Case Report Article

Journal of Current Trends in Computer Science Research

Smart phones surveillance methods

Christos P. Beretas

*MSc, Ph. D - Professor and Head of Cyber Security department of Innovative Knowledge Institute (Paris Graduate School), Paris, France.

*Corresponding Author
Christos P. Beretas, MSc, ph. D - Professor and Head of Cyber Security department of Innovative Knowledge Institute (Paris Graduate School), Paris, France.

Submitted: 25 Jan 2023; **Accepted**: 03 Feb 2023; **Published**: 07 Feb 2023

Citation: Beretas, P., B., (2023). Smart phones surveillance methods. *J Curr Trends Comp Sci Res*, 2(1), 01-06.

Keywords: smart phones, surveillance, monitoring, mobile networks, security, privacy

Introduction

Smart phone surveillance is a sensitive issue, so topical and important, which is about everyday life of all of us, I am talking about the smart phones, small smart phones, these small but powerful computers that everybody use them everyday by doing more internet browsing rather than doing calls. The questions that arise about the security of smart phones are many, for example: may someone watch us? may the government hear what we saying and what messages we send? may they know our location? How much important **meta-data** is and to what extent it can reveal important information about the subscribers identity and how it relates to privacy and personal data. Finally, it is worth mentioning the participation of mobile phone providers in various government monitoring projects of the citizens either with targeted software which is not detectable, or with the direct access to the Servers of the providers for copying sensitive information without of course the consent of the subscribers. Such projects are the **Carnivore, Prism, and other projects**, and the countries involved in information exchange programs are behind lists identified as **5 Eyes, 9 Eyes, and 14 Eyes.**

Surveillance Methods

When referring to a smart phone surveillance, refer to 6 spy methods, which are:

1. Signal interception & MITM attack.
2. Hardware circuit.
3. Spy phone application.
4. Use of specific software for Servers.
5. Meta-data analysis.
6. Government monitoring projects.

Case 1:

On this case, requires expensive equipment that is not legally sold on the market to be purchased by an interested customers, there are various approaches to low-cost material, but these tapping systems are cumbersome and complex in their operation, also may consider that the advent of 4G / 5G networks that offer more security than the old 2G / 3G these cheap eavesdropper devicese partly useless, say in partly because should consider that in smart phones devices in the choice of the network allows the following option 5G / 4G / 3G / 2G which means that where there is no 5G / 4G network coverage the smart phone will operate on the 3G / 2G network and this is a security hole as the network is over vulnerable to cheap type of interceptor devices since the 3G / 2G network encryption algorithm provide low security. An expensive stolen state equipment would also be useless since its use keys that should be renewed regularly. Thus, state-owned services that have legal co-op equipment have the ability to make legitimate signal interception, here at this point, someone might think of this, an employee who has access to the system could be tapping someone else phone? the answere is aware of it. Legally singnal interception systemss are divided into 2 categories, those located in central buildings where sometimes require the assistance of the telecom provider and the base stations where, depending on the needs of the service, they move.In both of the above categories, the subscriber does not realize the monitoring of his / her telephone line or the interception of the transmitted data. In the first category in which data interception is involved the telecommunications company the process is the easiest and simplest as extract information directly from the Servers. In the second category, which is popular in the secret services, mobile base stations are used which are used at close distances from the target victim. base station to proceed with data collection. The target victim does not perceive the difference in communication as the deceptive base stations are added to the network with a normal antenna ID so as not to affect the quality of communication or services so that the target victim understands the monitoring.

Detecting deceptive mobile base stations can be detected with specialized software, but most of them are not detected as they appear as transponders and not as communication antennas and even if they have received a normal antenna ID. Once a successful connection to a monitoring system is achieved, or with a deceptive mobile base station, the information extraction as well as the sending of commands to the mobile phone begin, where it is indicated, recording conversations, copying messages, modifying messages, browsing websites, receiving emails, collecting messages from network messaging applications, locating, opening the camera, and opening the microphone. These practices are commonly used to support criminal evidence in courts or in cases of terrorisn and national security. Figure 1.1 shows a deceptive mobile base station.

