



Experimental interfacing with the iPhone 6s through its PCIe communication bus

Mohamed Amine Khelif, Jordane Lorandel, Olivier Romain

► To cite this version:

Mohamed Amine Khelif, Jordane Lorandel, Olivier Romain. Experimental interfacing with the iPhone 6s through its PCIe communication bus. 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE), Jun 2022, Anchorage, France. pp.631-634, <10.1109/isie51582.2022.9831665>. <hal-03841047>

HAL Id: hal-03841047

<https://hal.science/hal-03841047v1>

Submitted on 6 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/362269212>

Experimental interfacing with the iPhone 6s through its PCIe communication bus

Conference Paper · June 2022

DOI: 10.1109/ISIE51582.2022.9831665

CITATIONS

0

READS

3

3 authors:



Mohamed Amine Khelif

Université de Cergy-Pontoise

7 PUBLICATIONS 25 CITATIONS

SEE PROFILE



Jordane Lorandel

Université de Rennes 1 - IETR

27 PUBLICATIONS 129 CITATIONS

SEE PROFILE



Olivier Romain

CY Cergy Paris University

219 PUBLICATIONS 1,823 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



SmartPose - Systems for Assisted Living [View project](#)



Cyclope [View project](#)

Experimental interfacing with the iPhone 6s through its PCIe communication bus

Mohamed Amine Khelif^{1,2}, Jordane Lorandel¹, Olivier Romain¹

¹ETIS Laboratory UMR 8051, CY Cergy Paris University, ENSEA, CNRS, F-95000 Cergy, France

²ESIEE-IT, 8 rue Pierre de Coubertin, 95300 Pontoise, France

{mohamed-amine.khelif, jordane.lorandel, olivier.romain}@ensea.fr

Abstract—One of the issues to perform hardware attacks on wired communication protocol is the physical access to the bus. Considering the iPhones, PCIe is used as a communication bus between the SoC and its non-volatile memory. This communication can be targeted by a MitM attack in order to access personal information. In this paper, we propose a physical way of interfacing between the motherboard and the non-volatile memory of an iPhone 6s. This was achieved by reverse-engineering the memory in order to retrieve the footprint and the pinout, defining a protocol to safely extract and resolder the memory, without altering its content, and multiple tests to validate the approach. The results obtained allow us to consider the fabrication of an interposer in order to realize a real hardware MitM and to exploit a large possibility of attacks such as real-time data analysis, data-replay, shadow-copy, and so on.

Index Terms—Hardware security, Man-in-the-Middle, PCIe, smartphones, Apple iPhone.

I. INTRODUCTION

Mobile Phones, and in particular Smartphones are widely adopted, with 6.4 Billion users worldwide in 2021 [1]. These devices became a part of our life, as used as a daily companion, keeping our personal information such as messages, photos, agenda, and more.

In iPhones for example [2], the non-volatile memory contains all the user's personal data as well as critical security data such as encryption keys or the password attempts counter. Usually, the stored data is encrypted by a dedicated cryptocyte in the SoC.

All this information including user and security data is exchanged through communication buses making access to such content a real threat, even if the communication is encrypted. In the state of the art, there are some hardware attacks targeting internal communication buses of smartphones or IoT devices such as USB [3], I2C [4] or even Apple's proprietary bus used until iPhone 6 [5]. Since the iPhone 6s, Apple has started to use PCIe as the communication protocol between the Processor and the non-volatile memory express (NVMe).

Thus, our approach consists of implementing a hardware MitM attack on this particular type of communication bus. The other advantage is that MitM can be performed on any iPhone or device using PCIe as a communication bus with the requirement to adapt the hardware interface to the targeted device. The considered hardware attack is one of the less exploited in the state of the art, while it is very promising

as it is the only one that allows direct access to data and, in addition, offers a wide attack vector possibilities including data replay, traffic analysis, and data corruption.



Fig. 1. Man-in-the-Middle principle [6].

In [7] and [8], a versatile hardware MitM architecture capable of interfacing with PCIe and three practical MitM attack scenarios was presented: packets log and filter, packets log and corruption, and shadow copy of all the data transmitted through the PCIe bus in real-time. These scenarios were developed and tested on FPGA used as a smartphone emulator. After this, work the remaining question is: how to Physically interface a MitM FPGA between the SoC and the memory of an iPhone 6s?

