Late Breaking Results: SoC-FPGA HW Trojan leaking data through EM Covert Channel

Marie-Aïnhoa Nicolas, Jordane Lorandel, Christophe Moy
Univ Rennes, CNRS, IETR UMR 6164, F 35000
Rennes, France
marie.nicolas@univ-rennes.fr, jordane.lorandel@univ-rennes.fr, christophe.moy@univ-rennes.fr

***Abstract*—This paper demonstrates an attack exploiting an Electromagnetic (EM) leak coming from the SoC-FPGA I/O. A covert channel is created by a dedicated Hardware Trojan controlling the EM emanations between the DDR3L SDRAM and the SoC-FPGA, exfiltrating sensitive data.**

***Index Terms*—SoC-FPGA, Electromagnetic leak, Pulse emanation, covert channel**

I. Introduction

System-on-Chip Field Programmable Gate Arrays (SoC-FPGA) have proven to be essential thanks to their programmability for specific application and execution speed. Its integrity and security has been studied thoroughly, from passive and active attacks to their associated countermeasures. Nowadays, with the expansion of Artificial Intelligence (AI), they have become a major actor for neural network inference. Their massive use in many application fields from edge-computing to cloud-based infrastructure highlights their attractiveness. New threats were revealed in the community, showing potential information leaks from this circuit. In [1], electromagnetic (EM) emanations from a SoC-FPGA with an open source neural network (NN) framework were studied. They successfully recovered the transmitted bitmap image from the EM emanations. Despite what was previously indicated, the leak was found to actually be coming from the SoC-FPGA input/outputs (I/O) towards the DDR3L SDRAM (Double Data Rate Synchronous Dynamic Random Access Memory) rather than the internal bus. This paper aims to demonstrate that the whole chip security could be compromised. More particularly, if an attacker is able to manipulate the communications entering or outgoing from the chip, an EM covert channel can be created to leak sensitive data and to recover them at distance. This paper focuses on the exchanges between the DDR memories and the SoC-FPGA.

II. Attack Scenario

The studied EM emanations occur in the form of pulses which are generated each time a transition from a state to another occurs [2]. In our case, the information leak is exacerbated by the state changes at the SoC-FPGA's I/O. Depending on the targeted I/O, an attacker could exploit the leak to potentially recover the initial data [1] or to create a covert-channel [3]. In this paper, communications between the SoC-FPGA and the DDR memory are considered. By writing or reading into the external memory, an attacker can control the corresponding EM pulses, leading to potential leaks of sensitive data. Similar work has been done on computer RAM [3] on which a malware was injected. Using this setup, the leaking RAM was able to generate a 1000 bits/s On-Off-Keying signal. In this work, a HT located inside the FPGA fabric is proposed to create a covert channel without software consideration [3].

A. DDR3L SDRAM Communication Protocol

DDR3L SDRAM is a high performance memory, widely used in many hardware platforms for data exchanges at very high throughput. At physical layer, multiple I/O are necessary, each one getting a specific role [4]. Data are sent on both positive and negative edges of the clock allowing a data transmission rate of twice the clock frequency. For example, the PYNQ-Z2 platform has a 525 MHz DDR3 clock frequency (T = 1.9 ns) resulting in 1.05 GHz data rate. The tracks for the read and write exchanges are called *DQ*. In our case, the DDR3 uses 16 *DQ* lines allowing 16 bits to be read or written every clock edge by burst of eight 16-bit data.

B. Hardware Trojan

The originality of this paper lies in the use of a malicious hardware IP allowing to shape the signal implemented into the logic fabric. The malicious IP implemented on the FPGA has a direct read and write access (AXI-Master interface) to the DDR through the High-Performance AXI port (HP AXI) of the SoC-FPGA. The attacker can then manipulate the data with the IP and control the shape of the resulting EM emanations accordingly. To perform an effective eavesdropping of the leaked information, the EM probe placement and polarity are decisive. According to the the SoC-FPGA package, the probe was placed on top of the *DQ* I/O to obtain the best quality of the signal.

III. Leak exploitation

The proposed attack is performed on a PYNQ-Z2 and depicted in Figure 1. The emanations are recovered with the RF Langer R-3-2 probe with a PA-203 amplifier and a Wavemaster 8620A oscilloscope to visualize the traces.

A. Preliminary experiments

The data request size must be adapted accordingly to the message that the attacker wants to transmit through the trojan. The write request is divided into packets, each one transporting 16 32-bit integers while the read request generates a single packet of the desired message length. For the attacker, it's

978-3-9826741-0-0/DATE25/© 2025 EDAA

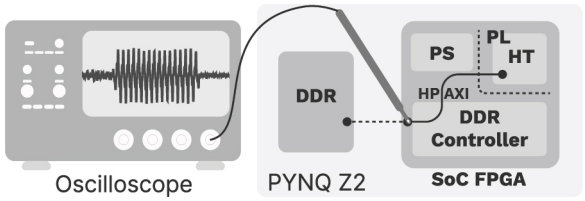

Fig. 1. Attack setup and scenario.

