Peertechz


CLINICAL GROUP

Forensic Science Today

DOI: https://dx.doi.org/10.17352/fst

Research Article

# Hardware Man-in-the-Middle Attacks on Smartphones

**Mohamed Amine Khelif*, Jordane Lorandel and Olivier Romain**

Laboratoire ETIS UMR 8051, CY Cergy Paris Universite,´ ENSEA, CNRS, F-95000 Cergy, France

**Received:** 17 April, 2020
**Accepted:** 27 April, 2020
**Published:** 28 April, 2020

***Corresponding author:** Mohamed Amine Khelif, Laboratoire ETIS UMR 8051, CY Cergy Paris Universite,´ ENSEA, CNRS, F-95000 Cergy, France, Tel No: +33 7 82 56 78 79; E-mail: mohamed-amine.khelif@ensea.fr

**ORCID:** https://orcid.org/0000-0001-9511-6038

**Keywords:** Forensic; Smartphones; Security; Hardware; Manin-the-middle; PCIe

https://www.peertechz.com



## Abstract

With the democratization of smartphones, law enforcement agencies are increasingly faced with the necessity of extracting data from criminal devices. Several vulnerabilities can be exploited to extract these data, but they are usually quickly fixed by a software update as soon as they are discovered by the manufacturers. We propose a new hardware/protocol based attack targeting data communication bus of a smartphone. This attack is more robust to countermeasures, and allows to have a real-time access to the data exchanged for further processing.

## Abbreviations

AES: Advanced Encryption Standard; EM: Electro-Magnetic; FPGA: Field-Programmable Gate Array; GPU: Graphics Processing Unit; M2M: Machine-to-Machine; MitM: Man-in-the-Middle; NVM: Non-Volatile Memory; NVMe: Non-Volatile Memory express; OS: Operating System; PCIe: Peripheral Component Interconnect Express; RAM: Random-Access Memory; SoC: System on a chip SSD: Solid-State Drive; UFS: Universal Flash Storage; UniPro: Unified Protocol; USB: Universal Serial Bus; WLAN: Wireless Local Area Network

## Smartphone in the iot ecosystem

With the arrival of 5G, a lot of communicating devices will be spread in our daily life environment. As indicated by Cisco's annual report [1], the number of overall connected devices will reach 29.3 billion by 2023 in comparison to 18.4 billion in 2018, with a 10% annual growth. In all these devices, smartphones will represent around a fourth of all these devices, among personal computers, laptops, TVs, tablets, M2M devices, etc. They are one of the most privileged ways of accessing internet nowadays. In 2019, the number of smartphone users reached 3.5 billion [2], which represents half of the world population. Such numbers enforce the particular interest of government agencies in smartphones and the amount of information they represent.

All these connected devices are very complex and dispose of increased computing power, a large memory storage capacity, and an improved wireless and wired connectivity. These devices are commonly used in our daily life, able to execute diverse applications, and in the same time, they collect and store a lot of personal data. This is also the case for many other electronic devices related to e-health, smart home, etc. Security represents one of the main issue in future systems built around such devices.

When considering smartphones, several levels of security exist, including software and hardware mechanisms. These solutions developed by the manufacturers themselves are voluntarily kept secret, preventing reverse engineering and simple communication with the device by a third party. Even if these devices already own sophisticated security protections, they still represent a valuable source of information for forensic experts, during their crime scene investigations. Mainly, because of the huge amount of personal data, including SMS, phone calls, GPS positions, contacts, photos, that can be very useful to solve criminal cases or cold cases.

One of the most known examples is the legal tussle between the FBI and Apple in 2015, for which the FBI had finally obtained the data contained into an encrypted iPhone 5 C belonging to the San Bernardino killer. Apple had been reticent to provide the federal agency a tool for accessing the data, prompting the FBI to find another method to extract the information from



**Citation:** Khelif MA, Lorandel J, Romain O (2020) Hardware Man-in-the-Middle Attacks on Smartphones. Forensic Sci Today 6(1): 012-015.
DOI: https://dx.doi.org/10.17352/fst.000016

the smartphone. They finally used a zero-day vulnerability discovered by a professional hacker, to bypass the passwords attempts counter and its 10 tries limitation to unlock the phone and access the data.

