Screaming Channels

When Electromagnetic Side Channels Meet Radio Transceivers
Giovanni Camurati, Sebastian Poeplau, Marius Muench,
Tom Hayes, Aurélien Francillon

RESSI
15-05-2019
Who are we?

System and Software Security Group at EURECOM
s3.eurecom.fr

I am a PhD student “on radio side channels”
Side Channels, The Idea

**Theory**
Secure lock is impossible to open

**Implementation**
Different sound if we make a partial correct guess

**Attack**
Open it with a few attempts
Embedded Devices and Side Channels

Secure systems:
- E-Passport,
- Smartcard, ...

Crypto against stealing, cloning, tampering, ...

Generally protected against attacks which require physical access
Conventional Side Channels

Power (current)

Direct EM

Clock harmonics as carriers

Physical activity depends on logic data

64MHz

P(f)

64MHz

Institut Carnot

Telacom & Société numérique

EURECOM

Sophia Antipolis
In Practice

Collection
E.g. loop probe
+ oscilloscope

Many Analyses/Attacks
SPA, CPA, TPA, ...
SEMA, CEMA, TEMA, ...

High correlation (strong leak)
Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

"TEMPEST AES"
Fox-IT, Riscure

\( \text{mm} \)

\( \text{cm} \)

\( 15 \text{ cm} \)

\( 30 \text{ cm} \)

\( 1 \text{ m} \)

wall
Embedded Devices and Side Channels

Secure systems:
E-Passport, Smartcard, ...
Crypto against stealing, cloning, tampering, ...
Generally protected against attacks which require physical access

Connected devices:
Smart watch, camera, ...
Crypto protects the communication channel
Only remote attacks are considered
Remote Side Channels

Remote Timing
Non constant time
Caches

AES, TLS, ...
WPA3 (Dragonblood)

EM?
Physical access
Local
Problems When Adding Wireless Capabilities
Implementation: Mixed-signal Chips

Idea:
CPU + Crypto + Radio
Same chip

Benefits:
Low Power, Cheap, Small
Easy to integrate

Examples:
BT, BLE, WiFi, GPS, etc
Issues

Reminder
Time vs. Frequency
Up-conversion
Issues

**Analog/RF**
Noise Sensitive

**Digital**
Noise resilient
Noise Source

**Same Chip**
Noise Coupling

**Careful Design**
Radio Still Works
Problems, the global view

Mixed-signal chip

Strong noise source

Digital Logic

Memory

Easy propagation
Screaming Channels
The Idea
Screaming Channels Idea

Conventional Side Channel Leak

Strong noise source

Mixed-signal chip

Digital Logic

Memory

Radio

Easy propagation Leak Propagation

Noise sensitive transmitter

Leak Is Broadcast

\[ P(f) \]

64 MHz 2.4 GHz
Screaming Channels in Action

Antenna + SDR RX

Radio Off
Radio TX
AES On

Cortex-M4
+ BT TX

2m

Wait loop
AES Starts

Noise
Packet

Time domain
Screaming Channels: Leak Broadcast

EM Leak, proximity

Radio Leak, e.g. 10m

$400 - $3000

Intended Transmission e.g. 1m

Other remote attacks

Alice

Bob

Eve
From Digital Noise
To Noise On The Radio Signal
Possible Impact on Radio Transmission

Digital:
- Inherently noisy

Analog:
- Noise sensitive

Propagation:
- Substrate coupling
- Power supply/Gnd
Practical Case We Observed

BT (GFSK modulation)

\[ I = A_k \cos(\varphi_k) \]
\[ Q = A_k \sin(\varphi_k) \]

\[ n(t) = AES(t) \cos(\omega_{clk}t) \]

Amplitude modulation
Extraction
Quadrature Amplitude Demodulation

\[ \frac{G_A_k}{2} AES(t) \cos((\omega + \omega_{\text{clk}})t + \varphi_k) \]
Extraction

\[ \frac{G A_k}{4} \]

AES(t)

Extract (trigger)

Align N (cross-corr.)