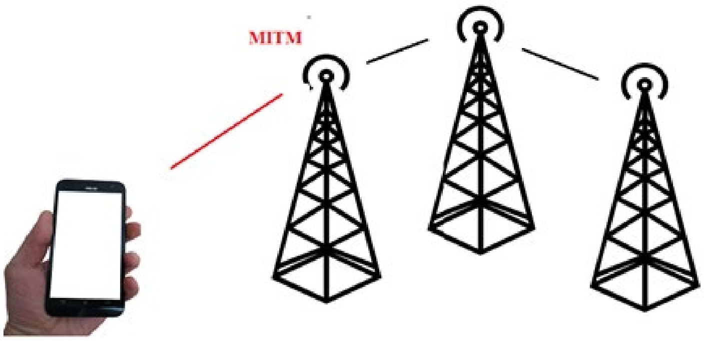

Figure 1.1 – Deceptive Mobile Base Station

Case 2:
On this case, could be said to be based on the ignorance of the subscriber, at this point say ignorance because in this case the smart phone has to be opened and a micro chip is placed inside, which will collect everything while the phone will be send it back to the target-victim person. Device data usage either when the smart phone is in close proximity to a mobile transceiver, the connection is made and the data is transferred. Detecting such a micro chip is very difficult, and with the breakthrough of Internet of Things this technology is evolving. That's why we need to buy smart phones from trusted places, also a smart phone that is a gift from someone is an easy way to deceive, but not always. Under no circumstances should be considered safe and reliable a sealed cell phone that is in its original jelly in brand new condition, just simillar as the ones cell phones selled in stores. This is a practice of the secret services, when there is a restriction on access for data mining in other ways, for the success of the mission there is usually cooperation with some traders so that the desired modified device falls into the hands of the target victim in such a way that perceived by the target victim. Even if the target victim somehow realizes that their communications are being monitored he / she will focus on either switching network providers or buying a new SIM card under another name from the same or different network provider, the most likely scenario is to use the same mobile device as the suspicion that the mobile phone device is modified will hardly cross his / her mind, on the one hand due to lack of knowledge and on the other hand he / she bought the device sealed from a store. The success of this method is based on this logic.

Case 3:
On this case presented the simplest and most widespread, based on the naive and ignorant of the target victim about the security and use of smart phone and applications. Some security tips are:

- *Do not leave the smart phone exposed to third parties.*
- *Use lock screen application.*
- *Keep both operating system and software applications updated.*
- *Use antivirus software with real time protection enabled, keep the antivirus database updated.*
- *Do not use VPN software.*
- *Do not install APK files from unknown sourcs.*
- *Do not ROOT your smartphone.*
- *Do not use software apps with low reputation.*
- *Do not open messages that do not know.*
- *Do not click hyperlinks that do not know.*
- *Do not open files from strangers.*
- *Smart phones are not as safe as you may believe.*

Generally, the signs that a smart phone is being taped are:

- *The battery discharge quickly after data is being used continuously, so check the applications. It can also be a coincidence.*
- *Interrupting calls while talking, also this could cause by interference in the connection, automatically changing location while trying again to set the correct location but still changed may be interference only at that specific area.*
- *Noise during speech, this is a sign of a interference, but keep in mind that with professional signal interception devices there is no noise, also the noise someone may hear may be either a device damage or is from Interference.*
- *The smart phone is warm, this meaning several processes are running.*
- *The smart phone crashes and becomes slow, this is due also to other reasons, depending on the smart phone and depending on the monitoring software sometimes the monitoring software is "heavy" and the smart phone can not respond.*
- *Text messages that are received by irrelevant numbers, messages that have been sent, and the recipient has received a different message than than the one that have been sent should be suspected of monitoring or network interference that may be due to other infections.*
- *The smart phone works alone and does not turn off. Surveillance spy software do not allow the user to have full control over the device for the simple reason that they are trying to keep the spy software on the device.*
- *Removal of software apps are not permitted or this operation is disabled.*
- *There is mysterious activities in social media networks which tere is access from the infected smart phone, also, my sterious activities may occur in mobile apps of exchanging messages.*

- *Nothing from the above.*
-

The above are the few rules that apply, continue reading.

- *Surveillance software do not appear in installed applications.*
- *Resetting to factory settings may not permanently eliminate the surveillance software.*
- *Scrambled applications are easily localized, while well-designed applications run on Stealth Mode and are extremely difficult to detect even with anti-malware software.*
- *A smart phone surveillance software can be downloaded to the smart phone through another application.*
- *Modern surveillance software is very difficult to detect while also provides no annomalies with operating system.*
- *Smart phone ROOTING makes easier the installation and proper use of surveillance software.*
- *A amart phone which its operating system is updated will prevent from the installation of various surveillance software which is installed into smart phones by using various well known security holes.*

