Mobile Platform Security - A Survey

Nandini Krupa Krishnamurthy
Clemson University
nandink@clemson.edu

***Abstract*—Mobile Platform Security has gained a lot of importance in the recent years due to the ever growing number of mobile devices. As the number of mobile devices are growing exponentially, so are the number of attacks on them. Researchers at Check-Point warn that there is a 50% rise of attacks on mobiles in 2019 as compared to 2018. Statistics show that as of August 2019, there are 24 million android phones vulnerable to attacks. Hence, security for these devices is the need of the hour. This paper focuses on mobile platform security. It also talks about the attacks on them also detection of these attacks and defenses against them.**

I. Introduction

The researches show that there are more mobile devices in the world than the actual human population. The time for which mobile phones were used to only text or call is long gone. The mobile devices take up the job of personal computers and also have automated services by various enterprises that carry out using applications. These make the tasks simpler. A few examples of mobile devices are smartphones, tablets, notebooks or similar devices. Recent years have seen an exponential growth of these devices and also their sales and adoption [1]. An operating system and applications are the two components of mobile device systems. Android is the largest used operating system, followed by iOS and Microsoft. Figure 1 shows the distribution of these operating systems from 2012 to 2015 [2].

Vendor	2014 Shipment Values (Million)	2014 market % share	2018 Shipment values (Million)	2018 market % Share	Growth
Android	950.5	78.9 %	1321.1	76.0 %	10.7 %
iOS	179.5	14.9 %	249.6	14.4 %	10.2 %
Windows Phone	47.0	3.9 %	121.8	7.0 %	29.5 %
Black-Berry	11.9	1.0 %	5.3	0.3 %	-22%
Others	15.1	1.3 %	40.7	2.3 %	32.7 %
Total	1204.4	100.0 %	1738.5	100.0 %	11.5 %

Fig. 1. Smartphone estimation by OS 2014 Shipment and Market share 2018 [3]

As the number and variety of mobile devices increase so do its malware. for example as the number of users installing the applications increase so does the chances of them installing malicious programs. Another example is the usage of mobile devices for online banking transactions that the user has to enter credentials for logging into applications. In this scenario does the high taxes of the user getting hacked by the potential attackers. in fact there is now a high rise in the number of operating system vulnerabilities.

Taking all of this into consideration this paper focuses on the threats, vulnerabilities, and issues related to mobile devices. We will also go through some of the challenges that are being faced currently in this regard and also the future challenges.

A. Mobile Technologies

In the section, we will go through some of the Technologies used by mobile devices. These Technologies may not be basically built for mobile devices but are largely used by them. There are broadly divided into Networking Technologies and wireless telecommunication technologies[4]. These Technologies are completely explained in this section.

1) Network Technologies: This section describes three main types of network technologies that are widely used. They are:

- WLAN
- Bluetooth
- IEEE 802.11

1) Wireless Local Area Network (WLAN)
WLAN has expanded in recent years due to the explosion of laptops and its ease of installation. It is used in connecting devices. This allows the users to be connected without the use of wires and also move in an area of the network coverage without getting disconnected from the network.

2) Bluetooth
By making use of short-wavelength radio transmissions, the users are able to exchange data over a small area by this technology called Bluetooth. Bluetooth creates Personal Area Networks with high security. This was developed in 1999 by Bluetooth Special Interest Group (SIG). Bluetooth is particularly useful for devices communicating with the following features:

- Lower consumptions
- Short range of communications (1-100 meters)
- Small production costs

Depending upon power consumption and range of communication Bluetooth devices can be classified under three classes as shown in Table 1.
Profiles to indicate services and services implementation is defined by SIG. Few of them are Generic Access Profile, GAP, or Headset Profile, HSP.

