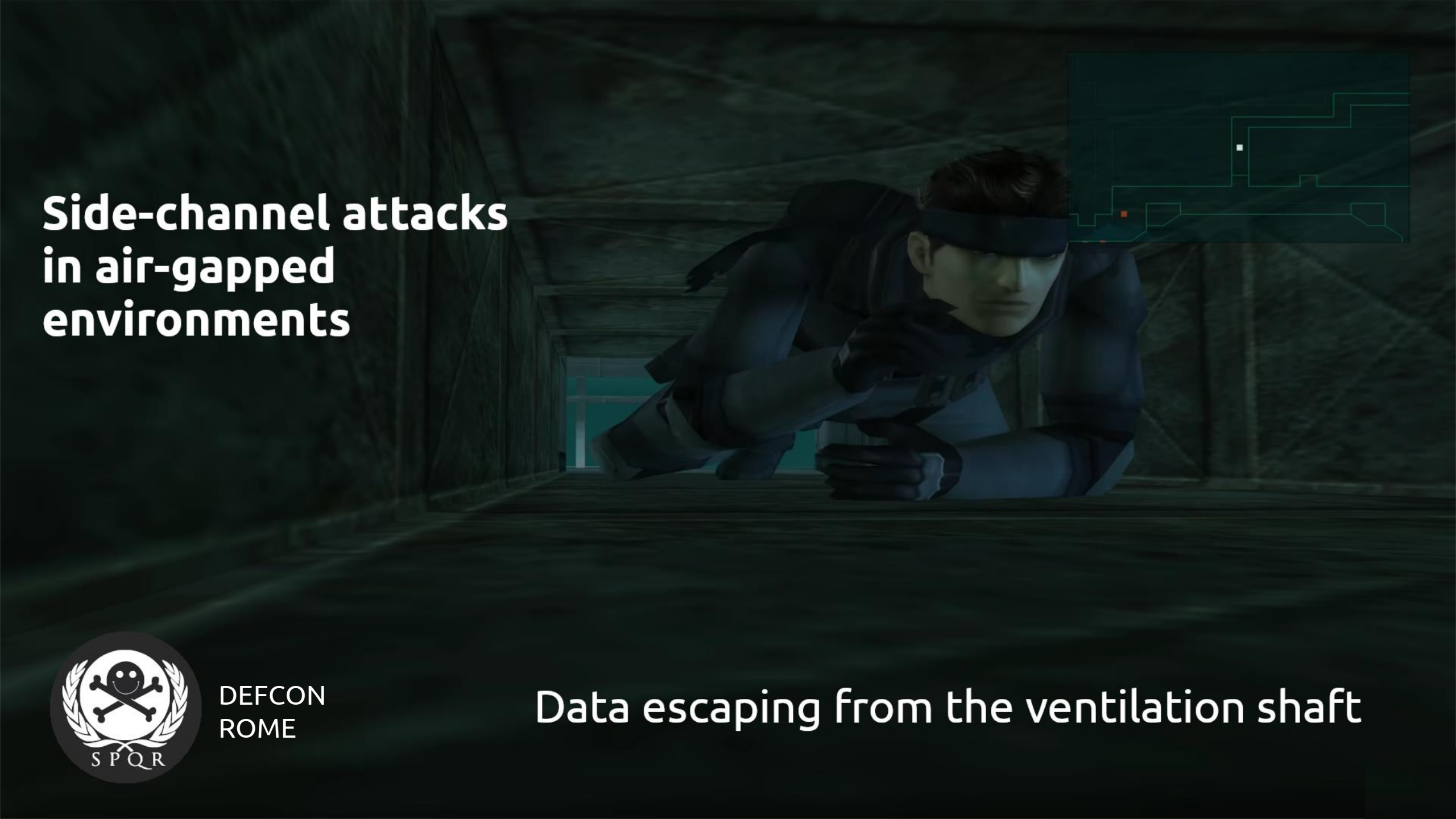
Side-channel attacks in air-gapped environments