Case 4:
In this case, the well-known Pegasus spyware is introduced. Pegasus is a spyware software for smartphones that install on iOS, Android, Blackberry O / S and any other Android O / S based operating system (custom Android versions). This software has interesting features both in the way it is installed on the target smartphones and the possibilities it offers to its operators. The target victim first receives an SMS with a link if then the target victim by clicking on the link then the smart phone becomes infected with Pegasus. In the previous pages among the security tips it has been mentioned that the operating system must be updated, the reason is that to install Pegasus on a Smartphone it exploits zero-day vulnerabilities of the operating systems, which means that an updated operating system from alone is not able to deal with Pegasus, so additional security measures are required, such as a very reliable antivirus / antispyware with application installation lock capabilities and avoiding ROOT may to some extent prevent the installation or smooth operation of Pegasus. Once Pegasus is installed on the target smartphone, then the ability to fully control the smartphone begin with capabilities to monitor and record phone calls, read emails, take screenshots, record keystrokes, generally have the general management of the Smartphone in to such an extent that the remote Pegasus operator has physical access to the Smartphone. As expected from such software with huge capabilities, it is an expensive, complex software that remains installed on the smartphone completely invisible, undetectable even by antivirus and antispyware. The specific software is used when there is a need to monitor important people and personalities, it is not used for monitoring children as parental control software for example or for low important purposes of low interest.

At this point it is worth noting **two things**, the first is that in darknet there are lists of zero-day vulnerabilities that can be used to create software spies similar to Pegasus. The second is that Pegasus is a software that is constantly updated and new features are added. An important peculiarity of its innovation is the way of installation which changes, as it has been mentioned above for the installation of the software the target-victim receives a link via SMS, this is the basic way of installation, but there is also an invisible way of installation, in this case the target-victim does not realize the existence of SMS nor do require by someone to click on a link to install Pegasus, because it is possible exploitation of zero-day security vulnerabilities that allow Pegasus to install on the target-victim's smartphone without the target-victim realizing anything. This is one of the features that makes Pegasus software so special.

Case 5:
Meta-data is everywhere in our electronic activities, meta-data is also present in the non-digital world. For the implementation of an activity or the execution of a service - function presupposes the execution of various functions which will be used to complete a process. All these processes that are required for the completion of a service - function in each stage of their implementation are accompanied by a significant number of data which is necessary for the completion of the final process. The data that is transferred and processed at each step of the implementation is of great and special importance-value, both because they contain important personal information and because determine the activities of mobile subscribers. Mobile telephony service providers that participate in government information exchange of meta-data programs distribute the meta-data content to government agencies for analysis. The secret services have the ability to process meta-data to a large extent. To create profiles with the habits of each subscriber. The meta-data collection can of course be performed with the cases mentioned above. The collection and analysis of meta-data is very important and the information extracted can be more important than the information itself. The reason is that neta-data contains subscriber information which contains:

- *Mobile network code.*
- *IMEI of Smartphone.*
- *Device location.*
- *Subscriber code.*
- *Frequency of manipulations.*
- *Social media preferences.*
- *Duration and frequency of calls.*
- *The destination of the calls.*
- *Duration of internet usage.*
- *Frequency of visits to websites.*
- *Frequency of use of the telephone.*
- *Determining the country of operation of the telephone.*
- *Determining the use of the mobile telephony antenna.*
- *Frequency of telephone connection per antenna.*

The above are some of the informationthat can be extracted from the meta-data. This information can be used as a first step before implementing a cell phone tracking method. It is worth noting at this point, the use of a simple non-smartphone mobile phone significantly reduces the chances of tracking, as there is a significant limitation to the use of tracking methods, while from the point of view of the created mta-data, eta-data is clearly less in terms of the size of the value of the information. The government services, and especially the secret services, are able to know about the information circulating in the interior of the country, the secret services that are active in the collection and analysis of information abroad (foreign intelligence) are able to know in globally the information that is circulated as meta-data, how this is done will be mentioned below.

Is important advantage of meta-data is the sale of information that can be extracted for advertising purposes, it is not uncommon for subscribers to accept calls by marketing companies to promote their products, when subscribers ask narketing companies where they found their phone numbers they answer that the subscribers themselves subscribed to information lists, someone else wrote them on their behalf, knowing that this is not the case, they just try to calm the subscriber by reassuring them that they have not received their contact details illegally extracting information from meta-data.

Meta-data is also created by mobile antena towers, these meta-data include subsecribr connections from antenna to antenna, the distance of the subscribers from the antenna, the data transferred, and other useful information that needs analysis, which I further analysis will reveal other sensitive information.

Case 6:

On this case presented the biggest threat regarding data security and privacy in the digital world is that the majority of data transferred on the Internet is not encrypted well, the existing security infrastructure in an environment of not well encrypted information must be considered totally inadequate. Not well encrypted communication means the government easy may have access to intercept any information. Government agencies and organizations knowing the telecommunication weaknesses, information intercepted by subscribers from offensive websites, the non-encrypted information, not well encrypted information, VPN servers that offers fake anonymity that is essentially Honey Pot systems with examples the secret services who collect information from the servers inside in the country or third countries that participating in the **PRISM** project.