As such devices become more and more complex, this complexity is, in some way, a source of vulnerability. Smartphones are now composed of several hardware and software elements, provided by many different suppliers. They also integrate a lot of wired and wireless communication elements based on multiple standards. All these considerations make the security a challenging issue to solve. This is also a critical task for leading companies to be able to ensure a high level of security of their devices, from the design phase and all along the product life.

Figure 1 illustrates the evolution of the number of detected vulnerabilities for Android and iOS devices. This reveals the increasing number of security breaches as well as their publication, which is probably linked to the willingness of identifying and disseminating security issues to a large community, with the aim of developing more secure smartphones. It can be seen than more vulnerabilities have been revealed for Android devices than iOS devices, probably due to a more drastic security policy and BlackBox strategy privileged by Apple.

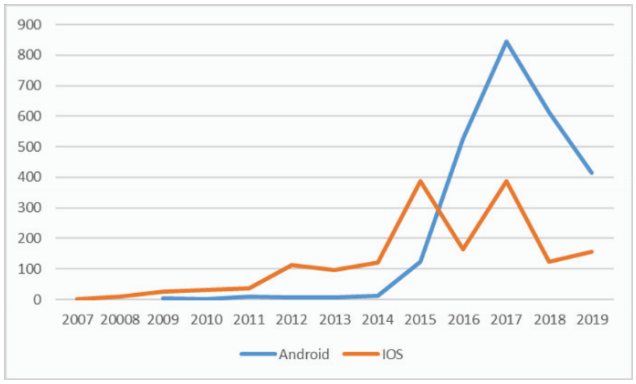


**Figure 1:** Vulnerability Trends Over Time [3].

## Vulnerabilities of smartphones

The architecture of a smartphone is based around a lot of generic components, including a system-on-chip (SoC), exchanging data with volatile and non-volatile memories, a baseband, and a WLAN engine for wireless connectivity, and some sensors, display, and power management units. The SoC, itself, integrates an application processor, a graphical processing unit (GPU), a crypto-processor, and some cache memories. Figure 2 illustrates this generic architecture, showing the type of communication protocol used in recent devices.

This architecture is subjected to different types of attacks, reported in the literature. We classified them into three main categories, respectively software, hardware, and protocol attacks.

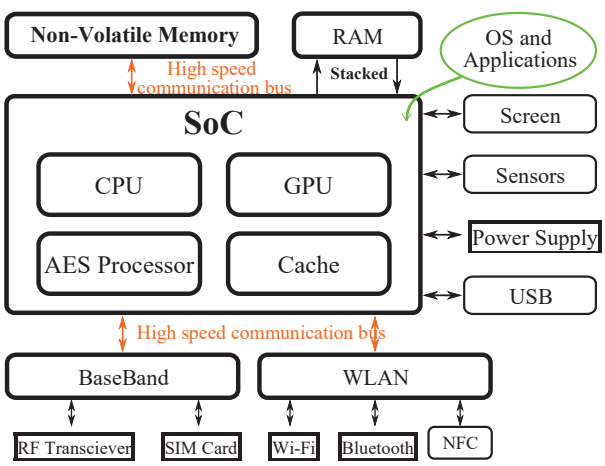


**Figure 2:** Generic Architecture of Smartphone.

Software attacks [4], also known as malware, allow an attacker to steal data from a device or even take control of it by exploiting vulnerabilities in the Operating System (OS) or thirdparty applications. These attacks include several types, e.g. viruses, spyware, trojans, rootkits, and key loggers. Malware will often combine several of them in order to accomplish its purpose. Countermeasures for these attacks can be done through an antivirus or a software security updates for the OS and the apps.

