Screaming Channels

Giovanni Camurati* and Aurélien Francillon†

Related Concepts

Compromising Emanations, Side channels, Electromagnetic Attacks

Definitions

Modern devices often require wireless communication interfaces and therefore contain both digital, analog, and RF electronics. The term 'Screaming Channels' denotes a leakage of sensitive information that occurs when side-channel leakage is accidentally broadcast by the radio transmitter alongside the intentional wireless communication, making it possible to recover cryptographic secrets from a large distance. Mixed-signal chips, containing both digital and radio blocks on the same chip are especially vulnerable to Screaming Channels.

Background

Radio Transmitters

Radios transmit data using electromagnetic waves at radio frequency. Data is typically encoded in the amplitude, frequency, and/or phase of a baseband signal, which is then multiplied with a radio-frequency carrier by a mixer (up-conversion), and amplified by a power amplifier (Behzad 2008). At the receiver, the inverse process consists in down-converting the signal to baseband and demodulating it.

* Corresponding author
ETH Zurich, Zurich, Switzerland
giovanni.camurati@eurecom.fr

† EURECOM, Sophia-Antipolis, France
aurelien.francillon@eurecom.fr

Mixed-Signal Chips

Modern chips include not only digital components, but also analog and radio-frequency parts. Mixed-signal chips including a digital processor and wireless transceivers are popular in modern connected devices. Despite their many advantages, mixed-signal chips suffer from the problem of interference between noisy digital blocks and noise-sensitive radio components (Bronckers et al 2009; Afzali-Kusha et al 2006).

Theory and Application

A Side Channel Over Radio

Overview

The radio transmitter in a mixed-signal chip might pick-up, amplify, and broadcast the side-channel leakage produced by the digital blocks on the same device (Camurati et al 2018). This side channel allows mounting key-recovery attacks against cryptographic algorithms running on the victim from a distance of several meters (Figure 1). The name 'Screaming Channels' highlights the strength of the amplified leakage on the radio channel, in contrast to the weak 'whisper' of conventional side channels.

Root Problem

The root cause of Screaming Channels is the coupling between compromising emanations, such as a digital system, and a radio transmitter. This coupling can in particular occur when both are on the same silicon substrate on a *mixed-signal chip*. As a consequence, many coupling paths exist for noise to flow between the two. In addition to this, digital blocks use square-wave signals that generate harmonics (noise) that is both strong and dependent on the logical data processed by the circuit, while radio components are very sensitive to noise. In principle, the flow of sensitive information from the digital domain to the radio transmission could happen through a coupling path to any of the components of the transceiver. A concrete instance of Screaming Channels occurs on Nordic Semiconductor nRF52832 Bluetooth Low Energy (BLE) chips. It is likely caused by coupling with the power amplifier resulting in an amplitude modulated leakage of the transmitted frequency-modulated BLE packets.

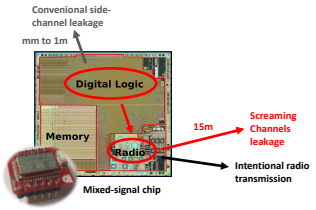

Fig. 1 Overview of Screaming Channels. Original picture by Zeptobars (2014), modified with annotations.

Characteristics

A thorough analysis of the nRF52832 reveals many characteristics of Screaming Channels (Camurati et al 2020).

A first set of observations is related to the coexistence of the side-channel leakage with the legitimate radio signal sent by the transmitter. While this facili-

tates attacks at large distance, it also requires a method to extract the leakage. For the nRF52832, independent demodulation of the leakage is simple, because amplitude modulation is orthogonal to frequency modulation. BLE data is sent in packets, causing 'holes' in the traces, but this problem can be solved by combining multiple traces.

A second set of observations is related to the side channel leakage itself. The leakage model is distorted compared to the conventional Hamming Weigth model, requiring a detailed profiling step. This is likely due to the coupling between digital and radio blocks. Indeed, such distortion is not observed for conventional electromagnetic leakage from the same chip, and it is independent of distance, setup, and device. Profile reuse is thus possible.

Attack

Large Distance

Key-recovery attacks against AES-128 using Screaming Channels have been demonstrated at a distance of 15 m in a realistic environment (Camurati et al 2020). A data-dependency was still detected at 40 m and AES traces were still extracted at 60 m. Using multiple receivers improves reception in presence of obstacles. Improvements with deep-learning have been studied by Wang et al (2020).

