Interception of Frequency-Hopping Signals for TEMPEST Attacks

Corentin Lavaud [1] Robin Gerzaguet [1] Matthieu Gautier [1]
Olivier Berder [1] Erwan Nogues [2,3] Stephane Molton [3]

[1]Univ Rennes, CNRS, IRISA

[2]Univ Rennes, INSA Rennes, IETR, CNRS

[3]DGA-MI

Financed by PEC

Introduction

- Side-channel denotes the presence of information in an illegitimate channel
- Can be at **hardware** (TEMPEST) or software levels
- E.g. **electromagnetic radiation**[1], power consumption[2], light[3], crosstalk[4]...

Main goals of this work are to:

  - detect frequency hopping signals
  - estimate the used channels
  - extract the baseband message
  - in low complexity manners

- Number of channels, spectrum distribution and the time slot duration are provided
- Hop sequence and time synchronization are unknown
- High bandwidth ($>$100 MHz) & short time slot duration ($<$10 μs)

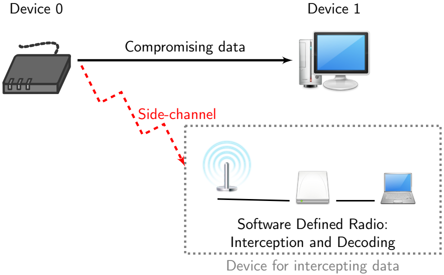


Figure: Side-channel overview

[1] R. Spreitzer et al. (2018). "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices". In: *IEEE Communications Surveys & Tutorials* 20.1, pp. 465–488
[2] Y. L. Du, Y.-H. Lu, and J.-L. Zhang (June 2013). "Novel Method to Detect and Recover the Keystrokes of PS/2 Keyboard". In: *Progress In Electromagnetics Research C* 41, pp. 151–161
[3] J. Loughry and D. A. Umphress (Aug. 2002). "Information leakage from optical emanations". In: *ACM Transactions on Information and System Security* 5.3, pp. 262–289
[4] Y. Su et al. (Aug. 2017). "USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs". In: *USENIX Security Symposium*, pp. 1145–1161

Interception system

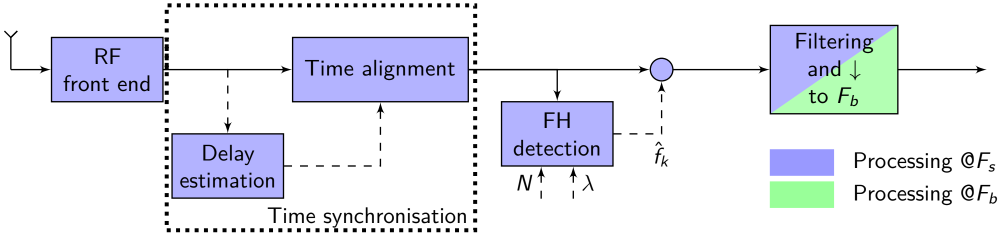


Figure: Proposed architecture of the interception system (N: number of channels, λ: average factor)

- *RF front end*: Receive and adjust the signal
- *Time alignment*: Reshape the data for FH detection
- *Delay estimation*: Hopping times estimation (done with SDFT)
- *FH detection*: Current channel estimation (done with FFT)
- *Filtering*: Baseband signal extraction from the estimated used channel (if any) (done with a derotor and low pass filter)

Bluetooth use case - Setup

- Validation performed on a Bluetooth link between a laptop and a headset
- Ettus X310 SDR has been used
- Non-controlled radio environment
- Difference in distance to the SDR between devices 1 and 2, in order to have a distinct receiving power (RSSI)
- Use of the relative RSSI and the used protocol (Bluetooth v2.1 + EDR) to better identify the devices

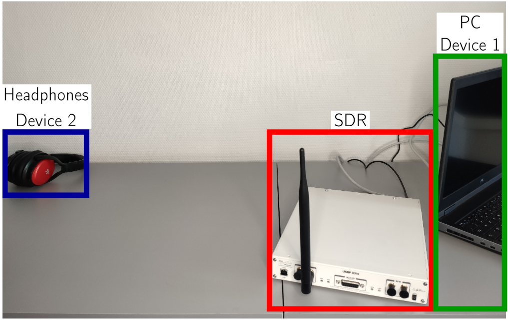


Figure: Experimental setup

Bluetooth use case - Results

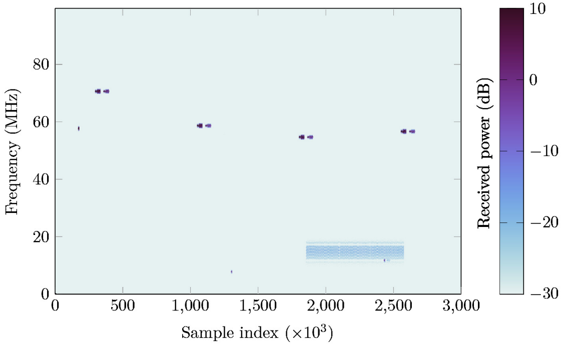
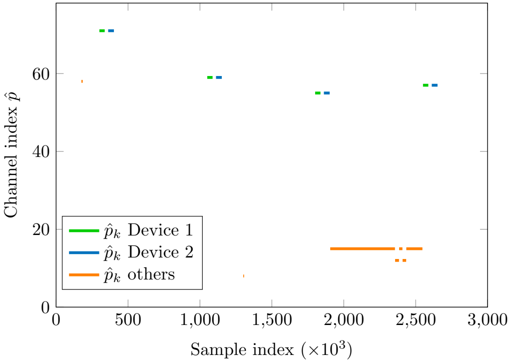


