Utilizing Cellular Infrastructure for Spying of Smart Phones

Sheikh Riyaz ul Haq
Department of Computer Science
Jamia Hamdard (Hamdard University)
New Delhi-62, India

Syed Imtiyaz Hassan, PhD
Department of Computer Science
Jamia Hamdard (Hamdard University)
New Delhi-62, India

ABSTRACT

Smart phones form essential part of our daily lives and remain almost always with us or in our close vicinity. They act as an interface for very crucial and personal information like images, videos, voice calls, video calls, downloaded media, text messages, call logs, banking transaction details, passwords etc., thus housing very large amount of private information which can provide deep insight into the personality of the concerned person and thus can be of pivotal importance for Secret service and law enforcement agencies. We have proposed a new Surveillance scheme utilizing the existing Cellular Infrastructure to monitor and extract the information from the blacklisted smart phone devices i.e. devices of terrorists, corrupt politicians, hard core Criminals, drug dealers etc. We will review several attacks over the Smart phones via Communication channels in order to provide the insight for using the Cellular Infrastructure for the purpose of Surveillance and extraction of information from the Blacklisted Smart phone devices and for conducting those very attacks. Surveillance and extraction of information via Cellular infrastructure would be capable of providing both live feedbacks (like ongoing conference(in the vicinity of Smart phone device), ongoing voice/video call, present location etc.) as well as the information contained in the Smart Phone device's memory (including Downloaded media, Images, video Call logs, e-mails, passwords, credit card numbers etc.).

Keywords

Blacklisted smart phones, Spying of smart phones, Attacks over Communication Channels, Surveillance.

1. INTRODUCTION

Smart Phone devices have become omnipresent [1], as their number exceeds the count of PC's plus PDA's combined together [2] and is further increasing exponentially, thus most of the human beings whether criminals or not possess at least one Smart phone device. These smart phones are being used not only for communication purposes but for the storage and processing of data as well. The data stored in the smart phones can be categorized into three categories [3]:

a)User generated information (including pictures, audio, videos, maps, GPS waypoints, files stored, stored voice mails, list of connected computers).

b) Internet related information (online accounts, e-mail, Internet usage, social networking Information, purchased media).

c) Installed Third party applications (Substitute messaging and communication systems).

Thus the data present within these devices can prove to be a gold mine for Investigating and Law enforcement agencies. Smart phones, in short, are a wonderful technical innovation, but they also provide a terrific opportunity to spy over people [4].

Smart phones communicate with the Base Transceiver station (BTS)/Node B by means of radio waves which are logically divided into two parts namely control channels (Signaling channels) and traffic channels [5]. Traffic channels carry the information (data, voice) to and from the mobile station to the rest of network, while as control channels provide a medium to transmit control information .Our aim is the consideration of the fact that the mobile devices which are blacklisted or possess the blacklisted SIM (subscriber identity modules) cards(i.e. SIM of User's with criminal records or of those posing threat to a Nation), these devices can be monitored and the information contained in them can be extracted from the backend (Mobile Switching centre(MSC)/Core network(CN)) whenever the need is felt. The control channels can be used to initiate such process and the traffic channels can be used to carry the extracted information without users consent as shown in Figure 1. Due to advent in the throughput capacity of the cellular networks the data extracted from the devices of blacklisted users like terrorists, corrupt politicians, hard core Criminals, Drug Dealers can be transferred at a very fast rate. However the data extracted from the mobile phone device for acquiring Intelligence should not get reflected in the billing process.

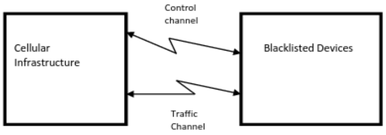

Figure 1. Cellular infrastructure utilizing channels for surveillance and extraction of information (adapted from [15])

The cellular network by means of which these Smart phones communicate has been studied for various possible attacks and vulnerabilities by several researchers. This cellular structure being wireless is vulnerable to several types of attacks by means of manipulating communication channels.

