The use of smartphones in surveillance

Esmeralda Kadëna

Doctoral School on Safety and Security Sciences, Óbuda University, Budapest, Hungary

kadena.esmeralda@phd.uni-obuda.hu

Abstract: Over the years, the surveillance methods have become more and more sophisticated. Countries always keep a close eye on their citizens' activities and rivals to ensure safety and security. Now we are living in the era of internet where everything is connected and smart gadgets are used to gather information. Smartphone has become a popular spying tool and we are faced with a growing concern, mass surveillance. This work aims to explain how smartphones can be compromised and how the use of them as spying tool is causing threats to human rights.

Keywords: Smartphones; Surveillance; Threats; Human rights.

1 Introduction

Spying, the secret gathering of intelligence has been practiced for thousands of years. Many have called it as the second profession oldest in the world. Spies have proved themselves to be highly inventive when wedging their secret war while the human element of spying has remain essentially the same. Today the cutting edge of espionage relies on every technological breakthrough of the 20th century from satellites to lasers to DNA testing. Methods of spying have become sophisticated and invasive and they can pose threats to the right of privacy.

One of the earliest references of espionage comes from "The art of war", a book on military strategy written more than two thousand years before by Sun Tzu, a Chinese philosopher [1]. According to Tzu, a hundred ounces of silver spend for information may save ten thousand spend on war. The tricks of the trade evolved into a codified body of knowledge known to its practitioners as tradecraft. It evolves any aspect of the activity as a spy to obtain information that can include secret privacy codes, surveillance, etc., and all of these have been collected and refined over the years by every nation.

As far back as Roman Empire, military leaders grappled with the question of how best to transmit messages over vast distances. If the information was confidential, emissaries were forced to either memorise it or to communicate in a form of letter code writing [2]. One of the biggest inventions appeared at the end of World War I, Enigma machine invented by the German engineer Arthur Scherbius to protect confidential communication and designed to automatically generate new and highly complex code up to three times per day [3]. Military and government services of several countries, especially Germany, adopted and used it before and during World War II. In order to break Enigma, Alan Turing specified and developed an electromechanical machine called the "Colossus" which was believed to be the first mechanical computer [4].

Over the years, the surveillance methods became more and more sophisticated. Now we are living in the era of internet where everything is connected. Countries and specific agencies now are using smart gadgets to gather information. Among them is the most popular, smartphone.

2 Smartphone as a spying tool

Smartphone has become an attractive spying tool for many reasons. At first smartphones are gaining a lot of popularity. Everyday life of people is connected with them and attackers are taking advantage. We are used to take smartphones everywhere and due to their features they have the capability to capture everything we say, see and to track every movement of us. What is more, they are increasingly becoming a hub to access and control also other devices paired with sensors and that collect data such as Internet of Things (IoT) devices. This combination make them a perfect tool to gather information.

Another reason is due to their technological features such as sensors. Microphones now have the capability to capture every word even the voice in conversation is too low. Usually they are equipped with two cameras, high definition. All smartphones are using radio frequencies like cellular, Wi-Fi, Bluetooth and GPS in order to provide information about location that can be used to track the users' location and to record all their movements. Furthermore smartphones software and hardware ecosystem is very complex with many layers. Each of the elements and layers of the system can be "victim" of attack vectors and malicious actors. Actually each layer is protected but is very difficult to manage the threat when the higher layers are at risk.

One of the biggest challenges are people, as the weakest link in the security chain. When attackers are looking to gain access to a device they will take advantage

from users' behaviour. People may not be aware enough about the risks that the use of smartphone brings. For instance they may download a wrong application (like apps not from official stores, clicking on the wrong link, opening the wrong email, etc.) and because of these wrong practices, might happen that the attackers can have control on their microphones, cameras and radio frequencies information as well.

To achieve an effective cybersecurity an essential factor is the management of information systems risks [5]. Lack of the tools available to detect, analyse and protect from these vulnerabilities is also a significant concern. There are practices related to applications policies, data encryption and searching for system anomalies. But sometimes this is not enough and the exact solutions yet do not exist [6].

