Cyber Attacks Targeting Android Cellphones

Nurhayat Varol
TBMYO
Firat University/Turkey
nurhayat_varol@yahoo.com

Ahmet Furkan Aydoğan
Software Engineering
College of Technology
Firat University/Turkey
furkan.aydogan@hotmail.com

Asaf Varol
Software Engineering
College of Technology
Firat University/Turkey
varol.asaf@gmail.com

***Abstract*— Mobile attack approaches can be categorized as Application Based Attacks and Frequency Based Attacks. Application based attacks are reviewed extensively in the literature. However, frequency based attacks to mobile phones are not experimented in detail. In this work, we have experimentally succeeded to attack an Android smartphone using a simple software based radio circuit. We have developed a software "Primary Mobile Hack Builder" to control Android operated cellphone as a distance. The SMS information and pictures in the cellphone can be obtained using this device. On the other hand, after launching a software into targeting cellphone, the camera of the cellphone can be controlled for taking pictures and downloading them into our computers. It was also possible to eavesdropping the conversation.**

Keywords—Primary Mobile Hack Builder, Application Based Mobile Attackers, Frequency Based Mobile Attackers.

I. INTRODUCTION

Mobile communication security has become even more important after the use of these devices increases. Many new methods and measures have been developed by manufacturers and research communities to protect the personal information while keeping the integrity and availability. Still, these devices are vulnerable and each new innovation brings a threat to the system.

The first attack against the communication devices occurred in 1971, and new attack methods have been developed each day [1]. With the development of computer systems, some of the attempted attacks on this system have succeeded, but the attack strategy did not change much from the traditional structure. In the traditional structure, communication devices, which are usually guided by the help of frequencies, have caused a great information grudge and material damage. Although various encryption methods, sub-structures, and security protocols have been installed into devices and software-based measures are taken, it has been mostly not enough to protect our devices from the attacks. Indeed, according to a research done at the University of Pennsylvania in 2010, 68% of existing mobile devices could not provide security against an attack [2].

Smartphones' detection capabilities have created new opportunities for innovative User Interface (UI) and context sensitive applications. But, it has also caused new issues for user privacy and potential risks to security breaches. For example, researchers have recently explored a new attack vector that utilizes built-in motion sensors to remove user touches on smartphone touch screens. This new development has resulted in threat to lock the smartphone despite the lack of a physical keyboard [3].

In this study, we will focus on two types of cyber-attacks based on application and frequency techniques. Specifically, we are going to explain how some attacks can be done based on application or frequency techniques to a smartphone device.

II. MOBILE ATTACK APPROACHES

Mobile Ad Hoc Networks (MANETs) are vulnerable to various threats due to the lack of dynamic inheritance and centralized control points. Collaborative attacks occur when multiple attackers together synchronize their actions to corrupt a target network. A wormhole attack is one of the most violent joint attacks, as it can damage the network in various forms. It is very difficult to detect wormhole attacks because two or more nodes are launched in cooperation with each other and work in two stages. In the first stage, malicious nodes try to persuade legitimate nodes to transfer data to them in order to gain access to more routes. In the second stage, malicious nodes use the received data in various forms [4].

In a node replication attack, an enemy creates copies of the sensor nodes that are seized to attempt to control information accessing the base station, or more generally to compromise network functionality. Dimitriou et al have developed a fully decentralized schemes for finding and dealing with a large number of fraudsters in Mobile Wireless Sensor Networks (MWSNs). Suggested schemes not only do not quarantine these harmful nodes, but they are also based on a confidential agreement made against fraudsters trying to get the network's legitimate nodes on the black list. Therefore, the completeness and robustness of the protocols are guaranteed. Their protocols have been combined with extensive mathematical and experimental results to make them suitable for realistic mobile sensor network deployments [5].

