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
Side Channels, The Idea

**Theory**
Secure lock is impossible to open
Side Channels, The Idea

Theory
Secure lock is impossible to open

Implementation
Different sound if we make a partial correct guess
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
Secure systems: E-Passport, Smartcard, ...
Secure systems:
E-Passport,
Smartcard, ...

Crypto against
stealing, cloning,
tampering, ...
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

Physical activity depends on logic data
Conventional Side Channels

Power (current)

Physical activity depends on logic data
Conventional Side Channels

Direct EM

Physical activity depends on logic data

Power (current)
Conventional Side Channels

Physical activity depends on logic data

Direct EM

Clock harmonics as carriers

Power (current)

\[ 64 \text{MHz} \]

\[ P(f) \]

\[ 64 \text{MHz} \]
In Practice

**Collection**
E.g. loop probe
+ oscilloscope

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

---

**AES**

High correlation (strong leak)
Many Side Channels Involving EM

- mm
- cm
- 15 cm wall
- 30 cm 1 m
- >10 m
Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

mm 15 cm 30 cm >10 m

wall 1 m
Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

mm

15 cm

wall

30 cm

1 m

>10 m
Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

"TEMPEST AES"
Fox-IT, Riscure [3]

mm
15 cm
30 cm
>10 m

cm
wall
1 m
Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

"TEMPEST AES"
Fox-IT, Riscure [3]

TEMPEST
Van Eck '85 [4]

mm
15 cm
wall
30 cm
1 m
>10 m
Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

"TEMPEST AES"
Fox-IT, Riscure [3]

TEMPEST
von Eck '85 [4]

mm
15 cm
30 cm
wall
1 m
Many Side Channels Involve EM

- Classic EM Attack: Agrawal et al. [1]
- Laptop Intel CPU: Genkin et al. [2]
- "TEMPEST AES": Fox-IT, Riscure

- mm
- cm
- 15 cm
- wall
- 30 cm
- 1 m
Embedded Devices and Side Channels

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

Crypto against
stealing, cloning,
tampering, ...

Generally protected
against attacks
which require
physical access
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, ...

---

Embedded Devices and Side Channels
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
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
Implementation: Mixed-signal Chips

Idea:
CPU + Crypto + Radio
Same chip

Benefits:
Low Power, Cheap, Small
Easy to integrate
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

Reminder
Time vs. Frequency
Up-conversion
Issues

Reminder
Time vs. Frequency
Up-conversion

\[ a(t) \quad A(f) \]
\[ c(t) \quad C(f) \]
Issues

Reminder
Time vs. Frequency
Up-conversion

\[ a(t) \quad A(f) \]
\[ c(t) \quad C(f) \]
\[ r(t) \quad R(f) \]
Issues
Issues

Analog/RF
Noise Sensitive
Issues

Analog/RF
Noise Sensitive

Digital
Noise resilient
Noise Source
Issues

**Analog/RF**
Noise Sensitive

**Digital**
Noise resilient
Noise Source

**Same Chip**
Noise Coupling
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
Problems, the global view

Mixed-signal chip

Digital Logic

Memory

Strong noise source
Problems, the global view

- Mixed-signal chip
- Strong noise source
- Digital Logic
- Memory
- Radio
- Noise sensitive transmitter
Problems, the global view

Mixed-signal chip

Strong noise source

Digital Logic

Memory

Radio

Noise sensitive transmitter

Easy propagation
Screaming Channels
The Idea
Screaming Channels Idea

Mixed-signal chip

Strong noise source

Digital Logic

Memory

Radio

Easy propagation

Noise sensitive transmitter

P(f)

64 MHz 2.4 GHz
Screaming Channels Idea

- Mixed-signal chip
- Strong noise source
- Noise sensitive transmitter
- Easy propagation

Conventional Side Channel Leak

P(f) vs. Frequency:
- 64 MHz
- 2.4 GHz
Screaming Channels Idea

Conventional Side Channel Leak

Strong noise source

Mixed-signal chip

Digital Logic

Memory

Radio

Easy propagation Leak Propagation

Noise sensitive transmitter

P(f)

64 MHz 2.4 GHz
Screaming Channels Idea

Conventional Side Channel Leak

Strong noise source

Mixed-signal chip

Digital Logic

Memory

Radio

Easy propagation Leakage propagation

Noise sensitive transmitter

Leak is broadcast

P(f)