2.1 Smartphones' risks

Smartphones' risks lean on threats, vulnerabilities and impacts of the attacks and can be classified as follows [6]:

- *Threats:* It is about who is attacking, people that execute possibly attacks. They are generally classified in five categories. The first are criminals who intent to obtain money through theft or fraud. In the second group are included spies, their intention is to steal confidential, private and secret information from governments as well as from private sector. Then in the third group are warriors on nation and state level. There are focused on improving qualifications on this field to attempt attacks in support of the strategic objectives of the state. Next are "hacktivists", their motivation to perform attacks is not monetary but political and social reasons. The last but not from the importance, are terrorists. They perform cyberattacks as a non-state form or warfare sponsored by the state.

- *Vulnerabilities*: This term is related to the weaknesses that hackers are attacking as a fight between them and defenders. Information and communication technology systems are very complex and on they have to face with attackers continuously search for weakest points of the systems. On the other side defenders fight for protecting against these critical points but very often have to deal with challenges. As the most problematic can be considered: unintended or with purpose acts by people known as insiders that are authorized to access the system; vulnerabilities of supply chain that can allow inclusion of malwares and the last ones are zero-day vulnerabilities or previously unknown. Even the countermeasures for vulnerabilities are known, sometimes is difficult or impossible to be implemented because of the lack of funds and actions.

- *User-based risks* [7]*:* Not technical attacks and directed to users. They are made through "social engineering" and aim to reach into private information [8]. The first challenge to protect the right to data protection today is related with the "volunteered" data, particularly through the rise in wearable devices and social media networks [9] .

2.2 Areas that can be comprised

- *Applications (Apps):* such as mobile browsers, messaging apps, platforms and official stores can be all compromised. As a result intruders can gain illegitimate access to mobile devices and legitimate apps may deceive in their collection of data [10]. For instance spywares are used to collect information and data regarding a target subject by specifying their usage is for advertising and promotional purposes (adware) or to offer better service to users (cookies), while they collect information about a person/organization and send to someone else without their permission) [6].

- *Operating systems (OS):* there are different kind of vulnerabilities within operating systems that can control a smartphone. For instance, in 2015 CIA aimed to steal Apple's secrets [11] and two attack campaigns against Android were discovered in 2016; one dedicated on rooting Androids OS ad gaining access to Google Gmail, Docs, Drive, accounts and the second one that aimed to steal information and to send messages [12].

- *Firmware/carrier:* it is possible that firmware/carrier can be hacked invisible to protections at the OS or application layer. Fake mobile phone towers (IMSI catchers) can inject malicious code or stand between the communication of the target and the real service provider's tower (man-in-the-middle: MITM attack) [13], [14]. The use of them from police has caused international headlines. In Norway they were not only used improperly but also used to spy the government itself [15]. The problem was that while they were searching for one number during the same time were collecting a hundred numbers. In New York, IMSI catchers have been used more than a thousand time by police since 2008 [16].

- *Hardware/Chips:* Code inside the hardware, i.e. clipper chip [17] developed by the United States National Security Agency (NSA) for the National Institute of Science and Technology (NIST) or printed circuit boards can be modified during manufacturing. By replacing the legitimate ones, can provide attackers control of compromised parts [18].

3 Mass surveillance

The major part of our daily life is stored on smartphones and due to the changes in technology, agents and hackers have been using the devices we pay for. Over the last years, it has not been so necessary for them to follow and spy us physically. Intelligence agencies dedicate people, money and time to the target and we can think it is possible that they can gain access on everyone smartphone, laptop, IPad or any smart gadget [19]. Thanks to the available technology and hacking methods, they may have control over the contact list, messages, phone conversations, where the phone is physically located. People tend to not really care about the privacy because most of these are happening invisibly. Everything and everyone can be spied through phone calls, such as conversation, from where and when they are talking. As a result, now investigators can know much better, when someone left his/her house, where and when he/she went, who he/she set with, how long he/she stayed and so on. This is called metadata.