DEFCON
ROME

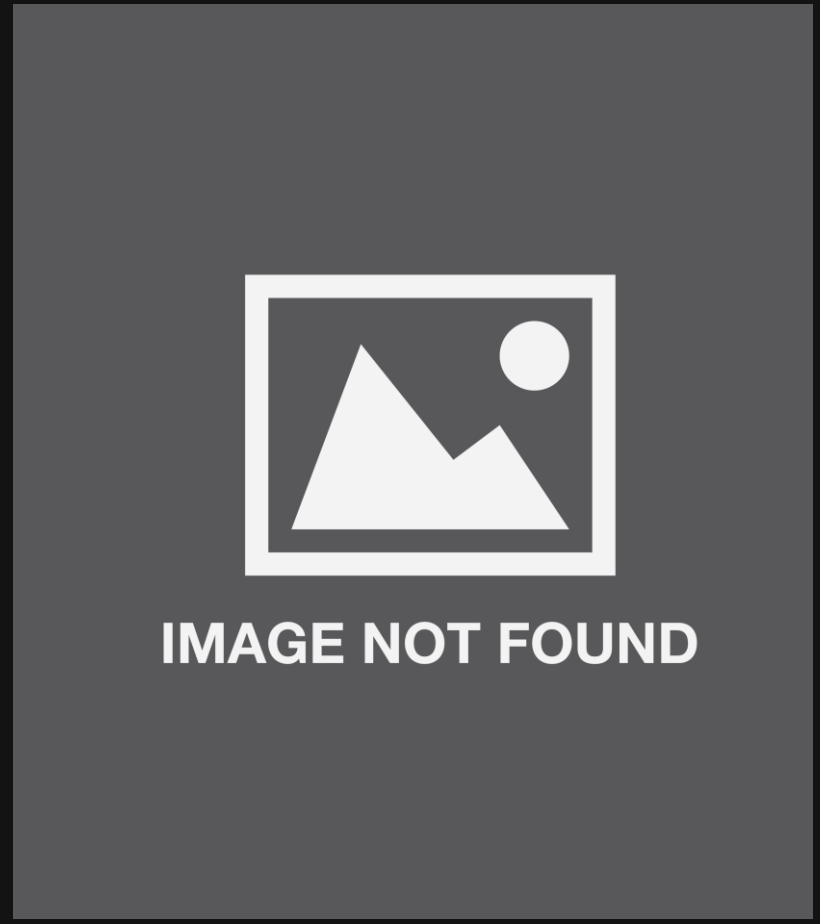
Data escaping from the ventilation shaft

About me

Giovanni De Luca

Computer Engineering graduate and student of Engineering in Computer Science Master's Degree @Sapienza.
Cybersecurity, AI, computer graphics and open source enthusiast, occasional contributor to several open source software projects.

3D artist and musician in my spare time (when I don't waste it playing videogames or watching anime). Green tea drinker.



jotaro-sama

@josuke_miyazawa

What this talk is about

- What an air-gapped environment is
- Traditional sound devices based side-channel attacks
- Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers (how it works)
- Other side-channel attack techniques

Disclaimer

The contents of this talk are potentially **DANGEROUS**!

Attacks are shown here **ONLY** for the purposes of self-defense and public awareness

I do **NOT** take responsibility for your own actions

What is an air-gapped environment?

- An air-gapped computer or network is one that has no connection to outside networks (i.e. the internet)
- Since an internet connection can represent a security vulnerability, systems with highly critical information are air-gapped.
- Is it possible for an attacker to retrieve information from an air-gapped system, assuming he somehow manages to put his exploit there?

What is a side-channel attack?

In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs).

Sound devices

- Air-gap doesn’t provide full isolation: the acoustic channel can be exploited for data exfiltration from an isolated computer to a nearby mobile phone (for example).
- Malware on a PC can use the ultrasonic frequency range in order to send data outside via the speakers or headphones.
- Furthermore, the microphone on the infected PC can be used to receive commands, fully simulating wireless connection.
- No speakers, headphones or microphones, is it enough?

Introducing Fansmitter

Made by a research group from Ben-Gurion University of the Negev in Israel, it shows how to exfiltrate data from an air-gapped, sound-gapped computer.

It utilizes the noise emitted from the CPU and chassis fans which are present in virtually every computer.

Attack model

We’re considering the case in which both the mobile phone and the PC are infected.

Malware on the PC gathers relevant data, modulates and transmits them via the soundwaves emitted from the fans. The phone receives it with it’s microphone, then demodulates it, decodes it and sends it to the attacker.