Out of band Control channels influencing sensors of the smart phone devices have been used for initiating attacks by presuming that a mobile malware is already installed in the device [6]. Voice channel has also been used as the covert channel for spreading the malware and for extraction of the information (i.e. data is being converted into the voice before being extracted from the device) [7].The Paging channel has also been used for initiating the Denial of service (DoS) and sleep deprivation attacks [8].

Our aim is to review the various attacks over the Smart phones by means of communication channels in order to provide the insight for using existing cellular infrastructure, for monitoring and/or extraction of the information for legal prosecution of the criminals by the law enforcing agencies as they have law in their favor to such access [9].This could significantly improve the prosecution rate and thus consequently decline the crime rate.

The paper is organized as follows: Section 2 discusses the attacks that have been carried via communication channels over the Smart phone devices and that could be carried utilizing cellular Infrastructure. Section 3 discusses our idea of initiating Information transfer from the Smart phone devices by making use of control Channel and utilizing the high Capacity (UMTS and beyond) of traffic channels for such transfer.

2. ATTACKS BASED ON CHANNELS

Several attacks based on utilizing the communication channels (either in band or out of band) are known to be performed over the Smart phone devices. These attacks are capable of providing stimulus to the Malware already pre-installed in the Smart phone device [6], spreading the malware across several non infected devices [6], covertly transferring the vital Information stored within the Smart phone device [7] and launching Denial of service [8,10] and Sleep deprivation attacks [10]. These attacks are mentioned in Table 1 and the possibility of achieving the same functionality by means of utilizing the Cellular Infrastructure is briefly defined in the corresponding subsections.

Table1. Attacks possible via communication channels

Attacks via communication channels	**Purpose**	**Can same Purpose be achieved via cellular infrastructure?**
Sensor based (out of band) attack	Providing stimulus to the Malware, Spreading the Malware.	Yes.
Voice Channel based Attack	Transforming data into voice for - covert transfer.	Yes.
Signaling Channel based attack	Denial of service, Sleep deprivation.	Yes.

2.1 Sensor Based (out of band) Attacks

Sensors based (out of band attacks) presume that the malware possessing the capability of launching an attack is already installed within the Smart phone device, such a malware is triggered by means of activating one of the several available sensors [6]. Due to the availability of multitude of smart phone sensors (Audio Sensor, Optical sensor, Magnetometer and accelerometer etc.) ,sensor based attacks can be carried out to influence a large number of infected devices, which can even span the international borders by means of Live Sports Events/ Famous TV Programs watched in several countries of the world.

These Sensors based attacks offer a very high degree of covertness and thus are very difficult to prevent, especially if covert and steganographic channels are used, simply because of the fact that malwares are not generally known to be triggered by means of providing input/stimulus to the sensors, enabling them (malwares) to gather sensitive information, learn characteristics of the surrounding environment, eavesdrop over a phone call etc. These malwares can also be commanded and controlled over context-aware out of band channels (acoustic, visual, magnetic and vibration signaling etc.).

If an anti-Malware solution is to be implemented against exploiting sensors, then it has to monitor all the sensors that too constantly, which will drastically reduce the battery life of a Smart phone device thus adding to the concern [6].Several types of Sensor based attacks both steganographic and non-steganographic utilizing the Audio, Magnetic, Optical, Vibration sensors can be used to launch attacks as discussed by [6] are mentioned in Table 2.

Table 2. Sensor based (out of band) attacks

Sensor based attack type	**Purpose**	**Can same Purpose be achieved via cellular infrastructure?**
Distributed denial of service attacks (DDoS)	To Deny any particular service(s)	Yes
Annoyance Attack	To cause Annoyance	Yes
Embarrassment Attack (Selective attack)	To Embarrass	Yes
Safety Hazards	To cause the harm/breach the security	Yes
Interference Attacks	To cause Electromagnetic Interference	Yes
Distraction Attacks	To distract	Yes

2.1.1 Distributed Denial of Service Attacks (DDoS)

The infected devices present in a Specific area (metro station, railway station or an airport) can be used to collectively launch DDoS by bringing down the Wi-Fi network of that area [6].

2.1.2 Annoyance Attack

The infected device can cause annoyance which can even extend to the level of chaos. For Example, in a sports arena an announcement may be used to send covert trigger to all the infected devices present; and then malware on one device can communicate (Sends messages/makes phone calls) with other devices present there thus causing annoyance. The infected devices could also collectively play some loud music thereby causing chaos [6].