Class	Power (dBm)	Distance (m)
Class 1	20	100
Class 2	4	10
Class 3	0	1

TABLE I
BLUETOOTH CLASSES [4]

Technology	Bandwidth (GHz)	Bitrate (Mbits.s)	Modulation
802.11b	2.4	5.5, 11	CCK
802.11g	2.4	6, 9, 12, 18, 24, 26, 48, 54	OFDM

TABLE II
802.11B AND 802.11G PROTOCOLS[4]

3) Wireless LAN IEEE 802.11
IEEE 802.11 is a family of standards for WLAN that includes several protocols for communicating at different frequencies (2.4, 3.6 and 5 GHz).
This standard operates in two different modes:
   - infrastructure mode - Here, an Access Point (AP) is used to regulate the network traffic and also coordinate all the devices connected in that Network
   - infrastructure-less mode (ad hoc mode) - The Access Point is gently called as a referee. In infrastructure-less mode there is no referee and the devices gain network access by monitoring the spectrum.

   Protocols are defined by 802.11b and 802.11g as shown in Table 2

B. Wireless Telecommunication Technologies

GSM, GPRS, EDGE, and UMTS are some of the widely used wireless technologies for communication.

1) Global System for Mobile communications (GSM)
GSM (2G) was developed in 1990 by Group Special Mobile. GSM creates cellular networks where one mobile station can communicate with another through base stations, networks, and switching subsystems. Other services offered are data transmission, digital fax, e-mail, call forwarding, teleconferencing service and Short Message Service (SMS).
2) General Packet Radio Service (GPRS)
GPRS (2.5 generation) was developed to provide an improvised version of GSM wherein users could enjoy better performances with higher data rates and lower access time. To exchange data between users GPRS uses a packet switching mechanism. GPRS also led to the introduction of Wireless Application Protocol (WAP) and Multimedia Messaging Service (MMS).
3) Enhanced Data rates for GSM Evolution (EDGE)
EDGE was introduced as a technology that outperforms GPRS by providing better features including higher data transmission rate and higher reliability.
4) The Universal Mobile Telecommunications System (UMTS)
UMTS (third generation, 3G) provides a higher transmission rate when compared to 2G and 3-g mobile by around 2 Mbps. This provides circuit switching along with packet switching thereby offering services from different classes including conversational interactive and background.

II. MAIN TECHNIQUES

This section talks about the challenges faced by the security of the mobile device. To understand this, a threat model for mobile platforms is presented. This is again divided into three sections - attack goals, attack vectors and mobile malware [5]. This is shown in Figure 2.

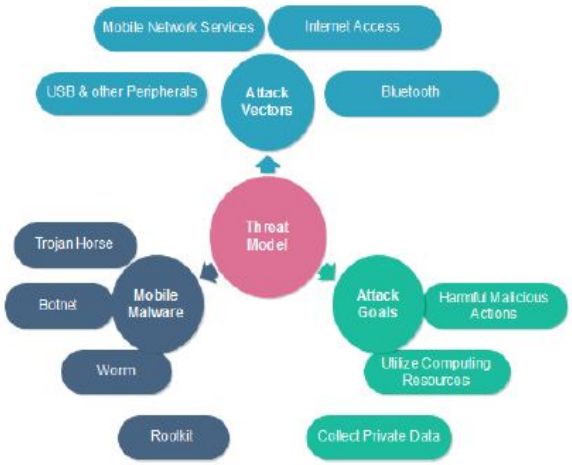

Fig. 2. Mobile Platform Model Threats (MPMT) [9]

A. Attack Goals

This section talks about the motives behind causing an attack on a mobile device. These goals can be classified under two categories – one, in which the normal user activity is not disrupted (covert) and two, in which the user activity is disturbed (harmful)[5]. The first two described below are from the former category and the second one from the latter category.

*1) **Collect Private Data**:* Users store personal data on their mobile devices. Attackers make use of this and breach user's privacy to collect stored information. In cases os successful attacks, the attackers can read the user's SMS and MMS messages, emails, call logs, contact details. An attacker can also cause a sending of fake MMS or SMS or forward emails. Any data located in the device's SD card like videos, pictures may also be attacked. Another important attack is when the compromised hardware can be used to steal user information such as the voice recorder can be used to record the user's conversation or camera may be used to record user surroundings. Even the location of the user can be accessed by using GPS module.