Figure: Time-frequency representation of the Bluetooth signal, $F_s = 100$ MHz



its

Figure: Extracted channel index and device recognition ($\lambda = 625$, $N = 80$)

- FH hop detection is possible at 100 MHz
- Several devices can communicate on the same frequency and while still being differentiated

Conclusion and Perspectives

- The evolution of SDR allows the monitoring of large bandwidth
- Sporadic signals are difficult to eavesdrop (bandwidth requirement, fast hopping)
- Proposed method capable to estimate the used channel even with a fast hopping with a low complexity
- Our method has been validated by listening to commercial Bluetooth devices and blindly detecting their frequency hops

Perspectives

- Automatically deals with any number of channels and hop speed
- Enhance the implementation part with FPGA acceleration
- Toward real time exploit: automatically estimating if a side-channel is hidden

References

Du, Y. L., Y.-H. Lu, and J.-L. Zhang (June 2013). "Novel Method to Detect and Recover the Keystrokes of PS/2 Keyboard". In: *Progress In Electromagnetics Research C* 41, pp. 151–161.

Loughry, J. and D. A. Umphress (Aug. 2002). "Information leakage from optical emanations". In: *ACM Transactions on Information and System Security* 5.3, pp. 262–289.

Spreitzer, R. et al. (2018). "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices". In: *IEEE Communications Surveys & Tutorials* 20.1, pp. 465–488.

Su, Y. et al. (Aug. 2017). "USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs". In: *USENIX Security Symposium*, pp. 1145–1161.

Thank You!

Do you have any questions?

HW/SW Architecture

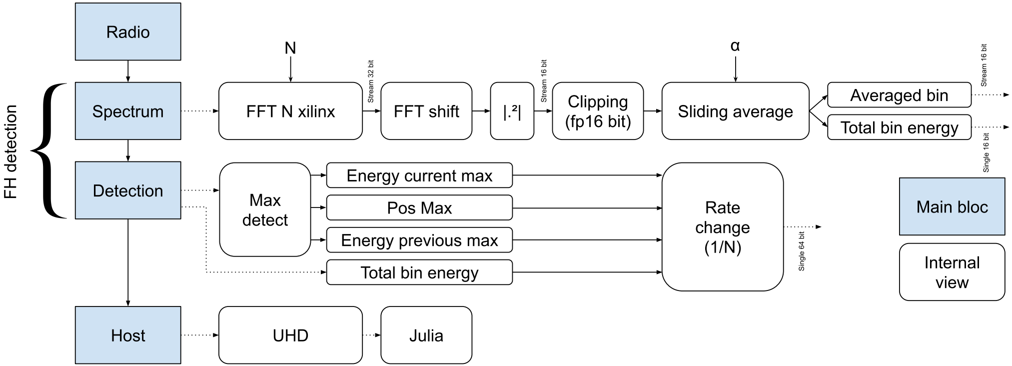


Figure: FPGA Architecture

- Working FH detection (20 μs hop time) & side-channel extraction (audio 4 *khz* bandwidth)
- *Energy current max* and *Pos max*: core data interception
- *Energy previous max*: energy from the last detected channel, in case of sync error
- *Total bin energy*: sum of fft energy, basic interference spectrum measurement
- Due to speed constraints, the data are not valid at α bin extremum of the spectrum.

Side-channel recovering

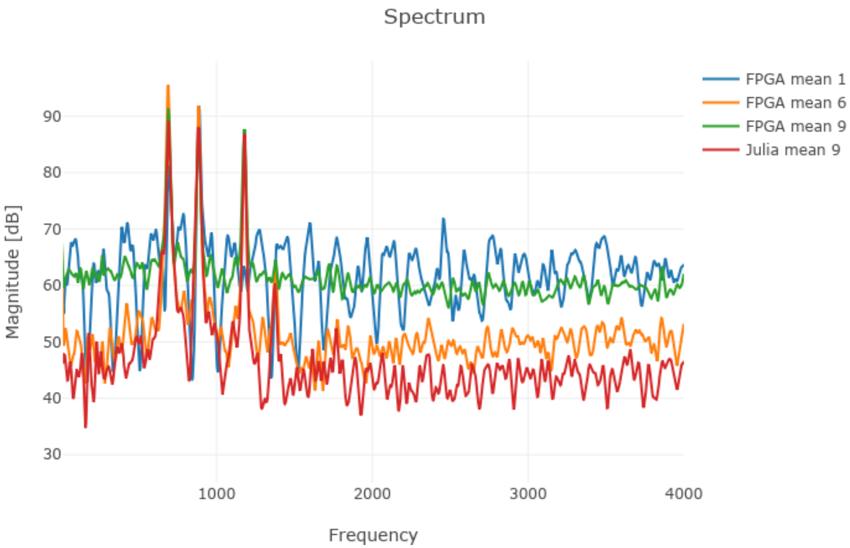


Figure: Audio spectrum recovered (display kama filtered)