2.1.3 Embarrassment Attack

The infected device can be used to cause embarrassment to a specific person or to a group of people present nearby. For example a person may connect his/her phone with the Projector for a presentation in an important meeting. As soon as the person starts or is about to speak, another nearby phone may trigger the malware which would cause to project an embarrassing picture or video onto the screen [6].

2.1.4 Safety Hazards

The infected device may be able to interact with the car's internal network and may cause over acceleration or sudden breaking thus leading to the health hazard of the persons within and outside the car, also the car's steering system may be controlled to specifically kill a particular person [6].

2.1.5 Interference Attacks

The infected device could be used to cause an interference with the surrounding environment. For example, the Malware on the infected mobile devices can be used to interfere (Electromagnetic interference (EMI), Radiofrequency Signals) with the aircraft radio system [11]. Interference attack can also be used to target selective medical devices (pacemakers, Implantable Cardioverter-Defibrillator etc.) used in hospitals [12, 13].

2.1.6 Distraction Attacks

This type of attack could distract the user from performing a specific task which malware wouldn't like to be performed, like when user tries to perform a security task, the malware could cause distraction by playing a ringtone or a song.

The above mentioned attacks are also possible by utilizing cellular infrastructure for providing stimulus to the embedded software/ malware within the Smart phone device by means of Control channel in order to achieve the corresponding functionality out of it.

2.2 Voice Channel Based Attack

Voice channel based attack incorporates the voice channel for spreading the malware and for covertly exchanging the information which is there in the Smart phone gadget by first changing it into voice and afterwards transmitting the same, this type of attack is a feasible one as smart phone manufacturers, cellular network protocol developers do not take into consideration a voice channel as a threat over which information may be leaked, consequently there are lesser security countermeasures to guard the voice traffic as discussed by [7].

The extraction of information from the Smart phone device and its conversion to the voice form is possible via cellular infrastructure. The process will be initiated by the Control channel after successful conversion the information can be carried via Traffic channel.

2.3 Signaling Channel Based Attack

In Signaling based attacks mobile services are disturbed by overloading the control plane resulting in excessive signaling caused by either the malware present in the smart phones [8] or by the misbehaving mobile apps [14].

2.3.1 Paging Channel Based Attack

Paging Channel based attacks is a type of attack carried by manipulating the paging channel (paging channel is a downlink control (or signaling) channel basically, which broadcasts control information to several users within a cell [15] and notifies about an incoming call to a particular user equipment [5]) thus blocking the access of all the devices in a particular paging area as discussed by the [8].

Paging channel attack can lead to the:

a) Denial of service (DoS) attack. The entire paging area could get affected by overloading the paging channel with paging requests thus resulting in the denial of service to the entire users in whole of the paging area [8].

b) Sleep deprivation attack. is essentially the kind of denial of service attack where a device's battery is depleted more rapidly than it would be under ordinary use. The attacker attacks (by means of service request power attacks, benign power attacks and malignant power attacks) the device until its battery power is fully discharged thus achieving the task of making the device inoperable [10].

The Signaling channel attacks over the Smart phone devices for the purpose of sleep deprivation and denial of services by means of cellular infrastructure can be carried via Signaling/Control channels.

3. OVERVIEW OF SURVEILLANCE SYSTEM UTILIZING CELLULAR INFRASTRUCTURE

The system utilizing cellular infrastructure for surveillance and extraction of information from the black listed Smart phone Devices requires Processing and Storage Systems possessing the list of following identities:

a) Blacklisted devices (in terms of IMEI (International Mobile equipment identity))

b) list of blacklisted SIM cards (in terms of IMSI(International Mobile Subscriber Identity)

c)MSISDN (Mobile Station International Subscriber Directory Number)).