Apple uses in these iPhones many proprietary chips that are specially developed for its devices. In order to perform a hardware-based MitM attack on the PCIe bus, it is essential to obtain as much information about the target as possible and validate its accuracy through testing. To make the hardware MitM possible, the following challenges appear:

- Define a protocol to safely unsolder and solder the memory, without altering its content.
- Recreate the footprint and the pinout of the memory chip.
- Analyze the impact of an interposer on iPhone operating.
- Define the specifications for the interposer daughterboard, to be compliant with both the smartphone and our FPGA board.

II. PRELIMINARY WORK

In order to interface with PCIe bus, we will need to perform preliminary works on the motherboard and reverse-engineering the Memory.

A. Memory Footprint and Pinout

Here we will show the logical process followed to recreate Apple's NVMe VLGA U1500 chip under Eagle software through the realization of the footprint and pinout of the chip from information at our disposal.

Footprint: Due to the size of the chip and in order to be able to measure as accurately as possible, several methods exist

based on cameras or binoculars. In our case, we used an X-ray tomography with manual measuring tools, which allowed us to have approximate measurements but still enough precision to obtain the following results.

Pinout: Apple's iPhone 6s uses an NVMe memory chip U1500 (70 pads) according to the VLGA standard derived from the LGA standard (Land Grid Array). There are 3 manufacturers supplying Apple with these chips: Toshiba, Sandisk, and SKhynix. In the naming convention of the pads [9], there are several types of LGA chips but none corresponds to the chip used by Apple and which must be certainly a proprietary fingerprint. However, the pinout must respect the standard of LGA pin naming. Also in the LGA chip standard [9], the 52 pads chip is the closest to the iPhone 6s VLGA chip. It has the same positioning of the pads for those present and gives an idea of how the convention works. The pins are assigned to the fingerprint according to their coordinates present in the schematics. In the case of the iPhone 6s, the unofficial schematic is available online and contains the NVMe memory schematic.

The measurements obtained by X-ray tomography and the pinout defined make possible the creation of a chip in Eagle software. A new library has been created for the Apple NVMe VLGA U1500 memory which contains the schematic of the component, the PCB footprint, and a device file that allows linking the schematic to the footprint in order to have the pinout represented on the PCB.

Two PCBs were made in order to be able to do the first tests, to validate the measurements of the footprint and the pinout, and also to have an estimation of the resiliency for adding extra lines of a few centimeters to the existing data PCIe line. The PCBs are two-layer with metalized vias. As the objective of these PCBs is to perform preliminary tests and for tools limitations we restricted ourselves to only two layers PCBs and we did not take into account the length of the lines for the same differential pair since the main objective here is not to recover the PCIe packets but just the validation of the reverse engineering performed. The first PCB we made is composed only of metalized vias and has the same size as the NVMe chip. The main purpose of this PCB is to elevate the memory footprint on the mother board above the surrounding passive components, thus making easier the positioning of larger PCBs. The second PCB is a flexible one that is responsible for transferring communication signals between NVMe and the motherboard such as power supply signals, clock lane, and a PCIe lane (RX0 and TX1) in order to validate the feasibility of our approach. It will be positioned between the memory and the first PCB.

III. TEST INTERPOSER

Now the objective is to define a precise, reliable, and reproducible protocol for unsoldering and resoldering the memory and/or deporting it without damaging it or altering the stored data.

A. Memory extraction and insertion

Memory extraction: For protecting the components of their smartphones, Apple encloses them with an underfill that is solid at room temperature and soft at high temperatures. This underfill is notably present on the passive components around the memory as well as between the memory and the motherboard. This underfill must first be removed using a scalpel and hot air tool at 250°C before unsoldering the memory. Otherwise, it is highly probable that components at the edge of the memory will be pulled out during the NVMe chip extraction. Several tests were also performed to remove this underfill with chemicals. However, the most efficient solution is to use hot air to soften it and then gradually cut with a scalpel into the space between the memory and the components around it. When the underfill around the memory is removed, it is possible to unsolder the chip without the risk of damaging other components. However, because of the presence of underfill also between the memory and the motherboard that holds it in place, it is required to apply a leverage force on the component when the tin is fully melted. To do this, it will be necessary to define the right heating temperature and exposition time to extract the memory. A too high heating temperature and/or a too localized at one point and the pads will melt (may also damage the memory or its content), a too low heating temperature, not uniform, and/or not long enough and the pads will be ripped off.