Average N

normalized amplitude(t) freq(t)

t

t

t
Attack
Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS

Extraction:
Automated via radio
Known plaintext

Attacks:
Correlation, Template
Code based on
ChipWhisperer

Much more advanced attacks exist
Correlation @ 10m

Radio leak @ 2.528GHz

Strong even @ 10m!!
Quick Demo

```
> sc-attack --data-path ~/phd/dumps/traces/tinyae

s_anechoic_10m_080618_attack/ --bruteforce --num-traces 100 attack tra_templates/10m/ --variable p_xor_k
```
Evolution of the attack

Cable

15 cm

2 m

3 m

5 m

10 m
Protection
Countermeasures

Resource constraint devices:
Cost, power, time to market, etc.

Classic HW/SW:
Masking, noise, key refresh (expensive, not complete)

Specific (SW):
Radio off during sensitive computations (real time constraints)

Specific (HW):
Consider impact of coupling on security during design and test (hard, expensive)
Final remarks
Reference to a Similar Effect

Tempest Fundamentals [5]
From ‘80s
Declassified 2000

Propagation of leaks:
1. Radiation
2. Conduction
3. Modulation of an intended signal (redacted)
4. Acoustic
Responsible Disclosure

- Major vendors & multiple CERTS
- Multiple acknowledgements of the relevance and generality of the problem
- 2 vendors are reproducing our results
- 1 vendor is actively looking at short/long-term countermeasures
Conclusion

General problem if sensitive processing and wireless tx
- HW AES, WiFi, other chips
- any device with radio?

A new point in the threat model space
- Remote EM attacks

Must be considered
- Design and test of new devices
- Smart countermeasures (specific)

Many open directions for future research
- More distant, less traces
- Different crypto and wireless technologies
- Attack the protocol
Questions?

Code
https://www.github.com/eurecom-s3/screaming_channels

More Info
https://s3.eurecom.fr/tools/screaming_channels

Giovanni Camurati
@GioCamurati
Acknowledgements

- The authors acknowledge the support of SeCiF project within the French-German Academy for the Industry of the future, as well as the support by the DAPCods/IOTics ANR 2016 project (ANR-16-CE25-0015).
- We would like to thank the FIT R2lab team from Inria, Sophia Antipolis, for their help in using the R2lab testbed.
References

• [4] Van Eck Phreaking
  https://en.wikipedia.org/wiki/Van_Eck_phreaking
Third-Party Images

- "nRF51822 - Bluetooth LE SoC : weekend die-shot" - CC-BY–Modified with annotations. Original by zeptobars
  https://zeptobars.com/en/read/nRF51822-Bluetooth-LE-SoC-Cortex-M0
Backup Slides
## Some Attack Data

<table>
<thead>
<tr>
<th>Distance</th>
<th>Environment</th>
<th>Implementation</th>
<th># Attack Traces</th>
<th># Template Traces</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 m</td>
<td>Office</td>
<td>tinyAES</td>
<td>52589 x 500</td>
<td>70000 x 500</td>
</tr>
<tr>
<td>3 m</td>
<td>Anechoic Room</td>
<td>tinyAES</td>
<td>718 x 500</td>
<td>70000 x 500</td>
</tr>
<tr>
<td>5 m</td>
<td>Anechoic Room</td>
<td>tinyAES</td>
<td>428 x 500</td>
<td>70000 x 500</td>
</tr>
<tr>
<td>10 m</td>
<td>Anechoic Room</td>
<td>tinyAES</td>
<td>1428 x 500</td>
<td>130000 x 500</td>
</tr>
</tbody>
</table>
Attack on Hardware AES, possible?

• Hardware AES implementations are used for link layer encryption

• Attacking turns out to be more difficult than software AES
  – Faster calculation, higher radio resolution is needed
  – Most of the time blackbox implementations

• We ran some experiments
  – 4/16 bytes recovered