The above mentioned identities would be required at the Access Network and the Core Network level. These systems will initiate a transfer from the smart phone devices utilizing cellular infrastructure, process upon and store the processed information for coordination with the ground offensive team of law enforcing agencies in case of the raid or for acquiring evidence against blacklisted users for legalizing charges against them. Such system should be accessible only to the investigating and law Enforcement agencies i.e. the equipments capable of achieving this functionality will be physically isolated at the Access Network and the Core Network level and Investigating and Law Enforcement agencies will be given either the physical access or access by means of Microwave and/or Optical Communication. Figure 2 presents the general overview of such system. Whenever the need arises for surveillance, or for the extraction of information, the Blacklisted User can be traced out by utilizing the cellular infrastructure. When the blacklisted user is located the Control channel can be utilized for initiating the data transfer via the Traffic channel. The blacklisted device will now be uploading the information via cellular infrastructure without user's consent. The Uplink Capacity of such device should be increased during the process then restored to the normal, as the uplink capacity of devices communicating via cellular infrastructure is usually lower as compared to the downlink capacity unless asked for.

The Surveillance and extraction of information from the Black listed devices is possible if an agreement is reached between the Smart phone manufacturers, Telecom operators, International Telecommunication Union, Law Enforcing agencies and last but not the least if there is approval of the common people in terms of laws passed by the Parliament for the same. If such an agreement is possible the blacklisted smart phones of criminals, Terrorists, Corrupt Politicians, Organized Criminal Gangs can be monitored thus necessary information can be withdrawn to tackle any untoward incident or to legalize any charges against them. If the Smart phone Manufacturers do not agree then a Spyware capable of initiating such transfer is required to be installed on the Blacklisted user's device, the Spyware capable of being activated by means of control channel can facilitate such a transfer via the transport channel, whenever required without user's consent.

In fact there are laws in place, in many countries of the world which support the surveillance and possible extraction of the information:

a) In India Section 69B of Indian IT act enables any agency to collect, monitor traffic data/Information generated, stored, received or transmitted by a computer resource (including smart phones)[9].

b) In USA the Communications Assistance for Law Enforcement Act (CALEA) enables the agencies to do the surveillance and possible extraction. [16].

The Smart phone device consists of vast amount of data and possesses several gadgets like MIC, Camera, GPS enabled location determination which can play a pivotal role in information gathering against Blacklisted users. Such a system can be used to provide the live feedback of the blacklisted users as such a system will be capable to listen and thus record a live meeting/conference of the Blacklisted users by activating the MIC thus providing vital intelligence without risking anybody's life, also the camera of the Smart phone device can be activated to capture such incident. The GPS enabled location ability could be activated to know the exact location of such setup.

The Malware capable of being activated by the control channel and capable of interacting with the internal network of Blacklisted user's car can be used to neutralize him/her. Also such malware can be used to cause other forms of attacks like embarrassment attacks, distraction attacks, Inference attacks, Annoyance attacks as discussed by [3]. The Malware capable of being activated by means of the control channel can also lead to the Denial of service as discussed by [14] and sleep deprivation attacks as discussed by [10].

Thus ability to obtain the live feedback like position, ongoing conversation and ongoing movement around the vicinity of the Blacklisted device can serve as a third eye for the ground offensive team, keeping them one step ahead. Also it would be possible to launch pre-emptive attacks like Battery drainage [10], Denial of service [6] to sabotage a particular event.

The contents of the memory will be equally useful if not more than what has been discussed in the preceding paragraphs. The call log list e.g., will provide us the details about the persons with whom the blacklisted user has a concern with, they can be also included then in the Blacklist. The pictures, videos, text messages, e-mails, downloaded media, banking transactions all will prove to be useful for investigating agencies for collecting evidences and thus legalizing charges against the Blacklisted user.

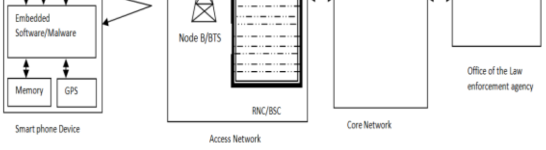

Figure 2. Overview of the Surveillance system employing Cellular Infrastructure.

Utilization of cellular infrastructure for spying of Smart phones would also enable Law enforcement agencies to zero in onto the persons who are indulged in heinous crime of child pornography (in browsing or collection) as per Section 67B of the Indian IT act [9].

