Compromising Electromagnetic Emanations: Side-Channel Leakages in (Connected) Embedded Devices

Pierre Ayoub*[1]

[1]Trustworthy systems: foundations and practices (LAAS-TRUST) – Laboratoire d'Analyse et d'Architecture des systèmes – France

Résumé

Modern electronic devices are increasingly interconnected and integrated. Communications security mainly relies on cryptographic algorithms which ensure a mathematically guaranteed level of confidentiality. However, when algorithms are executed by the hardware, they inevitably interact with their physical environment. This can lead to sensitive information being inferred from physical measurements. Attacks exploiting these measurements instead of the main channel are known as side-channel attacks, leveraging an unintentional relation between a physical quantity and the secret. In this talk, we will focus on new security risks impacting microcontrollers linked to unexpected interactions between heterogeneous digital and analog embedded modules. In particular, we analyze threats related to cross-layer interactions that can be exploited through electromagnetic side-channel analysis and look at two novel security issues. First, the applicability of newly discovered side-channel attacks regarding modern communication protocols is not systematically evaluated. An illustration of this is the Screaming Channels attack, which exploits a phenomenon of intermodulation between the leakage from a digital activity and the carrier of a radio transceiver in mixed-signal chips. Modern protocols only enable the radio transceiver for a short duration, introducing a serious limitation since Screaming Channels exploits leakage broadcasted through the radio transceiver. This part introduce BlueScream, which demonstrate how Screaming Channels impact the Bluetooth Low Energy protocol. We highlight how an attacker can manipulate the protocol parameters through traffic injection, forcing a victim to transmit during sensitive operations, demonstrating the threat introduced by Screaming Channels for the Internet of Things ecosystem. Second, despite a flourishing literature on electromagnetic side channels, the modulation of leaked signals remains a complex phenomenon which is not fully understood. Enhancing the understanding of how digital activity modulate leaked electromagnetic signals is critical for both offensive and defensive applications. In this context, electromagnetic side channels typically focus on the amplitude of leaked signals, neglecting the potential interest of other modulation types from a security perspective. This part introduce PhaseSCA, which uncovers unintended phase modulation in leaked signals as a novel source of side-channel. We also highlight that combining amplitude-modulated and phase-modulated emanations significantly improve existing side-channel attacks.

*Intervenant