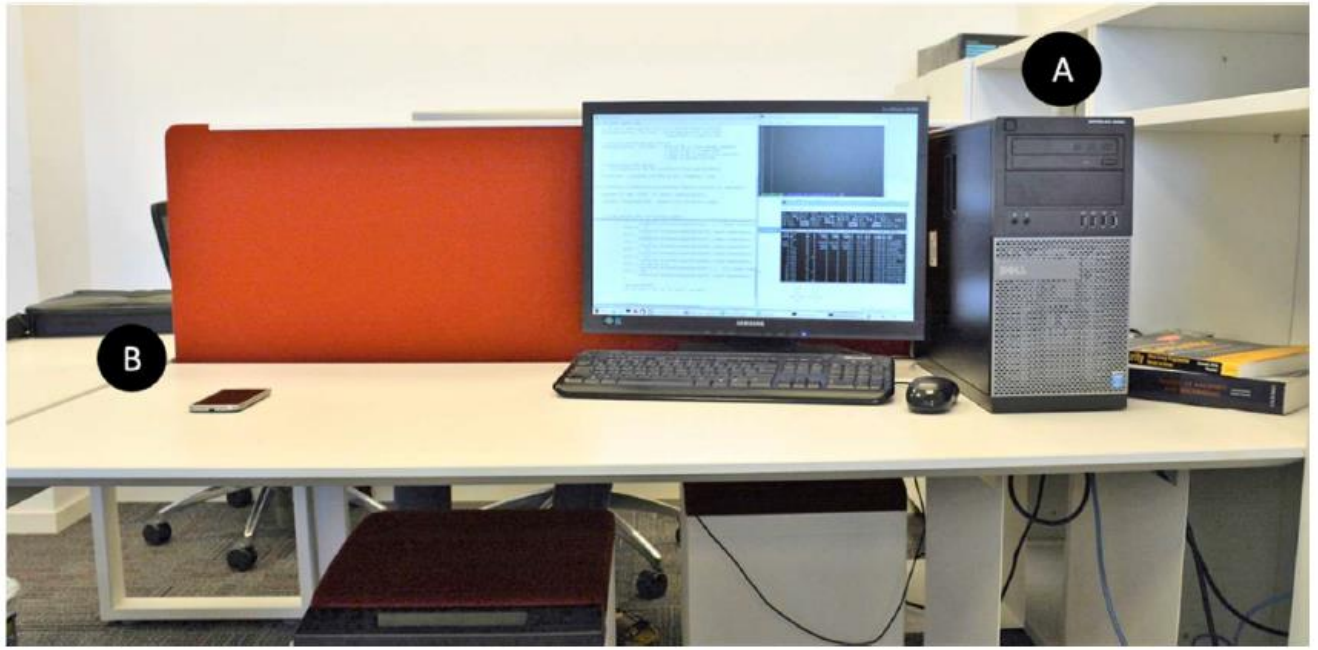


Figure 1. A typical exfiltration scenario. A compromised computer (A) - without speakers, and with audio hardware disabled - transmits sensitive information via acoustic signals. This information is received and decoded by a nearby mobile phone (B)

Fans on a modern computer

- PSU fan is generally regulated by an internal controller and can’t be manipulated or monitored via software.
- CPU and chassis fans are guaranteed to be on basically every computer: we’ll focus on these ones.

Fan control

- Most modern motherboards use four wires for the CPU and chassis fans
- Third and fourth wire can be used to monitor and alter the fan speed!

Pin	Symbol	Function
1 (red)	GROUND	Ground wire
2 (black)	12 V	12 V fan powering
3 (black)	FAN_TACH	Output signal reporting the fan speed
4 (yellow)	FAN_CONTROL	Input signal, allows adjustment of the fan speed

Fan rotation and acoustic signal

- The noise level mainly depends on the location, size, number of blades and the current RPM of the rotating fan.
- Since location, size and number of blades of a fan are fixed, the RPM is the main factor to determine the noise level.
- Fan noise (in dB) increases with the fifth power of the fan rotation speed: changes in the RPM cause an immediate change in the noise emitted.

Blade pass frequency (BPF)

- The main acoustic tone generated by a running fan
- Calculated by multiplying the number of blades (n) with the rotating speed (R) in revolutions per minute (RPM)
- BPF = n*R/60

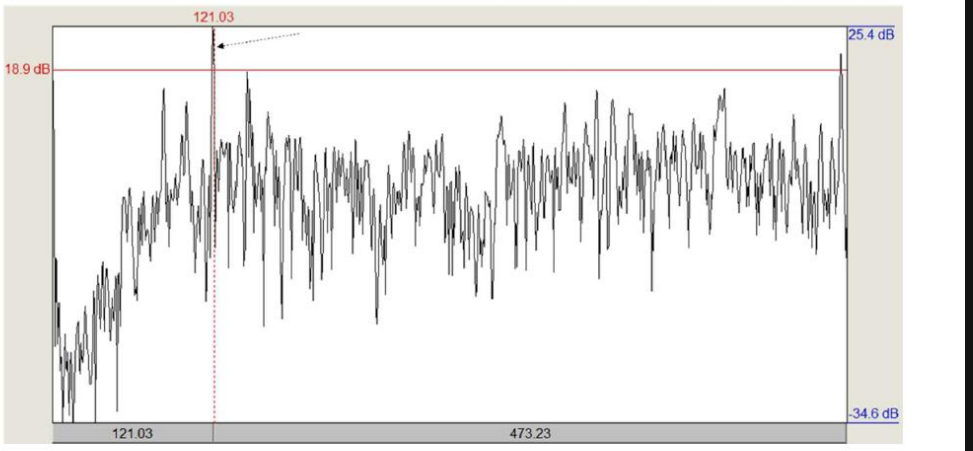


Figure 4. Typical BPF plot (R ~ 1000 RPM)