Re-solder the memory: In order to be able to solder the memory on its motherboard, it will be necessary to first re-ball the chip with tin. For this purpose, it is possible to use specific stencils, which are specially designed for a chip. In our case, we used a more general method which is manual reballing. This method with a bit of experience allows us to have an equivalent result, with a homogeneous amount of solder on all the pads. It will be necessary to use a hand hot air gun to heat as homogeneously as possible the component previously positioned on the motherboard while applying a slight vertical pressure to hold it in place. Once the soldering is done, an X-ray tomography was systematically done to check the quality of the contacts and the absence of short-circuits due to an excess of tin.

Interposing a PCB : Two incremental tests were carried out to validate the possibility of interposing a PCB without altering the communication between the board and the NVMe.

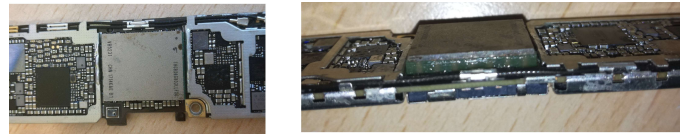


Fig. 2. iPhone 6s NVMe elevation using custom PCB.

Figure 2 shows how the first PCB was integrated between the memory and the motherboard. We used two tins with different melting temperatures in order to realize this manipulation. Finally, this PCB adds 2 mm distance between the

NVMe and the motherboard and the smartphone still works perfectly.

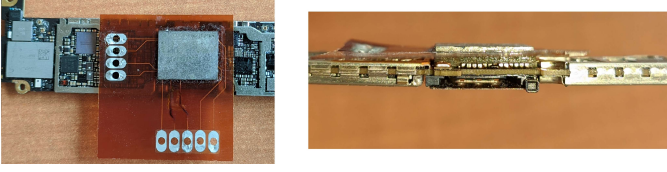


Fig. 3. iPhone 6s NVMe signal deportation using custom PCB.

The second version consists of the addition of the first PCB and the flex PCB between the memory and the motherboard of the iPhone 6s. Ideally, three tin temperatures should be used to integrate the PCBs into the smartphone. In our case, we only had access to two temperatures so the flexible PCB is a better solution in comparison to a rigid one. The result is shown in Figure 3. The welds are checked by X-ray tomography in order to validate that the contacts have been properly realized.



Fig. 4. iPhone 6s with a test interposer between the motherboard and its memory.

Once this part is completed, the smartphone is booted to check if it is still functional and that there is no overheating due to potential short circuits. As you can see on Figure 4, The iPhone starts normally and apparently without loss of data due to our interposer.

IV. MEASUREMENTS RESULTS

To measure the signals that are transferred using our interposer, we used the best oscilloscope available to us: a Teledyne LeCroy WaveMaster 804Zi-B 4GHz with three ZD1000 1GHz active differential probes. The active differential probes prevent adding perturbations to the communication while connecting to the data lanes. Neither the oscilloscope nor the differential probes go high enough in frequency to allow a proper acquisition of PCIe signals.

Even if the recovered signals are not usable, we can still validate the pinout performed since we got the right power supply values, clock reference signal, and PCIe lane on each pad. With Figure 5, we can see that the clock is activated just before communication, which is coherent with the behavior of memories in smartphones in order to save battery life. We can also see that the frequency of the PCIe bus reference clock on the iPhone 6s is 24MHz, which is lower than on computers, defined at 100MHz.

