International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
OPEN ACCESS
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST1625414

Evaluation of Smartphone Security Challenges and Measures

Sai Kiran Reddy Malikireddy, Kiranmayi Karri, Tejaswi Chirumalla
Department of Computer Science, University of South Florida, Tampa, Florida, USA

ABSTRACT

The term Smartphone refers to a mobile phone integrated with an operating system like Android, iOS, Windows. In today's technological world, Smartphone's have become ubiquitous[. The main reason of such high usage of these phones is that their ability to perform multiple functions when compared to the traditional mobile phones. In addition to the features provided by the traditional mobile phones, these phones support a wide variety of operations such as access to the internet through Wi-Fi/3G/4G connectivity, most of such devices have an in-built browser to perform this operation[1][2]. Apart from this feature, it also provides Bluetooth connectivity, access to digital media, for mobile payment transactions integrated with NFC technology, gives location accuracy, enable the feature of downloading third party applications. Most of functions which are performed by the personal computers can also be done using these. We are in a position where there is more utilization of Smartphone's when compared to the traditional PC's in today's market. These devices also carry highly confidential data such as bank details, social media accounts, email details and more. One could also observe that with the increase in the utilization of these devices, there is more and more storage of personal information on it. With this increase in the popularity of the devices, there are also many vulnerable attacks and many other security issues with them. Types of attacks can be mobile malware, phishing scams, and network spoofing attacks, surveillance attacks, and network congestion. In this interim report, we focus and provide our analysis or survey on various such kinds of attacks, give few in depth details and report accordingly.

Keywords : Smartphone's, Security, Attacks, Malware, Detection

Introduction

Nowadays smart phones provide with capabilities such as a traditional computer with large connectivity options such as connectivity options, Bluetooth, GSM, GPRS,3G/4G ,Wi-Fi. Providing such large features for smart phones also resulted as a target for large number of attackers. In the beginning, the OS used in smart phones were easy for attackers to exploit vulnerable attacks. These years we have various number of operating systems coming up such as Symbian OS, Windows OS, Android and iOS[3]. The emergence of Open source platform in mobile devices played a significant role for the attraction by a large number of individuals where many PCs were replaced by mobile devices in many organizations. The more advanced malware attacks were performed on the smart phones because of some of the exceptional facilities provided by them like large storage capacity ,processing power ,location estimation. Though the number of smart phones malware is very less when

Received: 01 July 2016 | Accepted: 20 July 2016 | July-August-2016 [(2)4: 382-391]

compared to the traditional PC malwares, we can still expect that to increase same as traditional PC malwares in next few years.

To justify the above statement, we could consider an example of smart phone users downloading the third party applications, with this kind of action we can say that the chance of attacks may increase as well[3]. Not only the malware attacks, as there is increase in the number of users using these phones to perform various kind of transactions like online banking or online shopping, the attackers are creating new kind of attacks to make some profit out of such sensitive information. The confidential information such as login credentials to various applications is being hacked by the intruders, which is creating serious threat to the users. Therefore the more we use the applications of the smart phones devices the more are the security risks associated with them. To detect such kind of malicious events, there has been a technique called intrusion detection developed to protect sensitive information. This statement is being proved in one of the paper where it states that the attackers are now concentrating on the mobile platforms instead of traditional PC's, it is being reported that in one year from 2009 to 2010 there was 42% increase in the number of malware attacks[2].

The paper is organized as follows. We first introduced the concept of smart phones, the OS's used in it and the attacks on high level. The further sections provides us with the information on various types of mobile malware attacks, threats which may appear in future, comparison of various solutions from our survey of many related references. And finally provide conclusion of the paper.

SMARTPHONE SECURITY CONCERNS

As the usages of smart phones are growing rapidly for business and personal use, it is becoming more critical to assure smart phone security and reliability. There are many security concerns related with smart phones. Smart phones were initially effected with viruses, spam, spyware and malicious software. The amount of malware detection related to android platform has been rising since 2011. Smartphone can be secured using the same techniques which are applied in the use of traditional computers with the help of antivirus software, but Smartphone's have some extreme security challenges since they are consumer products and different people have different preferences for security of the Smartphone's. Also, the tools that are used for the security must be easily configurable to meet the security needs of the various groups of people.