3.1 Related events

In 2013 Edward Snowden leaked details of massive government surveillance programs [20]. Since then a raging debate initiated over digital privacy and security. That debate came to a head in 2016, when Apple refused an FBI court order to access the iPhone of alleged San Bernardino terrorist. Meanwhile, journalists and activists have been under attacks from foreign agents. Is it possible for people to truly protect sensitive information? FBI argued on the court that Apple has the exclusive technical means to get into mobile phones but according to Snowden results, that was possible without the help of Apple [21].

A joint CIA/NSA project called “Shenanigans” [22] was to mount on airplanes an IMSI catcher and fly it around the city. They can tell when the target person have travelled and when he moves. It was happening in Yemen aiming the missiles at terrorists. But usually these programs has a tendency and can move from war front to home front. After 6 months was reported by Wall Street Journal that the same technology is used domestically in US. FBI has an aviation unit flying around cities monitoring protesters instead of violent criminals. But spying technology is used also against state activists like in case of Shehabi who was target of the FinSpy malware emails and became a victim of government surveillance. The malware aim was to turn on the camera and microphone.

Mass surveillance is becoming a big concern. In US during the last years, news highlighted the possibilities of collecting data of Americans from NSA [23]. Foreign intelligence surveillance act (FISA) [24] authorises the secret courts to green light domestic spying programs. In the fundamental law was not mentioned

anything about metadata and collecting records on law abiding people. Furthermore reports claimed that NSA's mass surveillance programs do not have a track record to prevent the attacks [25].

3.2 Threats to human rights

In a Big Data world, mass surveillance is posing threats to private lives of citizens and freedom among political activists and journals. The surveillance practices are putting in risk the fundamental human rights in democracy: the rights to privacy [26], freedom of information and expression [27], the rights to a fair trial [28] and freedom of religion [29]. If the juridical control is inadequate the violation of these rights also jeopardizes the rule of law. National law should allow the collection and analysis of metadata only if the person will be consent or if the following court order granted on the basis of reasonable suspicion of the target being involved in criminal activity otherwise everything unlawful should penalised.

A lack of proper legal regulation and technical protection at the national and international level, and its effective enforcement was shown. Data protection laws existed in most western countries but limited in terms of regulation of "personal data" and the enforcing existing mechanisms for these regulations were insufficient in the majority of cases [30], [31]. In order to ensure creditability, control mechanism can enforce the national and international legal framework. The law in most states provides some protection for the privacy of their own citizens, but not of foreigners. The Snowden files have shown that the NSA and their foreign partners, in particular among the "Five Eyes" partners (United States, United Kingdom, Canada, Australia, New Zealand) circumvent national restrictions by exchanging data on each other's citizens [32]. There is a need for transatlantic cooperation in the fight against terrorism and other organised crime forms [33] and for cooperation based on trust and on respect for human rights and the rule of law.

Schuster et.al argue that there is a need to strength the basic structure of the internet and to policies addressing software and hardware vulnerabilities and weaknesses of the Internet architecture should be improved [34]. Despite efforts in the field of quality assurance, most hardware and software products and services still include many vulnerabilities that can be exploited. Security measures should be included in the design from the starting point [35]. If malicious practices will be taken into account during the design phase they will not only prevent vulnerabilities but can also reduce their impact. Putting more emphasizes in increasing the use of algorithms to predict upcoming crimes can help on preventing the consequences [36].

From 25th of May 2018 to make consistent data privacy laws across Europe, will take effect the General Data Protection Regulation (GDPR) [37]. Organisations are enforced to look at potential vulnerabilities where sensitive data could be lost or exploited. However, the framing of data protection as a right appears to have imposed much greater obligations on private actors than most other human rights. Under GDPR is required that system designers must take into account human right when developing new products and this might be difficult from their part. As regards international data transfer, GDPR updates legal obligations with new concepts but no massive changes are presented over provisions in the DPD (Data Protection Directive) [38]. EU data protection law can be seen in the lights of limitations as it does not provide emendation for non-EU citizens and only data subjects in the EU are under protection of the GDPR [39]. Nevertheless, user based attacks will be always present and people should be conscious about the risks that the use of smartphones poses.