Security agencies have access in data of any internet and smartphone subscribers in the world. This practice on several countries is legal and is based on **several privacy protection laws** This laws gives the freedom to governmental agencies to store and to process huge amounts of data without exception if these people are criminalized or not. The **PRISM** project became quite popular and reinforced worries of the world on the violation of privacy and data. The Project **PRISM** named after the word outlet means mirror - reflection and this is because the data pass through an internet node continue their route but the items are copied (reflection) from the **PRISM** project without harming their quality neither have been some form of alteration to worry the subscriber that something is wrong. Below in **Figure 6.1** is an simple example of Project **PRISM**.

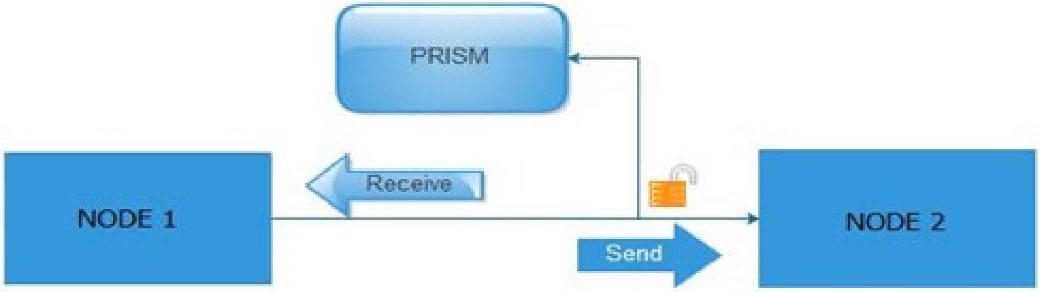

Figure 6.1

As shown in the figure above, to make a data breach between nodes the data must be copied without the subscriber knowledge. Usually this makes it coherent with telecoms operators and other services that there are active subscribers. All of the above would be useless if there was not the necessary data mining tool and statistical tests, called **XKEYSCORE** by pressing a few keys are able to know everything related to a human, such as telephones, e-mails, habits, searches has done in search engines, behaviors, internet of Things activities **(IOT)** and of course building electronic profile **“e-profile”**. The security services have advanced already on potential networking devices controls and firewalls of known companies manufacturing such devices. The **XKEYSCORE**, used in conjunction with another program called **TURBULENCE**, the **TURBULENCE** are two subsystems the **TURMOIL** and TURBINE. Briefly mention that **TURMOIL** is an information collection system of satellite and cable communications, while TURBINE unleashes attacks on serial systems (Greenwald, 2015). From the above could not be missing collection of information from social media, Cookies, Internet services, Internet of Things, etc. Once the target is locked: the next step is the **QUANTUMTHEORY** attacks and **QUANTUMNATION** which will give full control of the remote device, even is a smart phone, Internet of Things, computer, or anything else. In **Figure 6.2** shows how is working the intermediary fake Server.

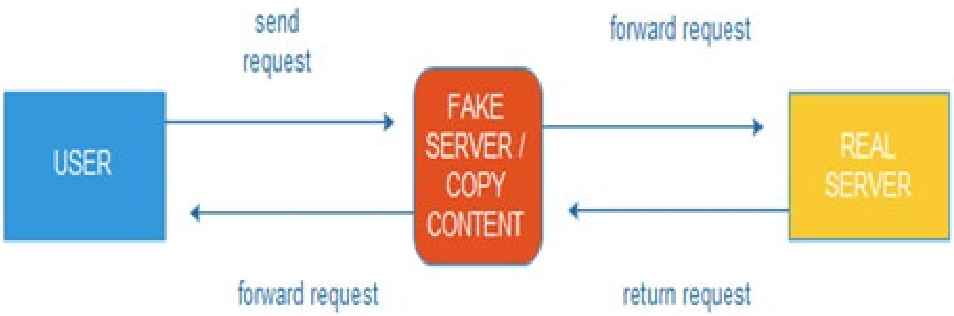

Figure 6.2

The data collection and processing is performed by each device connected to the Internet, the mobile network providers collect personal data transferred to Servers of their infrastructures, telecommunications providers know all about digital life and human conversations, applications for smart phones collect personal data and data about subscribers behavior. Imagine a Smart phone devices which will send personal data to the manufacturer or other organizations and then those organizations to have remote access to Smartphome and opened the camera, or perform real time data analysis. Many automated bot trying to break different kinds of access codes to gain access. interception of data is shown in **Figure 6.3** and **6.4** below.