Smart phone has three important layers. Application layer, Communication layer and Resource layer. The malware can make any of these layers of smart phone as its target to spread the malicious code. All the smart phone applications like social networking software, email, text message, and synchronization software comes under application layer. At this layer the malware from subscriber point of view is seen as a normal application and is downloaded. The communication channels to smart phone include carrier networks, WiFi connectivity, Bluetooth network, Micro USB port, and MicroSD slot[12]. There is a possibility for the malware attack thorough any of these communication channels. The flash memory, camera, microphone, and sensors within a smartphone are included under Resource layer. Here as these resources contain the sensitive data the sensitive data, the malware takes control of these resources and manipulates them.

Among all the security concerns, the malware/spyware attacks are being major concerns for most of the Smartphone users, so before discussing all the security concerns, let us see what actually these attacks mean.

The Smartphone threat model generally consists of four parts, a malicious user, malware, a smartphone, and premium accounts/malicious websites. The working of this malware is as follows, using the application store or website the malicious user publishes the malware. Here the smart phone is chosen as the target, as the smart phone consists of huge amounts of sensitive data. Once this application is downloaded by the smart phone then the phone gets effected by the malware which consists of threats and attacks. Once the smart phone is prone to malware then the smart phone resources would be in the control of the malware. The data collection or websites getting redirected to malicious sites or premium accounts are few activities being performed when malware controls the smart phone.

Few things which malware does when it gets access to the smart phone resources are, reprogramming of flash memory takes place. This reprogramming of flash memory by malware once done will only be changed when the user reprograms it. Malicious user when gains access to microSD memory card can easily disclose the content of memory card. Sometimes the smart phone users don’t like their location information to be disclosed but this disclosing happens through the sensors such as GPS, gyroscopic sensor, and accelerometers GPS[6]. The effect of malware becomes very powerful when it gains complete access to smart phone .At this stage the smart phone functions as a tapping device. The camera ,microphone cameras and microphone would be turned off and on without the users notice. While the data is being transferred through smart phone to computer or other devices through Wi-Fi or Bluetooth, data leakage can happen without the user knowing it. The malware smart phones falls into three categories namely virus, Trojan and spyware[6]. Trojan and spyware are the most prominent malwares in smart phones.

Virus: The viruses are disguised as security patch, as a game or as other desirable application. The virus spreading started through internet downloads, through memory cards and through Bluetooth. The Bluetooth viruses are categorized into Blue jacking and Bluesnarfing. When the devices are within 33feet range the unsolicited messages are sent over Bluetooth to blue tooth enabled devices which is termed as blue jacking. In bluesnarfing,the unauthorized access to the information of Smartphone is done through Bluetooth.

Trojan: The other type of malware in Smartphone is Trojan. Recording calls, instant messages, locating via GPS, forwarding call logs and other vital data are the activities which Trojans are mostly related to. One of the largest wide spread categories of Trojan is SMStorjan[7]. This SMS Trojan which runs in the background of an application sends SMS messages to premium rate account owned by an attacker. Hippo SMS is an example of this SMS trojan. The SMS trojan increases the mobile billing charges by sending SMS messages to premium mobiles and by blocking the messages from the service providers regarding the additional costs regarding the billing charges.

CLASSIFICATION OF CHALLENGES

Challenges faced by the Smartphone users could be classified based on the type of attacks on them. Below are some of the challenges.

a) DATA LEAKAGE RESULTING FROM DEVICE LOSS OR THEFT We encounter this type of security issue whenever the phone is stolen or lost, and in this case if the removable media is unprotected, which allows the attacker to access the data in it. Smartphone's may contain very sensitive data such as online account details, bank login credentials, credit card information, personal data etc.,,

b) ATTACKS ON DECOMMISSIONED SMARTPHONES Though users are removing or wiping the data from the memory before decommissioning the phones, there is large amount of information which is retrieved by the attackers.