Mobile attacks are shaped by purpose. The factors that determine the diversity, size, and method of attack are application-based or frequency-based. During personal attacks, system files (Mac OSX and Apk, etc.) that can be created together with infiltration of existing operating systems of mobile devices are made available for social engineering or as a physical intervention. As a result of this endeavor; these methods can be used to get all kinds of

978-1-5090-5835-8/17/$31.00 ©2017 IEEE

information such as contacts, SMS, pictures, voice records, geo location, and instant camera access located on the device.

In the case of frequency-based attacks, the success rate is relatively low compared to the other methods. But basic information, speech or Short Message Service (SMS) information can be easily fetched by using the flowing signals without any physical intervention to the target devices.

Analysis and processing capabilities against vulnerabilities of software used in basic attack methods can be used for many different areas without being divided into categories. One of the most obvious examples against mobile devices is the application-based attack. By virtue of the back door built on a certain port, a small size software can provide information exchange with us at the same time.

These application based attacks affected largely Android based devices, but they hit iOS as well. For instance, iKee was the first iPhone virus. The virus, which can spread from phone to phone, changed the iPhone's wallpaper to a photograph of 1980s singer Rick Astley - best known for his hit Never Gonna Give You Up. The wallpaper features the words "Ikee is never gonna give you up". However, the virus can only infect phones which have been jailbroken by their owners [6]. These type of examples occurred more in Android platform. For instance the DroidDream Malware infected 68 apps on Android Market in March 2011. These applications were downloaded more than 260K in just 4 days and these rooted the phones via Android Debug Bridge vulnerability and sent not authorized premium-rate SMS messages at night [7]. Fake Angry Birds application was another sample for a bot-trojan type of attack. It masquerades as a game and used the Gingerbreak exploit to root Android devices to join them as botnet [8].

In the case of frequency-based mobile attacks, the processing abilities of outgoing chipsets can be used for attacking into mobile devices. The software of the terrestrial broadcasting devices used to provide IP-TV or Radio negotiation nowadays can open a door between the base stations to extract information there.

III. APPLICATION BASED ATTACKS

Social skills have played a very important role in application based attacks, although the method has been based on a simple technique. However, in these applications, where the social engineering field can be successfully used, the control of the ports and the back door software must be completely and accurately handled in all steps.

As pointed out by today's penetration systems, software is moving towards uniformity and functionality. The "Primary Mobile Hack Builder" program that we have developed has many features to be at the very beginning of this list. It is understandable with the parameters it contains, providing easy access and solutions.

For development phases; Bash, Ruby, and Perl languages have been made available for an active attack using a GTK # language to create a simple user interface. Once the APK or Mac OSX files are installed on the target device, the instant camera image, video recording, SMS and contacts recordings, audio recording, and geographic location can be obtained through port gateways. In the process of creating files, Bash codes are used. Information is written in Perl language. The information is sent to consoles developed by Metasploit Company [9] and attacks written in Ruby language are automated. The shell codes were processed on the target device during these operations and were set up for later processing.

A great deal of existing application-based attacks work with console access. It is an application that can be placed in the top row under the titles of access codes and ease of use in the field. The ability to access into existing programs again does not have instant results or a user-generated view. The process steps are shown in the Fig.1.

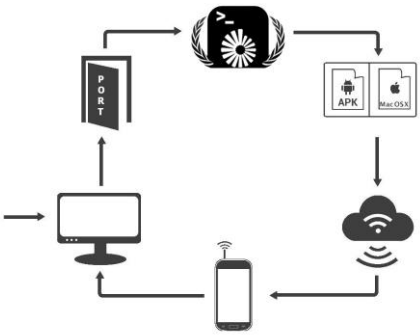

Fig. 1. Primary Mobile Hack Builder Working Principle

1) Steps Required to Implement Access

a) Performing updates of the operating system.

b) The port entry and the IP address are set for attack.

c) Follow the steps in the program interface.

d) Identification of internet based upload centers for access to the destination.

e) Enabling the application to process on the device.

f) The use of buttons for access requested files.

2) Steps Required to Block Access

a) Using a specific application controller on the device.

b) To follow application predicate phases and permissions.

c) Check application data transfers.

d) Making the necessary updates.

e) Checking background applications.