Figure 4 illustrates a typical fan spectrum at about 1000 RPM. The BPF is indicated in red at around $120\ Hz$, as expected for a seven blade fan.

Signal processing

- Frequencies we’re going to use are all under 1 kHz
- Downsample the signals from 44.1 to 2 kHz (Nyquist theorem)
- Bandpass filtered signals around the expected BPF
- Since the typical chassis fan has 7 blades, let’s precalculate expected BPF for the R ranges used in the experiments

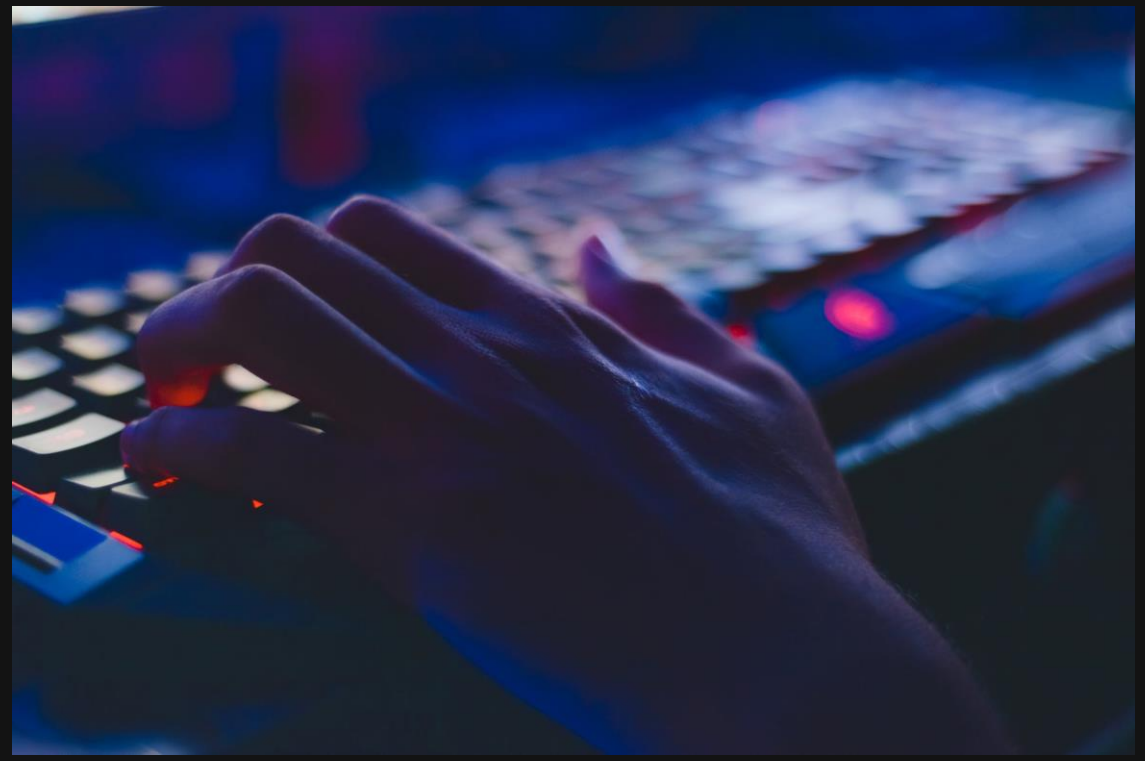
Table 3. Expected BPF values for seven blade fans

R (RPM)	BPF (Hz)
1000-1600	116-187
1600-3000	187-350
2000-2500	233-292
4000-4500	466-525

Channel stealth

There are three main strategies for making the transmission go unnoticed:

- Flexibility in terms of the time of the attack
- Use of low frequencies
- Use of close frequencies



Data modulation

- Amplitude Shift Keying (ASK)
  - More resilient to the type of fan in use
  - Slower
  - Used when the type of fan is unknown to the attacker
- Frequency Shift Keying (FSK)
  - More resilient to environmental noise
  - Faster
  - Used when the generic type of transmitting fan is known

Amplitude Shift Keying

- We assign an amplitude level of the carrier wave to 0 and another one to 1 in order to represent binary data (B-ASK).
- We have rotation levels R_0 and R_1 corresponding to the amplitude levels A_0 (representing 0) and A_1 (representing 1).
- $R_0 < R_1$ implies $A_0 < A_1$

Bit framing

- The amplitudes and frequencies encoding depends on the type of fan and exact RPM values used
- In the case of ASK, A_1 and A_2 depend on the distance between transmitting computer and receiver
- To solve this issue, we transmit data in small frames with a preamble used by the receiver to determine the amplitude levels or frequency values of 0 and 1.