Protocol attacks include all attacks on wired and wireless communication protocols. Regarding smartphones, Wi-Fi [5], Bluetooth [6], NFC [7] and USB [8], are the most targeted technologies. However, the attacker needs to be present in the operating range of the protocol. These attacks exploit vulnerabilities related to the implementation of the protocol stacks. Software security updates are the main countermeasures used to patch the vulnerability.

Considering hardware attacks, two types exist [9], namely invasive and non-invasive for the device, including sidechannel attacks, physical tampering attacks, fault injection attacks, and instruction skipping attacks. Other attacks like EM eavesdropping on display [10] have also proven to be a real threat for data security. Hardware attacks are very difficult to implement compared to the previous ones, but on the other side, they do not depend on a vulnerability to be effective. Countermeasures are also much more complicated since it usually requires a hardware update which is only available at the next-generation release of smartphones.

In the forensic field, law enforcement agencies are increasingly confronted with the problem of extracting data from locked smartphones, which can belong to an arrested criminal or to the victim found at a crime scene. The main advantage of forensic agencies is that they have physical access to the evidence and can, therefore, use any type of attack previously presented especially hardware attacks.

Emerging solutions have been proposed to combine several types of attack with the objective to benefit from the advantages of each one. For example, an hybrid attack was proposed [11],



**Citation:** Khelif MA, Lorandel J, Romain O (2020) Hardware Man-in-the-Middle Attacks on Smartphones. Forensic Sci Today 6(1): 012-015.
DOI: https://dx.doi.org/10.17352/fst.000016

which consists of physically interfacing with an internal data bus and interfering the communications in real-time using the same protocol. The hardware part of the attack consists of being able to physically access sensitive data while being invisible from both communication sides, and without triggering any potential security mechanism. For forensic experts, they could thus access sensitive data on any device compatible with the defined' communication protocol.

## Discussion

As the computing power of smartphones is constantly increasing, new high data rate communication standards are used for internal communication between chips, to meet the low latency and high bandwidth requirements of new applications. For example, recent smartphones are now integrating a new generation of storage devices based on Solid-State Drive Non-Volatile Memory express (SSD NVMe) technology with PCIe as the physical communication protocol. The latter was initially used in personal computers, to meet a high level of performance for massive data exchange between the processor, the memory, and the graphical units.

Regarding the newer generation of smartphones, all personal data, operating system, and apps are stored in the NVM. This memory communicates directly with the SoC through their serial data bus. Accessing the content of this memory, even encrypted, represents an opportunity for forensic experts. Two types of NVM are used in recent smartphones: the Universal Flash Storage (UFS) with UniPro bus and the Non-Volatile Memory express (NVMe) with PCIe bus. It is important to notice that NVMe memory and the PCIe bus are also widely used in many other connected objects and computers, and, in many application domains, representing a large area of potential targets.

In the case of unencrypted memory, forensic experts have the possibility to unsolder the chip and read it. All the memory content is then directly exploitable [12]. However, with the latest generations of smartphones, many security mechanisms have been proposed, most often based on data encryption. For example, a dedicated AES processor is directly integrated into the SoC to encrypt all sensitive data, password attempt counters using a unique encryption ID key fused in the AES processor. This strategy is very powerful, preventing most of the attacks.

Nowadays, several companies such as Cellebrite, MSAB or GreyShift provide data extraction and analysis solutions based on existing software vulnerabilities for the specific targeted smartphone. The durability of these attacks mainly relies on the confidentiality of the exploited vulnerabilities at the risk of being corrected by a software update.

In [11,13], a man-in-the-middle (MitM) approach was proposed at the interface between SoC/NVMe communication through PCIe bus. Figure 3 illustrates the principle of the approach. From our knowledge, there is no work dealing with a hardware MitM attack on smartphones targeting the PCIe bus. The main advantage of this approach is that the attacker will act as an undetectable router between the two communication peripherals by exploiting the PCIe protocol. In the case of non-encrypted data, the attacker will have direct access to communications in real-time. If the data are encrypted, the Man-in-the-Middle architecture can perform more evolved attacks such as traffic analysis, data corruption or replay data to identify and take advantage of sensitive data like password attempts counter.