Realistic Target

Screaming Channels has been used for a proof-of-concept attack against application-layer cryptography in a real system (Camurati et al 2020). Google Eddystone beacons are a type of BLE beacons designed with security in mind, for example, by including authentication, encrypted telemetry data, and ephemeral identifiers. The authentication protocol is such that the attacker can trigger AES-128 encryptions with known random plaintext. With Screaming Channels, the attacker can measure the corresponding leakage, amplified, on the radio channel. The attacker misuses the channel map of the BLE connection to force the victim to use only two BLE channels.

Future directions

Attacks

Hardware Encryption

Link-layer cryptography often leverages a dedicated hardware accelerator. While the leakage from internal operations is too weak to be measured on the target chip, the transfer of the plaintext from software to the hardware accelator can be observed (Camurati et al 2020). Using Screaming Channels to recover plaintext from hardware peripherals is an interesting research direction.

Other Radio Protocols

Extracting Screaming Channels leakage from protocols using more complex modulations remains an open question. Preliminary results for some WiFi chips have been shown (Camurati 2020).

Defenses

Software

A simple countermeasure to Screaming Channels consists in making sure that the radio is not transmitting while the processor is manipulating sensitive information. Though this countermeasure eliminates the leakage channel at its root, it might be challenging to implement in complex software stacks and in presence of tight timing constraints.

Hardware

Manufacturers aim to limit noise coupling between digital and radio parts, to comply with regulations, and to preserve radio transmissions performance. Reducing the coupling to prevent data leakage requires additional efforts. Hardware countermeasures will increase costs. Simulation tools capable of detecting information leakage in the early phases of design would be useful.

Cross-References

Differential Power Analysis, Electromagnetic Analysis, Electromagnetic Attack, Profiled side-channel attack, Radio Frequency Attacks, Rank Estimation, Side-Channel Attacks, Tempest.

References

Afzali-Kusha A, Nagata M, Verghese NK, Allstot DJ (2006) Substrate noise coupling in soc design: Modeling, avoidance, and validation. Proceedings of the IEEE 94(12):2109–2138, DOI 10.1109/JPROC.2006.886029, URL https://doi.org/10.1109/JPROC.2006.886029

Behzad A (2008) Wireless LAN Radios: System Definition to Transistor Design (IEEE Press Series on Microelectronic Systems). John Wiley & Sons, Inc., Hoboken, NJ, USA

Bronckers S, Van der Plas G, Vandersteen G, Rolain Y (2009) Substrate Noise Coupling in Analog/RF Circuits. ARTECH HOUSE, Norwood, MA, USA

Camurati G (2020) Security Threats Emerging from the Interaction Between Digital Activity and Radio Transceiver. Theses, Sorbonne Université, URL https://tel.archives-ouvertes.fr/tel-03414339

Camurati G, Poeplau S, Muench M, Hayes T, Francillon A (2018) Screaming channels: When electromagnetic side channels meet radio transceivers. In: Lie D, Mannan M, Backes M, Wang X (eds) Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, ACM, pp 163–177, DOI 10.1145/3243734.3243802, URL https://doi.org/10.1145/3243734.3243802

Camurati G, Francillon A, Standaert F (2020) Understanding screaming channels: From a detailed analysis to improved attacks. IACR Trans Cryptogr Hardw Embed Syst 2020(3):358–401, DOI 10.13154/tches.v2020.i3.358-401, URL https://doi.org/10.13154/tches.v2020.i3.358-401

Wang R, Wang H, Dubrova E (2020) Far field EM side-channel attack on AES using deep learning. In: Chang C, Rührmair U, Katzenbeisser S, Schaumont P (eds) Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security Workshop, ASHES@CCS 2020, Virtual Event, USA, November 13, 2020, ACM, pp 35–44, DOI 10.1145/3411504.3421214, URL https://doi.org/10.1145/3411504.3421214

Zeptobars (2014) nRF51822 - Bluetooth LE SoC : weekend die-shot CC-BY 3.0. https://zeptobars.com/en/read/nRF51822-Bluetooth-LE-SoC-Cortex-M0