c) PHISHING ATTACKS

In this case, an attacker may get to know the user information such as passwords and account numbers by means of fake SMS/emails/messages which look like genuine once. Some application stores are allowing to place fake apps which doesn't actually differ from the original once. Some Smartphone's provides us various types of channels such as SMiShing which can be used for SMS phishing. For example, many mobile applications include social sharing and payment buttons. A malicious application can similarly include a “Share on Facebook” button and redirect the users to a spoofed target application. The target application can then request the user’s secret credentials and steal the data[11][14].

d) SPYWARE ATTACKS

Spyware is nothing but malicious software that helps an attacker in collecting information from the phones and use for marketing purposes. Whenever a spyware software is installed, this allows the attacker to have access to all the personal information in our Smartphone's if it's not secured properly. For example, if we consider a application to know the weather of a location while connecting to the internet, we may feel this to be legitimate and provide information, however now the location data may be used for some other purposes by an attacker. For example, in iOS, whenever we install a new app, there is an option of giving permission to all the contacts in our phones, photos etc., here with this the attackers may also know the user's phone number which can be used for marketing purposes.

e) NETWORK SPOOFING ATTACKS

In this kind of attack, the attacker deploys a network access point, whenever a user connects to this network, the attacker would tampers the user's access. By this kind of access the attacker may change the default configurations of access points in the Smartphone's. Though this kind of attacks are detectable by the users, but they have to verify each and every time for SSL certificates and authentications.

f) SURVIELLANCE ATTACKS

This is done with the user's Smartphone. Smartphone have many features such as microphones, cameras, GPS which contain sensors. Whenever any third party software's or applications installed associated with such kind of features, it will be used as a spying tool[3]. Among all the kind of sensors/ features, GPS should be taken care as this might give attacker the location information of the users.

g) SNIFFING: This is a kind of attack where one can tap or snif the phone. Users having subscribed to GSM can be at more risk of such kind of attacks. Further, as eavesdropping software continues to become available and installed in Smartphone's, Smartphone subscribers with 3G or 4G networks are at risk too.

h) SPAM: Spam is a attack which is performed in carried through emails or MMS messages. Spam messages may include URLs which direct users to phishing websites. MMS spam can also be used for starting denial of service attacks.

i) VISHING: It is a kind of voice phishing attack where the attackers try to gain access to sensitive data from user by spoofing the "Caller ID", malicious users try to gain access to private and financial information from a smartphone user. Here the attacker ID would pretend as spoof the smartphone users to release their personal credentials.

j) VULNERABILITIES OF WEBKIT ENGINE: This is another kind of attack where using web browsers. In this the attackers will crash the user applications and execute the malicious code. They also install a remote tool and use that to eavesdrop on smartphone conversations and monitor the user locations.

DESIRED SECURITY FEATURES

Any Smartphone should possess certain features to mitigate the threats and security concerns. The most desirable features in a Smartphone are confidentiality, integrity, and authentication. Most Smartphone's support synchronization between the device and a computer. This function makes it possible for another user to access the smartphone file system. Thus, to keep data confidential, users should employ encryption techniques and avoid storing sensitive information in plaintext on a smartphone. Integrity applies to both data and the system. App stores should verify software integration to avoid malicious modification. Further, smartphones should provide mechanisms to protect system integrity. They should also block unauthorized data access requests. A smartphone authentication service could protect smartphone users against malware attacks that spoof caller IDs and MMS. Because these help improve both coverage and capacity, authentication becomes important to validate a carrier’s identity. In this report, we provided the topic chosen along with our initial analysis as part of our survey paper. Also, the plan of action detailing this approach is being dealt with the term project.

SMARTPHONE SECURITY SOLUTIONS

In this section, we classify and compare the various solutions available or under research for different kinds of attacks which were discussed in the previous sections. These are the solutions which we have encountered during our study/ survey done on this topic. Here, we discuss the solution for each and every attack on an high level. Later, in the final term paper we will be providing the details in depth.

SOLUTIONS FOR PHISHING ATTACKS

Phishing seriously threatens the confidential personal information in current Internet. One of the most important features in phishing attack is that it is difficult for common user to distinguish fake user interface from original interface[9]. Another feature in phishing attack is that there is a key-logger spy-ware which records the key clicks. Latter this information can be accessed by the attacker.