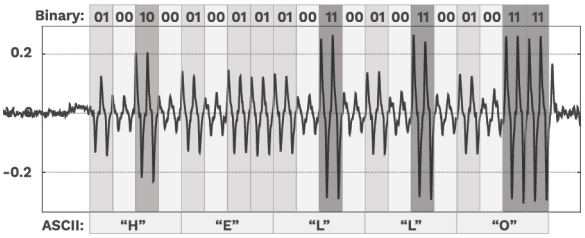

Fig. 3. Message successfully transmitted through the covert channel.

preferable to focus on the read request as the data is concatenated into a single transaction. By manipulating the data being exchanged, the attacker is able to create an emanation at the memory clock frequency and to modify its amplitude.

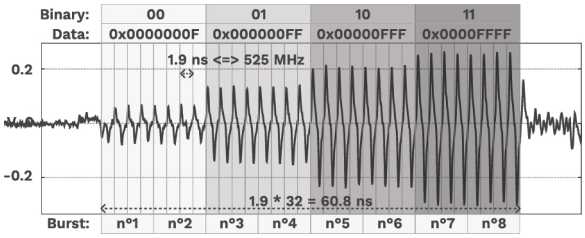

Fig. 2. Read packet emanation manipulation.

In our study, the DDR Clock frequency will act as carrier signal. For each state change, the generated pulse is shaped as a single peak. Depending on the change, positive (from 0 to 1) or negative (from 1 to 0), the peak direction is influenced (top or bottom). By continuously alternating between these two states, an emanation is created with the same period as the DDR clock. Otherwise, sending the same data does not create any pulse. The attacker has the capability to control the amplitude of the EM emanations by defining the number of switching bits in a transaction, which in our case, depends on the number of *DQ* tracks. For instance, if all the 16 tracks are switching simultaneously, the peak amplitude reaches its maximum with the value *0x0000FFFF*. Figure 2 depicts the corresponding EM emanations resulting from a read transaction. The amplitude of the emanation is associated to a binary symbol (e.g *00*, *01*, *10*, *11*). Every clock edge represents a 16-bits data exchange with the DDR, leading to a total transmission time of 60.8 ns. This creates a four-level amplitude modulation for which the carrier frequency corresponds to the DDR clock frequency.

B. EM Covert Channel

Figure 3 illustrates the resulting EM traces recorded on a PYNQ-Z2 board, in which the HT was configured to leak the message "Hello" through the covert channel with the DDR memory. Each binary symbol is identified from the signal amplitude on two clock periods. The resulting speed rate averages at 525 Mbits/s. For the word "Hello", the transmission is 76 ns long, since 40 integers are exchanged in total (five ASCII characters of 8 bits). The emations were successfully recovered and demodulated outside the chip.

C. Discussion

By using a HT, this paper brings a novel approach in comparison to [3]. Different modulations can be further investigated such as OOK, QAM, etc. Due to its low footprint, the HT can be hard to detect. Moreover, The HT could be used to leak critical information such as cryptographic keys directly from the FPGA fabric. Currently, the leaked data is recovered with a near-field EM probe but the attack range could be enhanced by using Software-Defined Radio (SDR) for which the major limitation is the sampling rate. For low end devices, the symbol identification time could be enlarged to match a lower sampling rate but this will decrease the transmission rate. One can consider that the HT would not be the only element accessing the DDR in real applications. The use of a preamble inserted to the sensitive data could also be considered as in [3] to make the covert transmission detection process easier.

IV. Conclusion

This paper shows that the SoC-FPGA I/O pins can be exploited as a way to create an AM covert channel. An attack was successfully performed by manipulating the data exchange with the DDR3L SDRAM to create a modulated signal carrying sensitive information. Here, only the I/O towards the DDR are studied, but it reveals that any other SoC-FPGA I/O pin could be used to perform this attack. Those leaks could be a critical security breach and must be investigated further.

V. Acknowledgments

This work is supported by the European Union through European Regional Development Fund (ERDF), Ministry of Higher Education and Research, CNRS, Brittany region, Conseils Départementaux d'Ille-et-Vilaine and Côtes d'Armor, Rennes Métropole, and Lannion Trégor Communauté, through the CPER Project CyMoCod.

References

[1] M. M. Thu, M. M. Réal, M. Pelcat, and P. Besnier, "Bus electrocardiogram: Vulnerability of soc-fpga internal axi bus to electromagnetic side-channel analysis," *2023 International Symposium on Electromagnetic Compatibility – EMC Europe*, 2023.

[2] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays," University of Cambridge, Computer Laboratory, Tech. Rep. UCAM-CL-TR-577, Dec. 2003.

[3] M. Guri, "Rambo: Leaking secrets from air-gap computers by spelling covert radio signals from computer ram," in *Secure IT Systems: 28th Nordic Conference, NordSec 2023, Oslo, Norway, November 16–17, 2023, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2023, p. 144–161.

[4] *8Gb: x4, x8, x16 DDR3L SDRAM*, Micron, 2015.