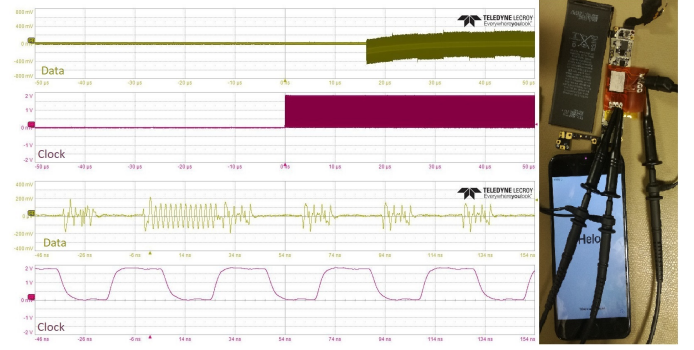


Fig. 5. Clock and data signals recorded from a real smartphone.

V. WORK IN PROGRESS MITM INTERPOSER

The objective is to develop an electronic card allowing the interception of PCIe communications for passive analysis (Sniffing) or active processing of communication on the fly (MitM). This interface will be composed of a flexible PCB that will be placed between the NAND chip and the motherboard of the iPhone 6s, and a daughter-board that will be connected to the smartphone via the flexible circuit. The daughter-board will be in charge of carrying out the necessary processing to allow the FPGA board to be interfaced.

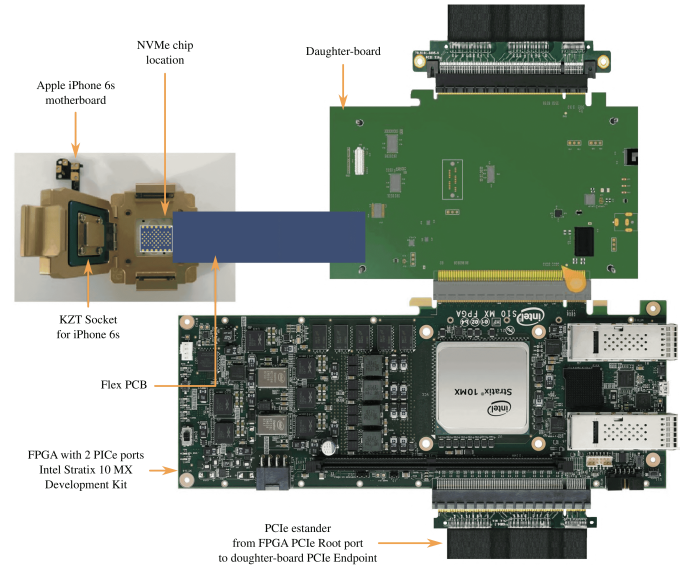


Fig. 6. Illustration of the MitM setup.

Figure 6 illustrates the setup to interpose an FPGA between the memory and the iPhone motherboard. To do this, we will use a KZT socket that will reconnect the memory to the motherboard using pogo pins instead of resoldering it. A flexible PCB will be in charge of redirecting the signals to the daughter-board that will take in charge the signal conditioning and routing to 2 PCIe gen3 x16 ports. Finally, the FPGA will be connected to the daughter-board using their PCIe ports and will be in charge of realizing the MitM and the different scenarios developed as in [7] [8] [10]. In this case, it is an

Intel Stratix 10 MX Development kit, which embeds 2 PCIe ports gen3 x16 as the daughter-board.

The Flex PCB locally connects all power supplies and transfers all signals including power supplies to a robust and high performance (15.5 GHz/ 31Gbps) SAMTEC ST4 60 point connector. The Flex uses the footprint and pinout realized during the reverse engineering phase. All the signals go back and forward on it except the power supply signals. This will allow switching between sniffer and MitM mode.

The Daughter-board ensures the isolation of the smartphone from the motherboard and affects all the signals to test points. The necessary control signals are sent to the FPGA. PCIe signals are routed according to the positioning of dedicated switches. This allows having both sniffer and MitM modes with the same daughter-board. In sniffer mode, the signals are looped back after the reception buffers. These buffers are used to transfer a copy of the signal to the FPGA, without altering the communication between the processor and the memory. In MitM mode, the lanes from the processor (RootComplex) are simply routed to the Root connector on the board. Signals coming from the memory are routed to the EndPoint connector. This configuration will permit to have the FPGA physically located between the memory and the SoC meaning that all the PCIe communication traffic is going through the FPGA.

The first versions of the daughter-board and the flex circuit are currently being manufactured.