IV. FREQUENCY BASED ATTACKS

Although it has a complex structure in terms of the processing steps, frequency based attacks are a very effective method. By listening to the frequencies transmitted by the Global System for Mobile Communication (GSM) stations, this information can first be converted into a binary number system and then into a sound file or written text. There are many application options but an unknown method will be followed in this

article. As stated previously, today's control or attack software is used for various operations in many areas. Among the process steps, the most important point is the use of software based radio devices [10].

In order to perform the listening of the GSM frequencies, the chipsets must receive the correct frequency followed by the restored frequency to transmit the waves to the binary number base. The correct frequency should be transferred into the Temporary Mobile Subscriber Identity (TMSI) and the Symmetric Encryption Key (KC). The steps of this particular communication protocol are shown in Fig. 2.

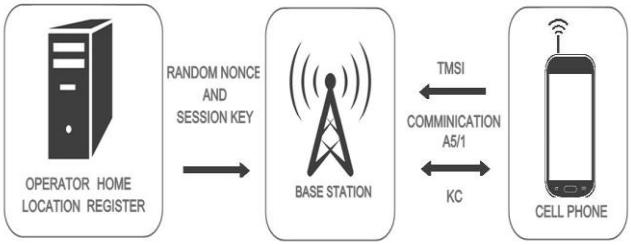

Fig. 2. Working principle of GSM Infrastructure

1) Identification of Process Steps

a) Temporary Mobile Subscriber Identity (TMSI)

It is used to provide a secure identification number between the base station and the pager. This information is taken from the Visiting Location Register (VLR) units and varies depending on the geographical area.

b) Symmetric Encryption

It is used for the encryption of a certain text or speech. Basically, the content to be encrypted is first transformed into an encapsulation cipher that cannot be understood by a cipher algorithm. In the GSM system, the A5 / 1 algorithm, as shown in Figure 3, is usually applied, but as these algorithms cannot meet the requirements, advanced versions are produced [11, 12, 13].

Rainbow table is used for a selected target. Randomly selected bits and scrolling passwords take a very long time with BruteForce method, and because of the persistent variability of TMSI ciphers, they require an immediate attack and result. Rainbow tables offer much faster solutions by trying to match the hash information in their hash contents with their hash information. Another approach is to estimate the TMSI numbers, but there is no possibility of estimating this feature presented with a different algorithm and order for each sim-card. However, the same phone models can add additional scrolling passwords to TMSI numbers, and these kinds of operations are not applied today [14].

The method is simply fitted with three linear-feedback shift register systems, which are formulated using XOR gates as shown in Figure 4.

LFSR number	Length in bits	Feedback polynomial	Clocking bit	Tapped bits
1	19	$x^{19} + x^{18} + x^{17} + x^{14} + 1$	8	13, 16, 17, 18
2	23	$x^{23} + x^{22} + x^{21} + x^{8} + 1$	10	7, 20, 21, 22
3	22	$x^{22} + x^{21} + 1$	10	20, 21

Fig. 3. A5/1 Encryption Algorithm Formula [13].

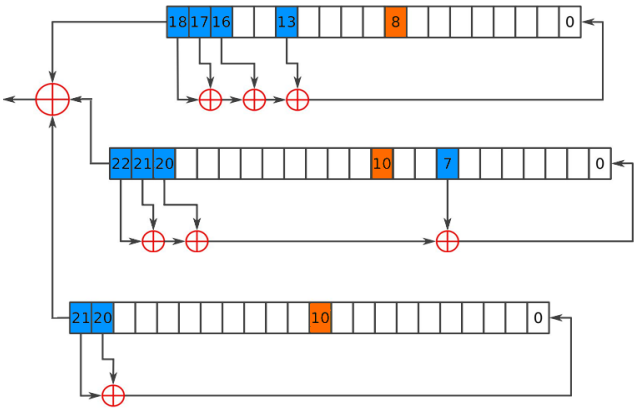

Fig. 4. A5/1 Example of Cryptographic Algorithm [13].