Phishing attack is threatening people's confidence to use the Web to conduct online finance-related activities[13][15]. Below are the few solutions proposed by the researches which are helped in the reduction of such attacks.

One solution for such kind of attacks is SpoofKiller, were the users have to press "home" button when they want to login to web site or application. The operating system then presents the user with a standardized login screen that displays security information and any other relevant security indicators like SSL status[18]. The main challenge for this approach are usability and adoption; users must be convinced to always press the button before supplying a password, and applications and web sites must support this form of password entry.

The second solution is Content Based Filtering where we implement this technique with challenge-response scheme. The combinations of these techniques are needed to improve the traditional spam filtering detection technique on mobile device since the content-based filtering alone is less efficient[15]. Moreover, content-Based filtering can be divided into rule based and statistic based.

The next solution is called Blacklist , this method that need human to verification. Since this technique have very low False Positive, it is widely applied in the industries as antiphishing in toolbar. If user enter the blacklist website, a warning will be appeared. This technique is also not efficient in update and verify the phishing attack database globally[17]. In addition this technique have less capabilities to protect users.

Whitelist is another solution for this attack. Whitelisting method is different from blacklist-based, this technique need to maintain all website in the cyber world. The limitation of this technique is impossible to cover all website[20]. This technique has been implemented by to detect SMS phishing.

SOLUTIONS FOR MALWARE ATTACKS

Malware is capable of many things, such as to steal and transfer the sensitive data stored in the phone like the contacts, credentials. Also, it locks the device, giving access to attackers remotely, sending SMS, MMS or messages etc.

Signature-based detection is one of the most commonly known technique to minimize this type of attacks. Signature-based technique models identifies the presence of the malicious malware using a signatures and uses this signature in the detection process[19]. There will be a repository maintained where all the software will be stored. This repository is considered to be a database where all the signature information is stored, whenever the user tries to identify the presence of malicious behavior, and then this can be searched. To make this detector to be accurate, the database should be updated whenever any new signature is created. The malware signature can be static signature or behaviour signature. This signature-based detection technique is classified into static signature-based detection technique and behaviour signature-based detection technique.

Static signature based detection technique is adopted by the most commercial Antiviruses. The use of this kind of technique is to scan the phone RAM, SD card and then compares the patterns with the detector database. The most common signatures used in this technique are bytesignature and hash-signature. Byte-signature is sequence of hexadecimal bytes that are present in a file or data stream. Byte-signature is very known form of detection and has been used since the first Antivirus detector. It is the most basic and easiest form of signature. Hash-signature is created using a hash function that converts a data into sequence of alpha-numeric characters. The most commonly used hash functions are MD5 and SHA-1. The main disadvantage of such type of attacks are the hash function will change the hash value for the same block which leads to various hash signatures for the same malware. Though Static signature-based technique is an efficient way to identify malwares, it cannot detect unknown malwares and variants of known malwares. Also, we need human intervention to develop these signatures. which is time consuming.

Behaviour signatures are used for complex meta-structures and are more effective to deal with obfuscation techniques such as binary packers, polymorphic, and encryption. This approach is being classified into static behaviour signature and dynamic behaviour signature[16]. In static behaviour signature, the signature is extracted by analyzing the malware code. In dynamic behaviour signature, the signature is extracted from runtime information by executing and monitoring the malware code.

Static Behaviour Signature Technique based on static code analysis technique, which uses information embedded in a given executable file or code templates to capture the functionality of a specific malware. It performs static and dynamic analysis. The static analysis runs on the device, decompresses the apk file, converts their class files into java source code, searches for suspicious patterns and marks them as benign or malicious. Static behaviour signature technique detects malware variants with one signature. It detects malwares before execution and all execution paths are available. The technique limitations are extraction is quite complex and requires several processing steps. It is computationally expensive because of disassembling and scanning big files, and then applies complicated classification algorithms.

Anomaly-based detection technique consists of two phases training phase and detection phase. A profile of system normal behaviour is constructed during the training phase. In detection phase any deviations from this profile are considered as anomalous[21]. This technique can detect unknown malwares and zero-day attacks. However this technique is a costly approach in term of memory usage, communication traffic, CPU computation, and power consumption, because it requires a program to run continuously on the device to monitor the system. Constructing a profile of normal behaviour of a program is not simple especially for complex programs. Anomalybased detection technique is classified into two categories:
a) Static anomaly-based technique, where the normal behaviour profile is constructed from program code static information. b) Dynamic anomaly-based technique, where the normal behaviour profile is constructed from program execution traces[13].