*2) **Utilize Computing Resources**:* The increase in computing resources is the main ground for attackers to cause a malicious attack which can be successfully exploited by a combination of raw computing power and broadband network access. Additionally, these mobile devices can also be used for the deployment of botnets.

*3) **Harmful Malicious Actions**:* These types of actions are used to annoy the user rather than getting any useful work done for the attacker. These attacks are easily detectable. Though this is the case, they are aimed at causing as much destruction as possible ranging from data loss to battery drain and high utilization of resources. In extreme cases the attacker can gain access to critical systems, the attacker can brick the device.

B. Attack vectors

Vectors can be used to successfully deliver malicious contents. These vectors can be broadly classified into four categories [5]. They are:

- Mobile network services
- Internet access
- Bluetooth
- USB and Other Peripherals

*1) **Mobile Network Services**:* SMS, MMS and voice calls are the most common type of attack vectors. SMS and MMS can be used to transfer malicious content. Since MMS contains rich content, an attacker can embed hidden XML messages. Voice calls can be used to cause phishing attacks. The two basic types of phishing attacks for mobile are:

- **Smishing:** SMS messages are used for this purpose. URL links are sent over SMS and if a user clicks on these URLs, it automatically opens browser window potentially leading to an attack.
- **Vishing:** Voice calls are used for this. The attackers mask the true voice call id and trick the user into believing the authenticity of the number and if the user calls the number, the attacker can gain access to sensitive information.

*2) **Internet Access**:* Wifi networks, 3G/4G services can provide high-performance services but they work on mobile devices in the same way they work on PCs. Added to these are the continuous connection to internet by mobile devices. This may lead to successful malicious attacks. Attackers may also use online social networks to spread malicious content for attacks. Facebook and Twitter are the most common ground for this. Furthermore, the URL shortening services add to the increase in the attacks. When the URLs are shortened because the original link is difficult to share, its authenticity becomes unknown and the destination of the web link can only be found out by clicking the link. These links may be harmful and can be used to cause an attack.

*3) **Bluetooth**:* Bluetooth can be used to direct the spreading of malware, i.e., device-to-device spreading. The attacker pairs the Bluetooth device to that of the device that is supposed to be compromised. When a connection is established, malicious content is sent to the compromised device. However, the attack using Bluetooth can be limited in the sense that the user than to confirm the received file identity and only then can open it and also pairing is not default and can only happen when the user knows which device is the pairing his device with.

4) USB and Other Peripherals: External devices like USB can be used to inject malicious content into a device. If the device is compromised by the software, then the attacker gains access to the private information in the device and can also install malicious applications.

C. Mobile Malware

The operation of operating systems in traditional computers and also mobile devices are similar. Thus, the malware that can be used to cause an attack on a personal computer can be migrated to cause an attack on mobile operating systems [5]. This section talks about some of this malware.

*1) **Trojan Horse**:* Trojans are used to steal some private information or to install some malicious applications like botnets or worms. These can also be used to cause phishing attacks.

*2) **Botnet**:* A botnet is a group of compromised devices that can be controlled and coordinated to perform remote attacks. The idea is used to use the computing power of compromised devices to cause an attack. The attacks range from sending spam emails to causing Denial of Service attacks.

*3) **Worm**:* When infected, worms replicate internally and spread unconventionally to those systems which are not infected. This, though originally designed for computers, has migrated to mobile platforms. Cabir [6] was the first worm to be transmitted. Another example is the Ikee.B [7].

*4) **Rootkit**:* Rootkit, though is a malicious application, runs on privileged mode. These mask their functionality and modifies the operating system functionalities. Rootkits don't exist currently for mobile devices but studies show that these can be potential harm to mobile devices in future.

III. Attacks on Mobiles

This section talks about some common type of attacks on mobile platforms [10]

1) Eavesdropping – Unauthorized stealing information from a communication without disrupting the services.
2) Black-hole Attack in which all nodes route packets to a single point.
3) Wormhole Attack – A tunnel is created in a network in which the packets keep replaying.
4) Malware – A disguised application causing a range of attacks
5) Byzantine Attack – a group of nodes within a network of nodes causing an attack.
6) Phishing – Deceives people to get personal information.
7) Replay Attack – Data is repeatedly injected to create unnecessary traffic.
8) Router Protocol Poisoning – Packet transmission is disrupted by poisoning the protocol.
9) Flooding – False packets are injected into the network.