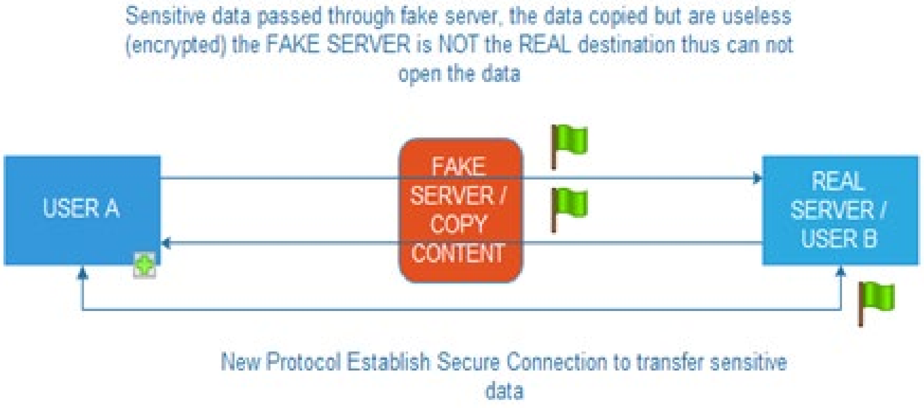
Sensitive data passed through fake server, the data copied but are useless (encrypted) the FAKE SERVER is NOT the REAL destination thus can not open the data
USER A
FAKE SERVER / COPY CONTENT
REAL SERVER / USER B
New Protocol Establish Secure Connection to transfer sensitive data

Figure 6.3

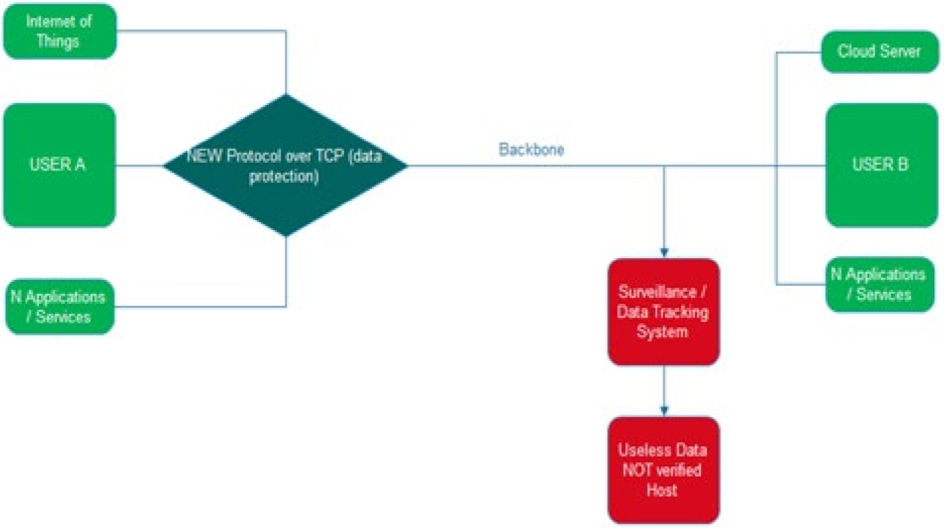
Internet of Things
USER A
N Applications / Services
NEW Protocol over TCP (data protection)
Backbone
Cloud Server
USER B
N Applications / Services
Surveillance / Data Tracking System
Useless Data NOT verified Host

Figure 6.4

A smartphone that work exclusively on 4G / 5G and not in 2G / 3G networks would be the best option. No security method can prevent the monitoring of a smartphone, as long as the subscriber tries to protect his / her smartphone, as the methods presented in this chapter are practically impossible, even if the subscriber uses an old mobile phone device no that is, a smartphone. No cell phones and no security methods should be considered secure, subscribers should consider their smartphones to be insecure and that their activities are not confidential, even if point-to-point encryption communication applications are used.

Refferences

1. Glenn Greenwald. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Picador; Reprint edition, 2015.
2. Christos Beretas. Research in Medical & Engineering Sciences, 2018.
3. Christos Beretas. Internet of Things and Privacy. Journal of Industrial Engineering and Safety, 2018.
4. Christos Beretas. How Really Secure is TOR and the Privacy it Offers. Nanotechnology and Advanced Material Science, 2020.
5. Christos Beretas. Cyber Hybrid Warfare: Asymmetric threat. Journal of Nanotechnology and Advanced Material Science, 2020.