64 MHz

2.4 GHz
Screaming Channels in Action

Antenna + SDR RX

Cortex-M4 + BT TX
Screaming Channels in Action

Antenna + SDR RX

Cortex-M4 + BT TX

Radio Off

Noise
Screaming Channels in Action

Antenna + SDR RX

Radio Off

Cortex-M4
+ BT TX

Radio TX

2m

Noise

Packet
Screaming Channels in Action

Antenna + SDR RX

Radio Off

Radio TX

Cortex-M4 + BT TX

2m

Noise Packet

Wait loop
Screaming Channels in Action

Antenna + SDR RX

Radio Off  Radio TX  AES On

Cortex-M4 + BT TX

2m

Wait loop

Noise  Packet
Screaming Channels in Action

Antenna + SDR RX

Cortex-M4 + BT TX

Radio Off  Radio TX  AES On

Wait loop  AES Starts

Noise  Packet

2m
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
Quick Demo

FFT

Demodulated

Center frequency

Spectrogram

Click, wheel or drag a digit to change center frequency; SPACE or numeric key for direct input. Hold SHIFT to disable carry.
Quick Demo Transmit continuous wave

FFT

Demodulated Center frequency

Spectrogram

Click, wheel or drag a digit to change center frequency; SPACE or numeric key for direct input. Hold SHIFT to disable carry.
Quick Demo

Transmit continuous wave

FFT

Spectrogram

Demodulated

Center frequency

AES
Screaming Channels: Leak Broadcast

EM Leak, proximity

Intended Transmission e.g. 1m

Other remote attacks
Screaming Channels: Leak Broadcast

- EM Leak, proximity
- Intended Transmission e.g. 1m
- Other remote attacks
Screaming Channels: Leak Broadcast

- EM Leak, proximity
- Intended Transmission e.g. 1m
- Other remote attacks
Screaming Channels: Leak Broadcast

- EM Leak, proximity
- Intended Transmission e.g. 1m
- Radio Leak, e.g. 10m
- Other remote attacks

Alice

$400 - $3000

Eve

Bob
Screaming Channels: Leak Broadcast

- EM Leak, proximity
- Intended Transmission e.g. 1m
- Radio Leak, e.g. 10m
- Other remote attacks

$400 - $3000
Screaming Channels: Leak Broadcast

- EM Leak, proximity
- Radio Leak, e.g. 10m
- Other remote attacks

Alice
- Intended Transmission e.g. 1m

Bob

Eve
- $400 - $3000
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

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

\[ \cos(\omega t) \]
\[ \sin(\omega t) \]

\[ V_{\text{supply}} \]
\[ GA_k \cos(\omega t + \varphi_k) \]
Practical Case We Observed

BT (GFSK modulation)

\[ I = A_k \cos(\phi_k) \]

\[ Q = A_k \sin(\phi_k) \]

\[ V_{\text{supply}} \]

\[ G \]

\[ G A_k \cos(\omega t + \phi_k) \]
Practical Case We Observed

BT (GFSK modulation)

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

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

\[ V_{\text{supply}} \]

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

\[ G \]

\[ GA_k \cos(\omega t + \varphi_k) \]
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

\[ GA_k \cos(\omega t + \varphi_k)[1+n(t)] \]
Extraction
Quadrature Amplitude Demodulation

\[ \frac{G A_k}{2} \text{AES}(t) \cos((\omega + \omega_{clk})t + \varphi_k) \]
Quadrature Amplitude Demodulation

\[
\frac{GA_k}{2} AES(t) \cos((\omega + \omega_{clk})t + \varphi_k)
\]
Quadrature Amplitude Demodulation

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

\[
\frac{GA_k}{4} \cdot AES(t)
\]
Extraction

\[ \frac{G A_k}{4} A E S(t) \]

Extract (trigger)

Normalized amplitude \( f(t) \)

Frequency \( f(t) \)
Extraction

\[ \frac{G A_k}{4} AES(t) \]

\[ f_{\text{trig}} \]

Extract (trigger)

 normalized amplitude(t) freq(t)
Extraction

\[
\frac{GA_k}{4} AES(t) \rightarrow f_{trig} \rightarrow \text{Extract (trigger)} \rightarrow \text{normalized amplitude}(t) \rightarrow \text{freq}(t)
\]
Extraction

\[ \frac{G_A_k}{4} \] AES(t)