10) Sinkhole – A node tends to deceive other neighboring nodes into sending data to itself.
11) Spoofing – False sites in disguise to spoof legitimate websites.
12) Denial of Service Attack – Goal is to disrupt service by flooding packets.
13) Man-in-middle Attack – an intruder sniffs out data from a communication.
14) Fabrication – False routing packets are created inside a network.

IV. Mobile Malware Detection

The malware detection systems can be broadly classified under two categories - host based detection and cloud based detection. Host based detection is the technique that is hosted in mobile systems.If, to increase computation efficiency, the work is offloaded to a server, then it is called as cloud based detection. Host based detection systems provide limited detection services and prove ineffective whereas cloud based detection systems do complicated, resource intensive detection.

A. *Host-Based Detection*

Host based detection systems can be used to do two type of analyses – static analysis and dynamic analysis.

1) Static analysis: When an applicate or a code is analyzed without executing it, then it is called as static analysis. It is simple and also time effective. There are three types of static analyses:

- System based call (Figure 2)
- Static taint analysis (Figure 3)
- Source code analysis (Figure 5)

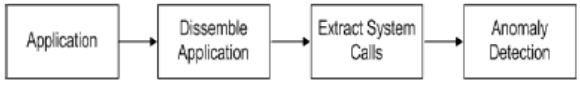

Fig. 3. System call based analysis [8]

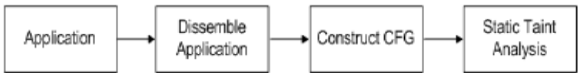

Fig. 4. Static taint analysis [8]

B. *Cloud-Based Detection*

In cloud based detection systems, a client based application monitors the system calls in the device and send all of them to a server which detects for malicious behavior. This is particularly useful in cases of heterogeneous devices connected to the server as offloading becomes easier as explained in

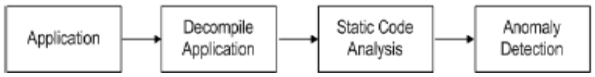

Fig. 5. Source code based static analysis [8]

Figure 5. Advantages of using cloud based detection system are:

1) Efficiency of detection is more
2) Resources from the devices are used less
3) Complexity of the device is very low

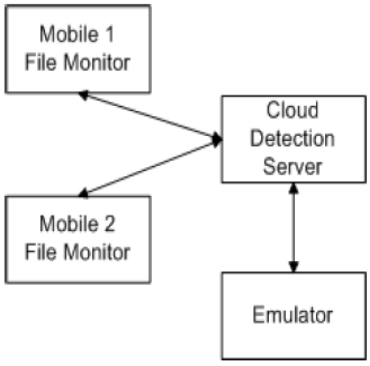

Fig. 6. Cloud detection system [8]

V. Defense Against Malware

This section talks about various defense mechanisms against mobile malware. The prevention-based system should be complementary to detection-based system.

A. *Defense against malware in iOS*

Few of the methods to control malware in iOS are:

1) Vetting process – in which a public market is offered and approval process is also complimented even before an application is hosted.
2) Making sure that jailbreaks do no create flaws thus offering attackers grounds to cause attacks.
3) Making the operating system insensitive to Rootkits.

B. *Defense against malware in Android*

The main techniques of defense against malware in android include:

1) Sandboxing which is a process of putting virtual walls between applications thus making them inaccessible by other parts of the phone.
2) Permissions- To protect data and resource on the mobile, android performs a permission check to enforce security.
3) Malware removal – whenever a new application is hosted, the available software scans it for any malware.

This application is called as Bouncer. If Bouncer detects any anomalies, it checks the behavior patterns with the available malware pattern. If it detects any malware, the application will be removed from the marketplace.

C. Defense against proximity malware

Proximity malware usually goes undetected by network providers. There are three methods to defend against these malware.