Thus Utilizing Cellular infrastructure for surveillance and extraction of information would enable Law enforcement agencies to gather evidence (without user's consent) up untill a point of time beyond which there is no doubt of user's innocence/guilt.

4. CONCLUSION

The Surveillance system discussed in this paper will utilize the existing Cellular infrastructure to carry an attack and to extract the information from the Smart phone device. The Surveillance system will provide an edge to security agencies by keeping them one step ahead of the criminals, thus will prove instrumental in helping to reduce the crime rate and increase the prosecution rate of the criminals. This system cannot be in place until and unless there is collaboration among smart phone manufacturers, telecom operators, International Telecommunication Union, Law Enforcing agencies and last but not the least the willingness among majority of the people to accept this system considering the fact that their privacy is at the stake. Incorporation of such a system will require State of the art technology to be developed and thus to be implemented across the entire Cellular Infrastructure.

5. ACKNOWLEDGMENTS

We thank Ms Karuna yogesh Tsunami and Mr..Sheikh Moeen ul Haque for their support and valuable suggestions.

6. REFERENCES

[1] Lunden, I. (2014). Tech Crunch: Gartner: Device Shipments Break 2.4B Units In 2014, Tablets To Overtake PC Sales In 2015. http://techcrunch.com/2014/07/06/gartner-device-shipments-break-2-4b-units-in-2014-tablets-to-overtake-pc-sales-in-2015/ .

[2] Murtagh, R. (2014). Search Engine Watch: Mobile Now Exceeds PC: The Biggest Shift Since the Internet Began. http://searchenginewatch.com/sew/opinion/2353616/mobile-now-exceeds-pc-the-biggest-shift-since-the-internet-began.

[3] Casey, E. (2011).Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.

[4] Rosenbach, M. (2013). Spiegel Online International: iSpy: How the NSA Accesses Smartphone Data.

[5] Rappaport, T. (2009). Wireless Communications: Principles and Practices. Pearson Education India.

[6] Hasan, R., Saxena, N., Haleviz, T., Zawoad, S., & Rinehart, D. (2013) Sensing-enabled channels for hard-to-detect command and control of mobile devices. In: Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS '13. ACM, New York, pp 469-480.

[7] Aloraini, B. (2014) A New Covert Channel Over Cellular Network Voice Channel. Thesis. Rochester Institute of Technology http://scholarworks.rit.edu/theses/8366 .

[8] Serror, J., Zang, H., & Bolot, J. (2006) Impact of paging channel overloads or attacks on a cellular network. In:

Proceedings of the 5th ACM workshop on Wireless security, WiSe '06. ACM, New York, pp 75-84.

[9] Department of Electronics & Information Technology: Cyber Laws,http://deity.gov.in/content/cyber-laws .

[10] Martin, T., Hsiao, M., Ha, D., & Krishnaswami, D. (2004) Denial-of-Service Attacks on Battery-powered Mobile Computers. In: Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications, PERCOM '04. IEEE Computer Society, Washington, p 309. www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html

[11] Bassen, H. (1998) Radiofrequency interference with medical devices. Technical information statement. IEEE Engineering in Medicine and Biology, 17(3):111-114.

[12] Hietanen, M., & Sibakov, V.: INTERFERENCE IN MEDICAL DEVICES BY RADIOFREQUENCY SIGNALS FROM CELLULAR PHONES. http://www.ursi.org/proceedings/procga05/pdf/KE.4(0944).pdf .

[13] Wong, M., Lim, C., Lee, K., Gouhier, B., & Sparks, P. (2015) MJA: An unusual case of implantable cardioverter-defibrillator inhibition. https://www.mja.com.au/journal/2015/202/6/unusual-case-implantable-cardioverter-defibrillator-inhibition .

[14] Gabriel, C. (2012). Rethink Wireless: DoCoMo demands Google's help with signalling storm. http://www.rethink-wireless.com/2012/01/30/docomo-demands-googles-signalling-storm.htm

[15] Kasera, S., & Narang, N. (2004). 3G Networks Architecture ,Protocols and Procedures. Tata McGraw-Hill Publishing Company Limited, New Delhi.

[16] FederalCommunicationsCommission:https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.