Extract (trigger)

Align N (cross-corr.)

normalized amplitude(t) freq(t)

\[ f_{trig} \]
Extraction

\[ \frac{GA_k}{4} AES(t) \]

- Extract (trigger)
- Align N (cross-corr.)
- Average N

normalized amplitude(t) \( f(t) \)

\( t \)

\( t \)

\( t \)
Attack
Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS
Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS

Extraction:
Automated via radio
Known plaintext
Attacking

Targets:
- Cortex-M4 + BT TX
- TinyAES, mbedTLS

Extraction:
- Automated via radio
- Known plaintext

Attacks:
- Correlation, Template
- Code based on ChipWhisperer
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

average trace (/home/giovanni/phd/dumps/traces/tinyaes_anechoic_10m_080618_template 10000 traces)

Radio leak @ 2.528GHz  Strong even @ 10m!!
Quick Demo

```bash
$ python2 src/screamingchannels/attack.py --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --num-traces 3000 attack tra_templates/10m
```

Template

Attack Traces
Quick Demo

> python2 src/screamingchannels/attack.py --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --num-traces 3000 attack tra_templates/10m

- Attack Traces
- Template
- Attack one byte at a time
Quick Demo

$>$ python2 src/screamingchannels/attack.py --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --num-traces 3000 attack tra_templates/10m

- Attack Traces
- Template
- Attack one byte at a time
- SUCCESS!
Evolution of the attack
Evolution of the attack

Cable
Evolution of the attack

Cable

15 cm
Evolution of the attack

**Cable**

15 cm

2 m
Evolution of the attack

Kable

15 cm

2 m

3 m
Evolution of the attack

Cable

15 cm

2 m

3 m

5 m
Evolution of the attack

Cable

15 cm

10 m

3 m

2 m

5 m
Protection
Countermeasures

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

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

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

I. (C) Propagation of TEMPEST Signals (U) – There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (4) Electromagnetic Radiation (U) – Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created: first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (4) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (4) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (4) [Six lines redacted.]

![Figure 1-5. - Amplitude-Modulated Carrier (U) (U)](image)

e. (4) Acoustics (U) – Characteristically plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays – these produce sound and consequently can be sources of compromise.

Tempest Fundamentals [5]
From ‘80s
Declassified 2000
1-5. (G) Propagation of TEMPEST Signals (U). - There are four basic ways by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (4) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (4) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. power lines.

c. (4) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (4) [Six lines redacted.]

e. (4) Acoustics (U). - Characteristically, plaintext processing systems are primarily electrical in function. However, other sources of CS exist where mechanical operations occur and sound is produced. Keyboards, printers, relays — these produce sound and consequently can be sources of compromise.

Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

Tempest Fundamentals [5]
From ‘80s
Declassified 2000
Reference to a Similar Effect

1-5. (G) Propagation of TEMPEST Signals (U). - There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (4) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (4) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (4) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (4) [Six lines redacted.]

e. (4) Acoustics (U) - Characteristically plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays -- these produce sound and consequently can be sources of compromise.

Tempest Fundamentals [5]
From ‘80s
Declassified 2000
Reference to a Similar Effect

1.5. (G) Propagation of TEMPEST Signals (U). - There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation, conduction, modulation of an intended signal, and acoustics. A brief explanation of each follows.

a. (4) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic, or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (4) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (4) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (4) Six lines redacted.

e. (4) Acoustics (U). - Characteristically plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays -- these produce sound and consequently can be sources of compromise.

1.5-1. (G) Amplitude-Modulated Carrier (U) (U)

Tempest Fundamentals [5]
From ‘80s
Declassified 2000

Propagation of leaks:
1. Radiation
2. Conduction

1. Acoustic
Reference to a Similar Effect

1-5. (G) Propagation of TEMPEST Signals (U). - There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (4) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created: first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exist the CS of the installation.

b. (4) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (4) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (4) [Six lines redacted.]

e. (4) Acoustics (U). - Characteristically plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays -- these produce sound and consequently can be sources of compromise.

Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

Tempest Fundamentals [5]
From ‘80s
Declassified 2000
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?
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
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)
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 DAPCODOs/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

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