1) Local detection : The device detects the malware (local detection) and services such as Bluetooth and WiFi are cancelled by it.
2) Proximity signature dissemination: Each device has a hash table such as MD5 which it used to maintain a record of signatures of malware. So when a malware is detected, the device is disabled.
3) Broadcast signature dissemination: Here, the mobile service provider broadcasts the signature. The compromised device sends the malicious contents to the server which computes the signature for it and also computes an update that removes the malware from all of the infected systems.

D. Defense against sensor sniffing attacks

1) Policy engine and application monitoring: Here, the system defending should effectively use policies such as Whitelisting and blacklisting and also continuously monitor the system.
2) Interceptor: When an interceptor is present between the sensor and the application, it can detect the cases of deviation of access control and initiate actions such as locking and blocking.
3) User interaction: This is the case of user authorization. A user is asked to authenticate his credentials and also gets notified when a sensor is used.

VI. Future Trends

This section talks about some of the topics that needs attention [11] [12].

1) Addressing cross-process attacks wherein a malicious applications tricks the user to send the desired information.
2) Another interesting area of application is addressing mobile security based on the environment in which it is operating.
3) It is also necessary to understand the effects of malicious application which besides stealing data , may cause potential physical harm to the user.
4) Fragmenting Android software and hardware is also an interesting scope for research.
5) Combining together new mechanisms with efficient consumption of mobile resources along with preserving user security is another need of the hour.

VII. Conclusion

In this paper we have gone through some of the interesting attacks on mobile platforms and also we have seen some of the methods to detect and defend them. As mobile devices are occupying a personal space, it is very important to maintain the confidentiality and integrity of these. When these are compromised, it forms a ground for attackers to cause malicious attacks. These attacks are usually hard to detect and hence goes unnoticed. Therefore, it is very important to develop methods to target these and provide users with a more secure environment thus preserving sensitive information and lessening the probability of attacks.

References

[1] L. Aron and P. Hanacek, "Overview of security on mobile devices," 2015 2nd World Symposium on Web Applications and Networking (WSWAN), Sousse, 2015, pp. 1-11. doi: 10.1109/WSWAN.2015.7210319

[2] Mahmood, Sardasht & Amen, Bakhtiar & Nabi, Rebwar. (2016). Mobile Application Security Platforms Survey. International Journal of Computer Applications. 133. 40-46. 10.5120/ijca2016907736.

[3] Farhan, Syed & Zaidi, Syed Farhan & Munam, Ali & Shah, Munam & Kamran, Muhammad & Javaid, Qaisar & Zhang, Sijing. (2016). A Survey on Security for Smartphone Device. International Journal of Advanced Computer Science and Applications. 7. 206-219. 10.14569/IJACSA.2016.070426.

[4] M. La Polla, F. Martinelli and D. Sgandurra, "A Survey on Security for Mobile Devices," in IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 446-471, First Quarter 2013. doi: 10.1109/SURV.2012.013012.00028

[5] Delac, Goran & Silic, Marin & Krolo, Jakov. (2011). Emerging security threats for mobile platforms. 1468-1473.

[6] K. Dunham, "Mobile Malware Attacks and Defense", Syngress Publishing, 2008.

[7] F-Secure, Worm:iPhoneOS/Ikee.B, [Online]. http://www.f-secure.com/v-descs/worm_iphoneos_ikee_b.shtml.

[8] Ramu, S. V.. "Mobile Malware Evolution , Detection and Defense." (2012).

[9] Delac, G. Silic, M. and Krolo, J. (2011), Emerging Security Threats for Mobile Platforms' MIPRO 2011, May 23-27, 2011, Opatija, Croatia

[10] Aljudaibi, Samaher. (2016). Research Paper for Mobile Devices Security. 10.13140/RG.2.2.32892.13440.

[11] Vylegzhanina, Violetta & Schmidt, Douglas & White, Jules. (2015). Gaps and future directions in mobile security research. 49-50. 10.1145/2846661.2846669.

[12] Alsaleh, Mansour, Noura Alomar and Abdulrahman Alarifi. "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods." PloS one (2017).