2) Steps Required for Access

Unlike existing radio systems, it is a product that has been made easy to use by computer processes and has many functions. Although it is usually used to process terrestrial digital television data, it is used for information from a frequency range of 60 to 1750 MHz, and its cost is much cheaper than the amount that can be allocated for the acquisition and connection of all devices. An example software-based radio circuit diagram is shown in Figure 5 [15].

Fig. 5 A Software Based Radio Circuit [15].

The operation diagram of this device is given in Figure 6.

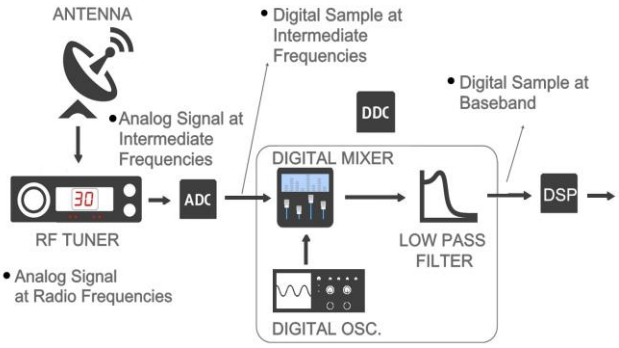

Fig. 6. Software Based Raio Operating Diamgram [15].

As shown in the operation diagram, it is now possible to collect frequencies from base stations, because the frequency bands used by GSM operators are in software based radio receiver range.

As a result of the determination of the frequency networks, different applications can be followed for the rest of these networks. The range of these listenings is in principle far from the point where the software-based radio is located to the nearest base station. For instance, the stations in the vicinity of "Petru Maior University" are shown in Figure 7.

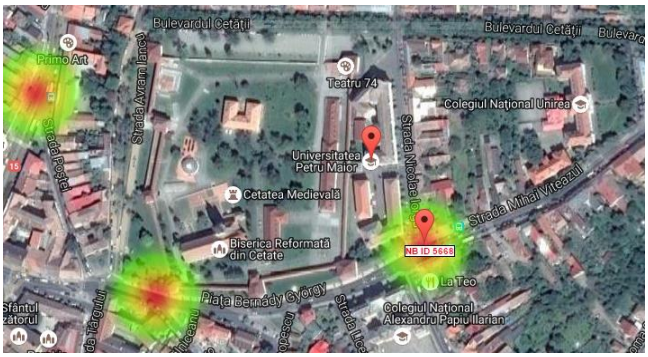

Fig. 7. GSM Stations located around Petru Maior University

All links to the nearest one of the displayed stations can be easily downloaded and resolved. This distance makes a good listening to the average 80 km area. With the development of GSM operators, these frequency levels increase, but the rate of increase in higher priced software-based radios increases, too. Preventing the attack is very difficult. However, the data capacity to store the encryption algorithms poses a lot of problems. The resolution of data packets may increase depending on the performance of the computer being processed.

After the identification phase, it is necessary to archive the information from the software based radio. Then, the necessary software is used to analyze the information converted into the binary number system. A diagram of an exemplary attack is given in Figure 8.

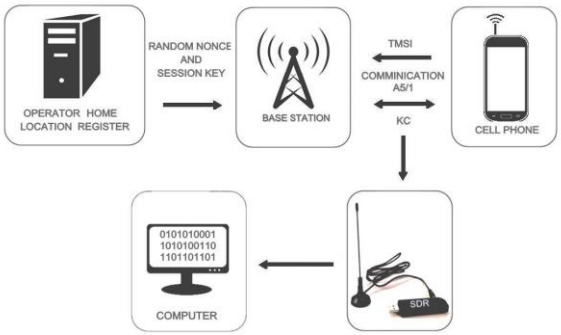

Fig.8. Frequency-Based Attack Diagram [15].

3) Steps Required to Block Access

a) High frequency bands should be used in the communication device.

b) Required updates must be made.

c) Avoid transmitting important information via SMS.

d) Secure or fixed lines should be preferred.