SOLUTIONS FOR NETWORK SPOOFING ATTACKS

Passive Access Point, is a DoC attack is through a Wi-Fi access point without an Internet connection. When an Smartphone enters the coverage area of a wireless router, it is automatically assigned an identifier and loaded into the Wi-Fi stack of the device. If the phone's is enabled with the Wi-Fi connectivity option and incase if the access point is open, it will automatically connect to it. And then it terminates any existing data mobile connections which are being established previous to this connection. Here, the device will never verify the functioning of internet connection over any access points at any time during or after the connectivity process. Therefore, by setting up a Wi-Fi access point that is not connected to the Internet, a
device can be prompted to abandon its mobile broadband data connection to establish another one that does not provide any data. This, in turn, denies the user of any type of data service[15]. The DoC attack can be executed in a variety of ways. One simple approach is through a wireless router that is not connected to the Internet. This method can be implemented with little resources and technical knowledge.

In order to defend such kind of attacks, there are solutions implemented where a network awareness protocol on device is installed in the form of a lightweight app. This app, is called as Wi-Fi Authenticator, automatically verifies that Wi-Fi access points have a functioning Internet connection without the need for any user intervention. To implement such defense mechanism, Wi-Fi Authenticator relies on the following two-step process. Whenever a connection is established with the access point, Wi-Fi authenticator sends a challenge to validation server. if there is no response from the server after certain time, the access point is considered to be invalid.On the other hand, if a response is received, next step is followed where the Wi-Fi Authenticator retrieves a key from the validation response and compares it with a key stored in the device. If the keys match, the access point is considered valid. This step prevents an attacker from easily fooling the authentication protocol by sending an arbitrary response to the challenge. If the Wi-Fi access point is considered invalid in either step, Wi-Fi Authenticator terminates and disables the connection. This prompts the Smartphone to transition back to a mobile broadband data connection returning data services to the victims. Also, it maintains the Wi-Fi capabilities of the device enabled allowing it to connect to other Wi-Fi access points that might become available in the future. In case of fake validation process can fool the above mechanism which cannot prevent the attack. In order address this weakness, we propose a novel network awareness protocol in which the validation key is dynamic. That is, it changes every time a validation test is performed[15]. We achieve this by relying on the smartphone to status validation key validation server validation server content and generate a different key for every validation test it performs. An attacker, therefore, is unable to fool the protocol by supplying the expected response because it is not known by them. This approach consists of five steps involved in the validation of Wi-Fi access point. The first step is to performed after encountering an accessible Wi-Fi access point, the device now generates a key and sends it along with its MAC address to the validation server through the cellular network. Depending on the user's billing agreements, this data can be send as a SMS or TCP package. These details such as the validation key and MAC address together are stored in the Wi-Fi authentication are stored. After connecting from the mobile broadband to the Wi-Fi connection, the smartphone sends a signal to the validation server. Now the validation server responds with the key corresponding to the smartphone's MAC address. Then the new key from the server will be compared against the generated earlier by the smartphone. If equal, the Wi-Fi connection is considered valid. Otherwise, it is considered invalid[19]. Similarly to previous, this validation test is performed automatically without the need for any user intervention. Also, if a Wi-Fi access point is considered invalid, the connection is terminated and disabled. This allows the device to regain Internet services by reconnecting to the mobile broadband while maintaining its Wi-Fi capabilities enabled.

The solutions for the remaining attacks will be detailed in the final term paper.

Apart from the above solutions, the Smartphone user's should follow some techniques to mitigate the security issues.

- To protect personal data, use encryption mechanisms if available.
- Features should be turned off whenever not required.
- Carefully understand the permissions you are giving when you download applications.
- Password protection should be used.
- Install malware protection softwares.
- Be aware of the application's that enable Geo-location.
- Don’t use jailbreak.
- Never connect to unknown wireless networks.
- Wipe the device incase if we are selling the device.
- Apply updates regularly.
- Avoid downloading software or links from unknown sources.