Preamble (4 bits)	Payload (12 bits)
1010	111010101110

Some results

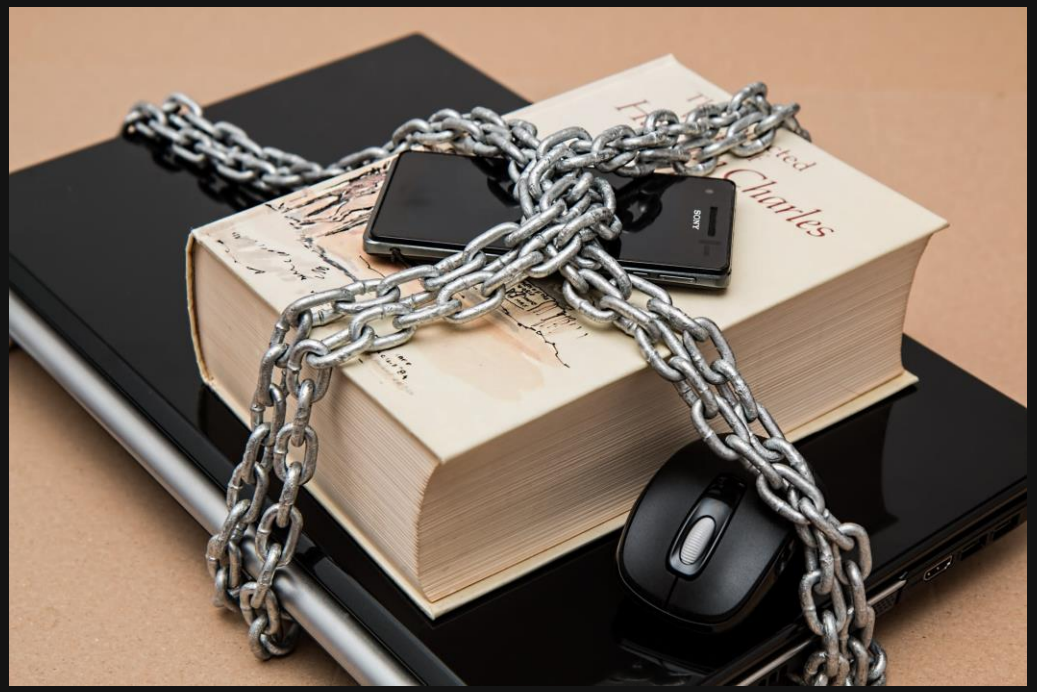
In a testing environment with ordinary background noise, seven workstations, several network switches and an active air conditioning system:

- B-FSK, $R_0 = 4000$ RPM, $R_1 = 4250$ RPM, $F_0 \approx 495$ Hz, $F_1 \approx 525$ Hz, 1 meter distance, no delay: 15 bits/min (900 bits/hour)
- B-FSK, $R_0 = 2000$ RPM, $R_1 = 2500$ RPM, $F_0 \approx 261$ Hz, $F_1 \approx 294$ Hz, 4 meters distance, no delay: 10 bits/min (600 bits/hour)

Countermeasures

They can be of three different types:

- Procedural
- Software based
- Hardware based

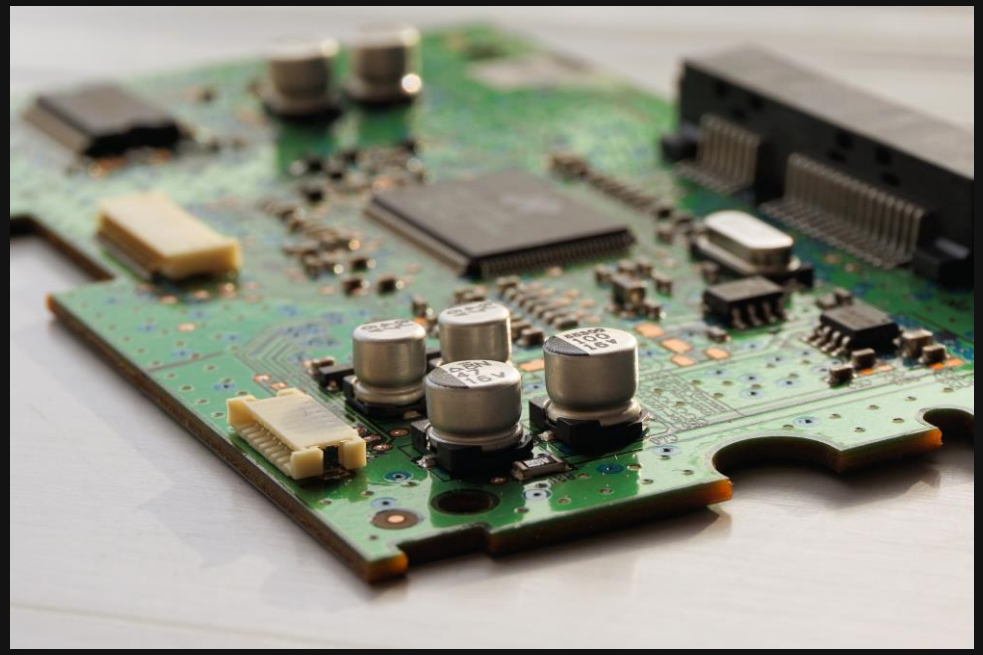


Method	Type	Challenges
'Zones' separation	Procedural	Space limitations
AV / monitoring	Software	Can be bypassed by rootkits or evasion techniques
Fan regulation	Software	Can be bypassed by low-level malware
Noise detection	Hardware	False positives and false alarms
Signal jamming	Hardware	Generate background noises
Fan replacement, Water cooling, etc.	Hardware	Financial limitations
Chassis isolation	Physical	Financial and space limitations

Even more advanced techniques

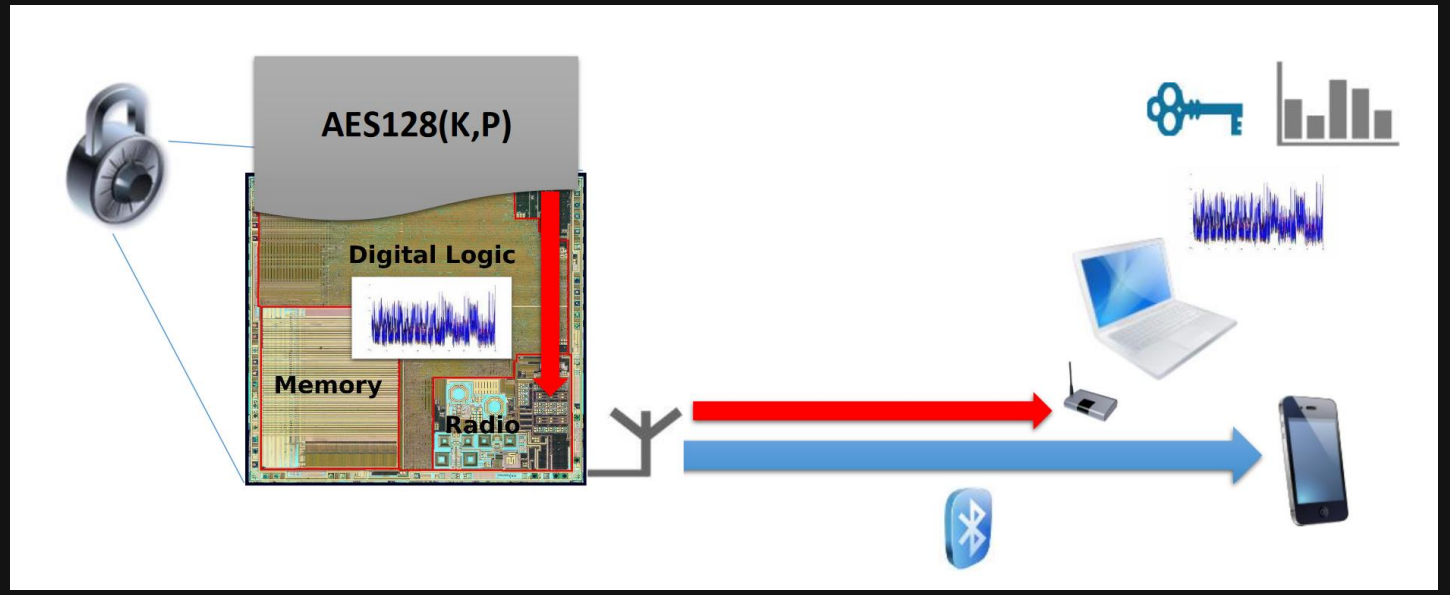
Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers (EURECOM researchers)

- “Noisy” digital circuits can leak information to sensitive analog radio components, if not properly separated
- Can work over a much longer range than usual electromagnetic side-channel attacks (at least 10 meters!)