In addition, the access points of software-based radios can receive and process radio talk, radio-based cameras, police and ambulance lines, aircraft and ship roots, airport towers, air balloons and satellites, without being restricted to GSM lines.

V. CONCLUSION

Today, the most widely used mobile devices are under the threat of many cyber-attacks. Many people are victims of these attacks. Personal information can be obtained and this information can be broadcasted on social media which will be harmful to individuals.

This kind of attacks can be done on the cellphones running with the Android operating system using a primitive software based radio circuit. The SMS records on the mobile phone can be accessed and the environment where the mobile phone is located can be listened to. Pictures can be taken with the camera of the mobile phone as a distance. A simple software based radio device was used to do this. The cost of the device is less than $10, but the size of the damage cannot be measured financially.

In practice, it has been seen that information on some mobile phones can be reached through base stations located around Petru Maior University as a distance. Mobile phones that run on the Android operating system are under threat because of a simple designed software based radio circuit. Emergency software must be developed to prevent access to the Android mobile phone via a radio frequency device which is operated by software based radio circuits.

VI. REFERENCES

[1] Kizza, J. M, Ethics in Computing: A Concise Module. Springer. 2016.

[2] Mobile Security, World Heritage Encyclopedia, http://self.gutenberg.org/articles/eng/Mobile_security, Last accesed date: January 7, 2016.

[3] Hussain, M., Al-Haigi, A., Zaidan, A. A., Zaidan, B. B., Kiah, M. L. M., Anuar, N. B., Abdulnabi, M. The rise of keyloggers on

smartphones: A survey and insight into motion-based tap inference attacks, Pervasive and Mobile Computing 25 (2016) 1-25

[4] Khan, F. A., Imran, M., Abbas, H. A Detection and Prevention System against Collaborative Attacks in Mobile Ad Hoc Networks, Future Generation Computer Systems 68 (2017) 416-427.

[5] Dimitriou, T., Alrashed, E. A., Karaata, M. H., Hamdan, A. Imposter detection for replication attacks in mobile sensor networks, Computer Networks 108 (2016) 210-222.

[6] Andersen B. Australian admits creating first iPhone virus, 10 Nov. 2009, http://www.abc.net.au/news/2009-11-09/australian-admits-creating-first-iphone-virus/1135474 . Last accesed date: March 24, 2017.

[7] Rastogi, V., Chen, Y., Jiang, X. DroidChameleon: Evaluating Android anti-malware against transformation attacks, Proc. ACM ASIACCS, May 2013, pp. 329–334.

[8] Cluley, G. Android malware poses as Angry Birds Space game. https://nakedsecurity.sophos.com/2012/04/12/android-malware-angry-birds-space-game/ Last accesed date: March 24, 2017.

[9] Maynor, D., Mookhey, K. K. Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research, Elsevier. 2007

[10] AlEroud, A., Alsmadi, I., Identifying cyber-attacks on software defined networks: An inference-based intrusion detection approach, Journal of Netwrok and Computer Application 80 (2017) 152-164.

[11] O'Brien, K., J.,"Cellphone Encryption Code Is Divulged" New York Times, http://www.nytimes.com/2009/12/29/technology/29hack.html, Last accesed date: January 7, 2017.

[12] "A5/1 Cracking Project". Archived from the original on 25 December 2009. Retrieved 30 December 2009

[13] Sadkhan, S. B.; Jawad, N. H., Simulink Based Inplementation of Developed A5/1 Stream Cipher Cryptosystems, Procedis Computer Science 65 (2015) 350-357

[14] Hosmer, C., Python Forensics, Rainbow in the Cloud, A Workbench for Inventing and Sharing Digital Forensics Technology, 2014 Elsevier, pages 289-303.

[15] RTL-SDR and GNU Radio with Realtek RTL2832U [Elonics E4000/Raphael Micro R820T] software defined radio receivers, http://superkuh.com/rtlsdr.html, Last accesed date: January 7, 2017.