CONCLUSION

In today's world Smartphone's are being widely used but there are many security concerns raising day by day. In this report, we detailed the types of attacks and compared various kind of solutions available to mitigate such kind of attacks. We also provide some best practices which can ensure to reduce the security issues. In the final term paper, we will be discussing further solutions for remaining attacks.

REFERENCES

1) Jaramillo, D.; Newhook, R.; Nassar, N. "Techniques and real world experiences in mobile device security", SOUTHEASTCON 2014, IEEE, On page(s): 1 - 6
2) Milosevic, J.; Dittrich, A.; Ferrante, A.; Malek, M. "A ResourceOptimized Approach to Efficient Early Detection of Mobile Malware", Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, On page(s): 333 - 340
3) “Smartphone security challenges” Yong Wang, Kevin Streff, and Sonell Raman, Dakota State University. December 2012
4) Smartphone malware detection: From a survey towardstaxonomy, Amamra, A. ; Talhi, C. ; Robert, J., Malicious and Unwanted Software (MALWARE), 2012 7th International Conference on DOI: 10.1109/MALWARE.2012.6461012

5) Research in Progress Defending Android Smartphone from malware attacks,Omar,M. ; Dawson,M. AdvancedComputingand Communication Technologies (ACCT), 2013 Third International Conference on DOI: 10.1109/ACCT.2013.69

6) Penning, N.; Hoffman, M.; Nikolai, J.; Yong Wang "Mobile malware security challeges and cloud-based detection", Collaboration Technologies and Systems (CTS), 2014 International Conference on, On page(s): 181 - 188

7) Yong Wang; Vangury, K.; Nikolai, J. "MobileGuardian: A security policy enforcement framework for mobile devices", Collaboration Technologies and Systems (CTS), 2014 International Conference on, On page(s): 197 - 202

8) “Smartphone Security Evaluation”Alexios Mylonas, Stelios Dritsas, Bill Tsoumas and Dimitris Gritzalis Department of Informatics, Athens University of Economics & Business (AUEB)

9) Performance analysis of intrusion detection systems forSmartphone security enhancements Salah, S. ; Abdulhak, S.A. ; Hyontai Sug ; Dae-Ki Kang ; HoonJae Lee Mobile IT Convergence (ICMIC), 2011 International Conference on Publication Year: 2011 , Page(s): 15 - 19

10) Smartphone security evaluation The malware attack case Mylonas, Alexios ; Dritsas, Stelios ; Tsoumas, Bill ; Gritzalis, Dimitris Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on Publication Year: 2011 , Page(s): 25 - 36 http://iacis.org/iis/2013/300_iis_2013_329-335.pdfMilosevic,

11) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/criticalapplications/smartphone-security-1/top-ten-risks/surveillance-attacks http://www.enck.org/pubs/enck-iciss11.pdf

12) Anti-Phishing by Smart Mobile Device,Weili Han ; Yi Wang ; Ye Cao ; Jiping Zhou ; Lixing Wang ,Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on DOI: 10.1109/NPC.2007.68 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.308.6665&rep =rep1&type=pdf

13) R. Dhamija, J. D. Tygar, and M. Hearst. Why Phishing Works. In CHI, 2006.

14) M. Jakobsson and W. Leddy. SpoofKiller. http://www.spoofkiller.com.

15) http://www.markus-jakobsson.com/wpcontent/uploads/SpoofKiller_Markus_Jakobsson_Hossein_Siadati.pdf

16) Mobile Attacks and Defense, Miller, C. ,Security & Privacy, IEEE Volume:9, Issue: 4,DOI: 10.1109/MSP.2011.85

17) Smartphone security awareness: Time to act Al-Hadadi, M. ; Al Shidhani, A. Current Trends in Information Technology (CTIT), 2013 International Conference on DOI: 10.1109/CTIT.2013.6749496

18) How secure is your smartphone: An analysis of smartphone security mechanismsKhan, S. ; Nauman, M. ; Othman, A.T. ; Musa, S. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on DOI: 10.1109/CyberSec.2012.6246082