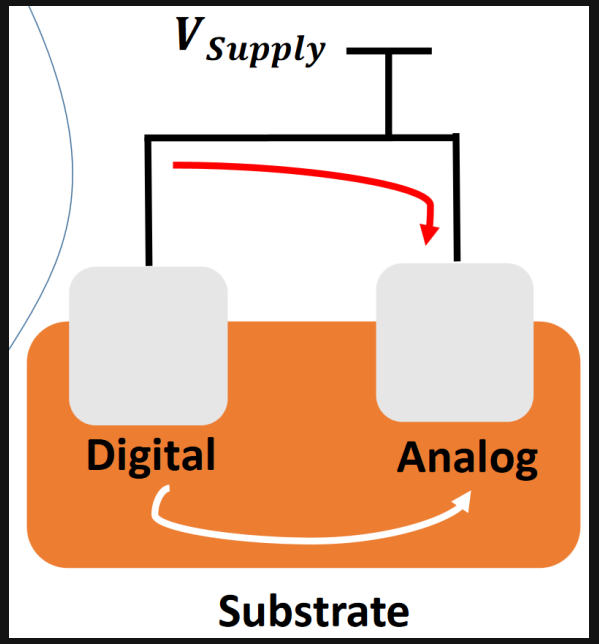
Mixed signal circuits

- Modern technology requiring very compact systems has driven to employing systems with the analog and digital part on the same chip more and more often.



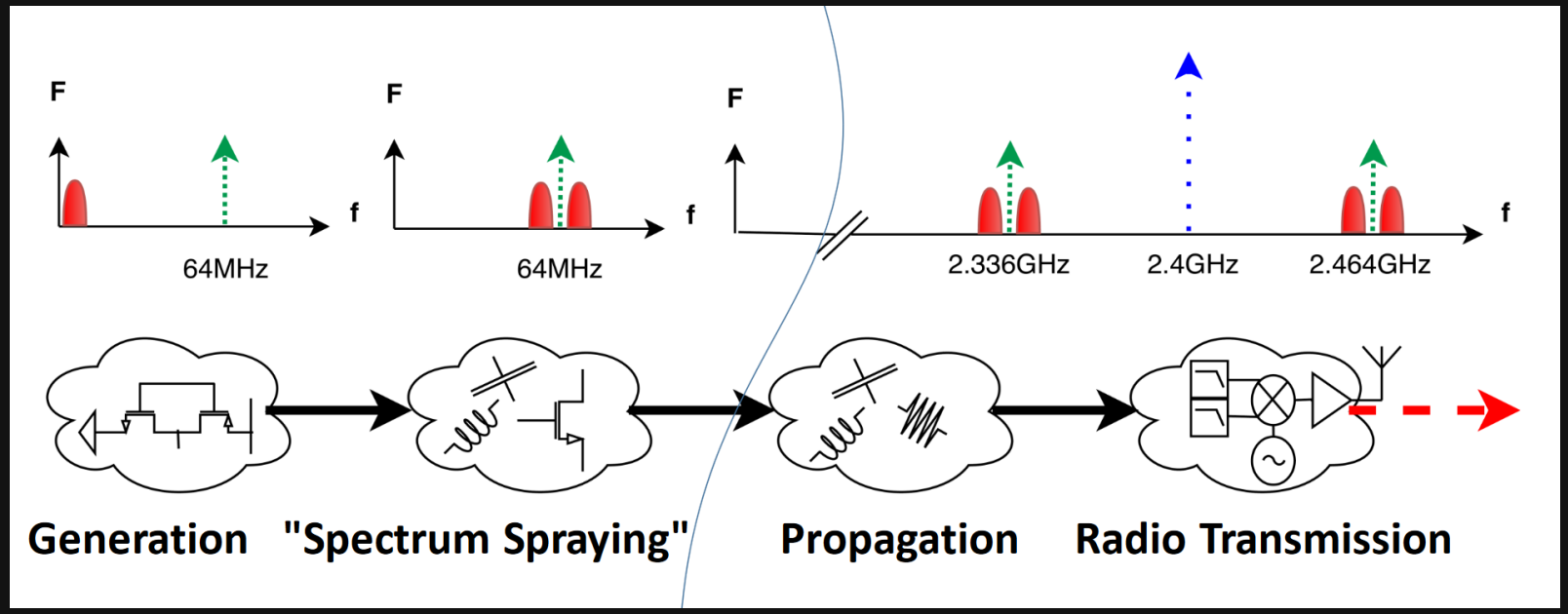
Digital to analog propagation

- The electromagnetic noise is generated by the transistors switching from 0 to 1 and viceversa
- There are two ways this leak propagates to the analog part
  - Substrate coupling (same silicon die)
  - Power supply coupling (same power supply)