Conclusions

As the number of smartphones, their functionalities and application scenarios increases and hence also the amount of data stored on them, it is interesting and important to understand the risks that brings the use of them. In this paper was shown that due to their features and capabilities, they are a convenient tool to be used in surveillance. Everyone should be aware of the smartphones' risks, whether legally (by user-based attacks), or illegally (by attackers look to compromise a smartphone). Mass surveillance is posing threats to fundamental human rights in democracy. Data protection and internet security are a necessity for people's safety while the main challenge is about the peoples' data that can be easily found.

Finding the right balance between the interests protected by the right to data protection and the effects coming from attacks will continue to be a subject of debate. The proper legal regulation and technical protection at the national and international level should take place in every organisation. In a changing global order, there is a need to strengthen the realisation of the right to data protection as a fundamental human right.

References

[1] S. Tzu, "XIII: The use of Spies," in *Art of War*, Leicester , Allandale Online Publishing, 2000, pp. 59-62.

[2] R. M. Sheldon, Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages, Jefferson, N.C: McFarland & Co, 2003.

[3] S. Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Knopf Doubleday Publishing Group, 2011.

[4] cryptomuseum.com, "History of the Enigma," 30 September 2017. [Online]. Available: http://www.cryptomuseum.com/crypto/enigma/hist.htm.

[5] Joint Task Force Transformation Initiative, "Managing Information Security Risk: Organization, Mission, and Information System View," National Institute of Standards and Technology, Gaithersburg, 2011.

[6] H. Bidgoli, "Volume III: Threats, Vulnerabilities, Prevention, Detection and Management," in *Handbook of Information Security*, New Jersey, John Wiley & Sons, Inc., 2006, pp. 146-165.

[7] R. J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., Indiana: Wiley Publishing, Inc., 2008.

[8] Symantec, "2016 Internet Security Threat Report," Symantec Website Security, 2016.

[9] D. Lyon, "Surveillance, Snowden, and Big Data: Capacities, consequences, critique," *Big Data & Society,* pp. 1-13, 2014.

[10] P. Ruggiero and J. Foote, "Cyber Threats to Mobile Phones," Carnegie Mellon University for US-CERT, 2011. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/cyber_threats_to_mobile_phones.pdf.

[11] J. Scahill and J. Begley, "The CIA campaign to steal Apple's secrets," The Intercept, 10 March 2015. [Online]. Available: https://theintercept.com/2015/03/10/ispy-cia-campaign-steal-apples-secrets/.

[12] K. Jackson Higgins, "Androids Under Attack: 1 Million Google Accounts Hijacked," Darkreading, 30 November 2016. [Online]. Available: https://www.darkreading.com/endpoint/androids-under-attack-1-million-google-accounts-hijacked-/d/d-id/1327604. [Accessed February 2018].

[13] M. Apuzzo and M. S. Schmidt, "Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say," The New York Times, 15 November 2016. [Online]. Available: https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html.

[14] imsicatcher.org, "A comprehensive Guide to How IMSI Catchers Work," Imsi catcher organisation, [Online]. Available: http://imsicatcher.org/imsi-explained/.

[15] A. B. Foss and P. A. Johansen, "New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service," Aftenposten, 26 June 2015. [Online]. Available: https://www.aftenposten.no/norge/i/kamWB/New-report-Clear-signs-of-mobile-surveillance-in-Oslo_-despite-denial-from-Police-Security-Service.

[16] J. Goldstein, "New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says," The New York Times, 12 February 2016. [Online]. Available: https://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html.

[17] D. E. Denning, "The Case for Clipper (Clipper Chip offers escrowed encryption)," Encryption_policies.tripod.com, September 1995. [Online]. Available: http://encryption_policies.tripod.com/us/denning_0795_clipper.htm.