VI. PERSPECTIVES AND FUTURE WORKS

With this MitM setup, we will be able to study the PCIe communications in real-time with more evolved algorithms which is impossible for now due to the lack of information. The information obtained through the sniffer mode will be used to create a dataset of iPhones communications between the SoC and the NVMe chip. With this dataset, we will be able to perform offline analysis of the communication between the CPU and the memory especially during the boot phases and during password updates. Performing this statistical analysis will show us the low occurrence events that could be related to the password attempts counter (limit of 10 attempts in iPhones) and help to locate more or less precisely the sensitive data in the memory. Other methods of information mining have to be investigated and compared in order to determine the best approach that can be done for our case of study: offline analysis or online analysis. Especially online methods, which will be more efficient if the location of the counter in memory is modified at each update. The hardware implementation of these algorithms on the FPGA target is also a challenge especially knowing the performance that must be achieved by the architecture to perform on the fly analysis with respecting PCIe protocol constraints. On the other hand, the MitM mode will be used to test and validate the attacks developed in previous works [7] [8] [10] such as traffic analysis, data replay, and a new approach that we propose and which is based on Intel's shadow copy technology. This hardware MitM will give us access to a large attack vector that could make

possible locating sensitive data or security mechanisms from the iPhones 6s.

VII. CONCLUSION

In this article, we discussed the problem of the physical interfacing of a MitM between the NAND chip and the motherboard of an Apple's iPhone 6s. An entire methodology of reverse engineering was done. It consists of creating the memory pinout and the footprint of the iPhone 6s proprietary NAND, defining a reproducible, reliable, and precise methodology to extract safely the memory. Moreover, several test PCBs were manufactured in order to validate the feasibility of the approach. These steps allowed us to prove the possibility of interfacing and transferring PCIe lanes without corrupting the behavior of the smartphone during the boot process and after. This, let us suppose the good integrity of the communication between the NAND and the SoC, even with the interposer. These tests, also permit obtaining more information about the clock frequency of the iPhone 6s PCIe bus. The final step of this work consists of the MitM interposer which is already developed for its first version and is currently being manufactured. The advantage of this method and the development that we are doing is that recent iPhones still use the same technologies and our approach can be applied easily to more recent devices at the expense of designing a new flexible PCB to adapt to the considered chip.

REFERENCES

- [1] Statista, "Number of smartphone users from 2016 to 2021," 2021, accessed: 2022-02-14.
- [2] Apple, "ios security ios 12.1," Apple Inc, Tech. Rep., 2018.
- [3] B. Lau, Y. Jang, C. Song, T. Wang, P. H. Chung, and P. Royal, "Mactans: Injecting malware into ios devices via malicious chargers," *Black Hat USA*, vol. 92, 2013.
- [4] M. A. Khelif, J. Lorandel, and O. Romain, "Non-invasive i2c hardware trojan attack vector," in *2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. IEEE, 2021, pp. 1–6.
- [5] S. Skorobogatov, "The bumpy road towards iphone 5c nand mirroring," *arXiv preprint arXiv:1609.04327*, 2016.
- [6] M. A. Khelif, J. Lorandel, O. Romain, M. Regnery, D. Baheux, and G. Barbu, "Toward a hardware man-in-the-middle attack on pcie bus," *Microprocessors and Microsystems*, vol. 77, p. 103198, 2020.
- [7] —, "Toward a hardware man-in-the-middle attack on pcie bus for smart data replay," in *2019 22nd Euromicro Conference on Digital System Design (DSD)*. IEEE, 2019, pp. 230–237.
- [8] M. A. Khelif, J. Lorandel, O. Romain, M. Regnery, and D. Baheux, "A versatile emulator of mitm for the identification of vulnerabilities of iot devices, a case of study: smartphones," in *Proceedings of the 3rd International Conference on Future Networks and Distributed Systems*, 2019, pp. 1–6.
- [9] R. . Open NAND, "Flash interface specification," 2020, online, <http://www.onfi.org/specifications>.
- [10] M. A. Khelif, J. Lorandel, and O. Romain, "Hardware man-in-the-middle attacks on smartphones," *Forensic Science Today*, vol. 6, no. 1, pp. 012–015, 2020.