tim Güneysu and Helena Handschuh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 207–228. ISBN: 978-3-662-48324-4.

[GPT15] Daniel Genkin, Itamar Pipman and Eran Tromer. 'Get your hands off my laptop: physical side-channel key-extraction attacks on PCs'. In: *Journal of Cryptographic Engineering* 5.2 (June 2015), pp. 95–112. ISSN: 2190-8516. DOI: 10.1007/s13389-015-0100-7.

[GST14] Daniel Genkin, Adi Shamir and Eran Tromer. 'RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis'. In: *Advances in Cryptology – CRYPTO 2014*. Ed. by JuanA. Garay and Rosario Gennaro. Vol. 8616. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2014, pp. 444–461. ISBN: 978-3-662-44370-5. DOI: 10.1007/978-3-662-44371-2_25. URL: http://dx.doi.org/10.1007/978-3-662-44371-2_25.

[Kuh04] Markus G Kuhn. 'Electromagnetic eavesdropping risks of flat-panel displays'. In: *Privacy Enhancing Technologies*. Springer. 2004, pp. 88–107.

[SWT01] Dawn Xiaodong Song, David Wagner and Xuqing Tian. ‘Timing Analysis of Keystrokes and Timing Attacks on SSH.’. In: *USENIX Security Symposium*. Vol. 2001. 2001.