[18] A. Greenberg, "How a Bug in an Obscure Chip Exposed a Billion Smartphones to Hackers," WIRED, 27 September 2017. [Online]. Available: https://www.wired.com/story/broadpwn-wi-fi-vulnerability-ios-android/.

[19] Electronic Frontier Foundation, "Cell-Site Simulators/IMSI Catchers," EFF.

[20] M. Hosenball, "NSA chief says Snowden leaked up to 200,000 secret documents," REUTERS, 14 November 2013. [Online]. Available: https://www.reuters.com/article/us-usa-security-nsa/nsa-chief-says-snowden-leaked-up-to-200000-secret-documents-idUSBRE9AD19B20131114.

[21] E. Levitz, "Obama administration: No pardon for Edward Snowden," MSNBC, 28 September 2015. [Online]. Available: http://www.msnbc.com/msnbc/obama-administration-no-pardon-edward-snowden.

[22] J. Scahill and G. Greenwald, "The NSA Secret role in the U.S assassination program," The Intercept, 10 February 2014. [Online]. Available: https://theintercept.com/2014/02/10/the-nsas-secret-role/.

[23] G. Kessler, "James Clapper's 'least untruthful' statement to the Senate," The Washington Post, 12 June 2013. [Online]. Available: https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html?utm_term=.c773c0da10e8.

[24] fas.org, "Foreign Intelligence Surveillance Act," FAS, 3 May 2017. [Online]. Available: https://fas.org/irp/agency/doj/fisa/.

[25] J. McLaughlin, "U.S. Mass surveillance has not record of thwarting large terror attacks, regardless of Snowden leaks," The Intercept, 17 November 2015. [Online]. Available: https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/.

[26] ECHR-COE, "European Convention of Human Rights," European Court of Human Rights - Council of Europe, Strasbourg.

[27] ECHR-COE, "Article 10, European Convention of Human Rights," ECHR-COE, Strasbourg.

[28] ECHR-COE, "Article 6, European Convention of Human Rights," ECHR-COE, Strasbourg.

[29] ECHR-COE, "Article 9, European Convention of Human Rights," ECHR-COE, Strasbourg.

[30] A. M. Arnbak, "Securing private communications: Protecting private communications security in EU law: fundamental rights, functional value chains and market incentives," 2015. [Online]. Available: https://pure.uva.nl/ws/files/2703068/166342_Securing_Private_Communications_PhDthesis_Arnbak_def311015.pdf. [Accessed January 2018].

[31] OECD, "Report on the cross-border enforcement of privacy laws," OECD, 2006.

[32] C. Nyst and A. Crow, "Unmasking the Five Eyes' global surveillance practices," APC and Hivos, 2014.

[33] P. Omtzigt, "Mass Surveillance," Committee on Legal Affairs and Human Rights, Strasbourg.

[34] S. Schuster, M. . van den Bergb, X. Larrucea, T. Sleweb and P. Ide-Kosticc, "Mass surveillance and technological policy options: Improving security of private communications," *Computer Standards & Interfaces,* vol. 50, pp. 76-82, 2017.

[35] J. Cowie, "The New Threat: Targeted Internet Traffic Misdirection," ORACLE+Dyn, 19 November 2013. [Online]. Available: https://dyn.com/blog/mitm-internet-hijacking/. [Accessed April 2018].

[36] M. de Goede, "The politics of privacy in the age of preemptive security," *International Political Sociology,* vol. 8, no. 1, pp. 100-104, 2014.

[37] European Parliament and Council , "General Data Protection Regulation (GDPR)," 2016. [Online]. Available: https://gdpr-info.eu/. [Accessed February 2018].

[38] T. Bräutigam, "The Land of Confusion: International Data Transfers between Schrems and the GDPR," *University of Helsinki Faculty of Law Legal Studies Research Paper Series,* pp. 140-177, 19 December 2016.

[39] E. Perotti, "The European Ruling on the Right to Be Forgotten and Its Extra-EU Implementation," *World Association of Newspapers and News Publishers (WAN-IFRA),* pp. 1-45, 2015.