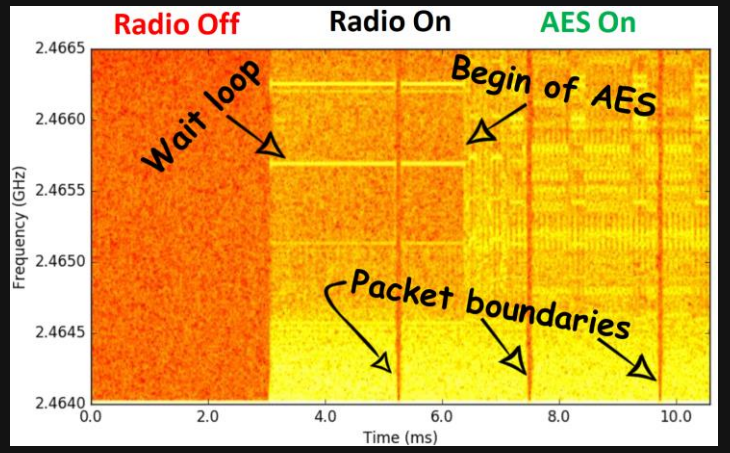
Signal transmission scheme

The noise is generated by the computations, modulated by the clock, leaked to the analog part and finally amplified and transmitted by the radio component along with the intended transmission on “close” frequencies.



How a proof of concept attack works

- By analyzing the frequency spectrum of the transmission, we can recognize patterns of an AES encryption being executed on the device.
- With a correlation attack while scanning the bluetooth transmission, the PoC exploit was able to correctly guess the whole 128 bits AES key (considered cryptographically secure) in a very short time!




```
Subkey 15, hyp = f2:  0.036744405776
Subkey 15, hyp = f3:  0.0794445830793
Subkey 15, hyp = f4:  0.0578478064227
Subkey 15, hyp = f5:  0.0599842735251
Subkey 15, hyp = f6:  0.044246817196
Subkey 15, hyp = f7:  0.0556983355754
Subkey 15, hyp = f8:  0.0492112150682
Subkey 15, hyp = f9:  0.0395435356938
Subkey 15, hyp = fa:  0.0627971665835
Subkey 15, hyp = fb:  0.0552149198924
Subkey 15, hyp = fc:  0.0446795354698
Subkey 15, hyp = fd:  0.0413364486661
Subkey 15, hyp = fe:  0.0468227709369
Subkey 15, hyp = ff:  0.056587945731
Best Key Guess:   fa   5e   76   25   5b   e8   b6   e4   27   73   27   67   d9   6a   3f   2f
Known Key:        fa   5e   76   25   5b   e8   b6   e4   27   73   27   67   d9   6a   3f   2f
PGE:             000  000  000  000  000  000  000  000  000  000  000  000  000  000  000  000
SUCCESS:           1    1    1    1    1    1    1    1    1    1    1    1    1    1    1    1
NUMBER OF CORRECT BYTES: 16
> exit
```

Countermeasures

- Classic (software or hardware)
  - Masking the leak with more noise
  - Expensive for low-cost, power-constrained chips
  - For more advanced defenses, more advanced attacks than a simple correlation attack could be used
- Software-specific
  - Turning off the radio part when critical computations (e.g. AES encryption) are being executed
  - Should completely prevent attacks on this channel
  - Could impact real-time performances and thus not always be applicable
- Hardware-specific
  - Consider security impact of noise coupling during design and testing of chips
  - Increasing costs in production too much?

Hope you enjoyed the talk!

References

- https://en.wikipedia.org/wiki/Air_gap_(networking)
- https://en.wikipedia.org/wiki/Side-channel_attack
- Hanspach, Michael; Goetz, Michael (November 2013). "On Covert Acoustical Mesh Networks in Air". Journal of Communications. **8**: 758–767
- Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, Yuval Elovici, Ben-Gurion University of the Negev (2016), “Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers”. arXiv:1606.05915v1 [cs.CR]
- Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon, EURECOM (2018) “Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers”. http://s3.eurecom.fr/docs/ccs18_camurati_preprint.pdf