**Figure 3:** Man-in-the-Middle principle.

To perform this attack the hacker needs to, first, interface between the SoC and the NVMe by reverse-engineering the motherboard of the smartphone. The second step is to use the dedicated material to perform real-time analysis of the communications between the components, detect sensitive data, and take control of the device without being detected by smartphone's security. As PCIe is a widely used technology, this type of attack could be applied to many chips, currently available off-the-shelf.

For smartphone, this attack is not limited to SoC/NVMe communications but can also be performed on SoC/BaseBand and SoC/WLAN communications since the same protocol is used. The only limitation is to be able to physically interface the bus.

As a summary, smartphones support now a wide range of communication capabilities that could be the target of multiple attacks, in order to create a known vulnerability or benefit from it. For forensic experts, even if security mechanisms have been developed, hardware MitM allows to make the attacker invisible and to propose a new vector of attack, leveraging smartphone security and sensitive data integrity.

## References

1. Cisco (2020) Cisco's annual internet report (2018–2023) white paper. **Link:** https://bit.ly/3bFO540

2. Statista. Number of smartphone users worldwide from 2016 to 2021. **Link:** https://bit.ly/3bTnXD7

3. Mitre Corporation. CVE Details the ultimate security vulnerability datasource. **Link:** https://bit.ly/3f0PRiv

4. Ahvanooey MT, Qianmu Li, Rabbani M, Rajput AR (2020) A survey on smartphones security: Software vulnerabilities, malware, and attacks. **Link:** https://bit.ly/3cQFVWD

5. Park MW, Choi YH, Eom JH, Chung TM (2014) Dangerous wi-fi access point: attacks to benign smartphone applications. Personal and ubiquitous computing 18: 1373-1386. **Link:** https://bit.ly/2VH04ZC

6. Babamir SM, Nowrouzi R, Naseri H (2010) Mining bluetooth attacks in smart phones. In Filip Zavoral, Jakub Yaghob, Pit Pichappan, and Eyas El-Qawasmeh, editors, Networked Digital Technologies, Berlin, Heidelberg 241–253. **Link:** https://bit.ly/2xTfykk



**Citation:** Khelif MA, Lorandel J, Romain O (2020) Hardware Man-in-the-Middle Attacks on Smartphones. Forensic Sci Today 6(1): 012-015.
DOI: https://dx.doi.org/10.17352/fst.000016

7. Chen CH, Lin IC Yang CC (2014) Nfc attacks analysis and survey. In 2014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. 458-462. **Link:** https://bit.ly/2yJkwAb

8. Lau B, Jang Y, Song C, Wang T, Chung PH, et al. (2013) Mactans: Injecting malware into ios devices via malicious chargers. Black Hat USA. **Link:** https://bit.ly/2W1Pz1Z

9. Tehranipoor M, Wang C (2011) Introduction to hardware security and trust. Springer Science & Business Media. **Link:** https://bit.ly/3bCBlex

10. Elibol F, Sarac U, Erer I (2012) Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In 2012 Proceedings of the 20th European Signal Processing Conference (EUSIPCO) 1767-1771. **Link:** https://bit.ly/3cRRCwl

11. Khelif MA, Lorandel J, Romain O, Regnery M, Baheux D (2019) Toward a hardware manin-the-middle attack on pcie bus for smart data replay. In 2019 22 nd Euromicro Conference on Digital System Design (DSD) 230-237.

12. Amin R (2019) Demystifying the i-device nvme nand (new storage used by apple). **Link:** https://bit.ly/3eTzhkr

13. Khelif MA, Lorandel J, Romain O, Regnery M, Baheux D (2019) 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 1-6. **Link:** https://bit.ly/3bCA8Ux







**Citation:** Khelif MA, Lorandel J, Romain O (2020) Hardware Man-in-the-Middle Attacks on Smartphones. Forensic Sci Today 6(1): 012-015.
DOI: https://dx.doi.org/10.17352/fst.000016