Academic Journal of Nawroz University (AJNU), Vol.9, No.4, 2020

https://doi.org/10.25007/ajnu.v9n4a989

Threats, Attacks, and Mitigations of Smartphone Security

Hewa Majeed Zangana[1], Marwan Omar [2]

[1] Department of Computer Science, Nawroz University, Duhok, Kurdistan Region of Iraq
[2] Department of Computer Science, Saint Leo University, Florida, USA

ABSTRACT

Mobile devices such as Smart Phones and Personal Assistant Devices (PDA) that are Internet based are becoming much more capable of handling complex tasks such as online shopping, online banking as well as social media networking; However, the security mechanisms and defense measures that are built into those devices are not commensurate with those powerful communication and computational capabilities. This in turn, creates critical vulnerabilities thus promoting the chance for imminent security threats. The intent of this paper is to take a look into some of the vulnerabilities and risks associated with the use of smart phones that are Internet based, explore the current security mechanisms and strategies that are in place, and finally propose some proactive defense strategies to ensure appropriate protection of critical information contained in Smart phone devices.

KEY WORDS: smartphone security, personally identifiable information, malware, Android application security, Smartphone protection mechanisms.

1. Introduction

Recent studies have shown that the number of smart phone devices shipped is expected to rise to 600 million units in 2025 (Kharif, 2009); this is a significant increase from 2009 when the number of smart phone users was about 178 million. The new generation of smart phones is highly capable of handling complex computational tasks such as e-mails, online shopping, and online banking; With this new generation of smart phones comes the increasing ability of running third party software applications on the phones operating system; Having said smart devices- that are Internet based- contain personally identifiable information entices hackers to launch attacks more effectively due to lack of robust security mechanisms. This problem is compounded by the lack of user security awareness. These problems creates a gap in the balance between the high performance and the security vulnerabilities those smart devices expose. Thereby, offering an easy soft target for high profile criminal hackers to cause vandalism and financial losses, not to mention the privacy issues that arise with this type of attacks. As such the main intent of this paper will be to:

- Explore various types of attacks that smart phones users have encountered recently.
- Identify the nature of some of those attacks; take a deep look into the root cause of those harmful attacks.
- Investigate the current state of threats and risks associated with the use of smart phones with Internet connection.
- Present the current state of security counter measures and how ineffective they are in providing the appropriate protection level required for the sensitive data contained in smart phones.

Then the paper will conclude with offering an enhanced security framework that consists of multiple layers of security defenses and a proactive approach to address emerging security risks and challenges associated with the operation of smart phone devices with inter connection.

2. Literature Review

For the last few years, mobile computing has gained

much adoption and momentum by individuals and organizations alike due to the highly powerful computational tasks that mobile devices can handle such as online shopping, online banking, E-mail, web browsing, in addition to many other tasks that truly make the use of hand-held devices both enticing and entertaining. Performing such complex computational activities and transmitting their data via various transmission mediums such as Bluetooth, Internet, SMS (short message service), and Wi-Fi involves communicating some private and sensitive information that would require some level of security to maintain the confidentiality, integrity, and availability of information for authorized users of mobile devices. According to Smart phones experts and researchers; there will be a continuous increase and adoption for smart phones in the next five years; therefore, attackers are on the look-out for this increase to happen because it will open doors of opportunities for them to launch innovative attacks that will mainly target critical personal and financial information contained in those smart devices with Internet connectivity (Leavitt, 2005).

An interesting attack motive for hackers is the ability and applicability of using some of the same attack strategies and mechanisms targeting Personal Computers (PC c) on smart phone operating systems in which not much of security countermeasures are present nor users of smart phones have sufficient security awareness to avoid such attacks. Not to mention the fact that hand-held devices (Smart Phones, I-Phones, and Personal Digital Assistants) introduce new and more security vulnerabilities because of their mobility as well as unattended communication medium. Its equally important to note here that hackers usually target the applications and mediums that are most commonly used and least protected such as e-mails, SMS, games as well as web browsing, which are tools and utilities that are used by typical users of those smart devices with internet connection.

3. Smart Phone's Security Threats

Smart phones are vulnerable to a variety of threats and risks whether they are physical threats such as mechanical damage or loss, in addition to imminent software threats that normally target their operating systems and the application programming interfaces (APIs) supported by operating systems (Schmidt and Albayrak, 2008). Such security threats can pose tough challenges and cause disruption as well as financial loss when using smart phones that are capable of performing web activities that make an easy target for hackers; hackers tend to target smart phones applications by worms, viruses, and Trojan horses thus making the smart phone vulnerable to imminent threats and risks.

Security experts and industry professionals have found that high profile criminals are increasingly targeting smart phones applications due to the immature security approaches that are currently in place, in addition to lack of user's security awareness that collectively creates an allure for hackers to launch attacks seeking personal and financial information that are likely to be found on those hand-held devices (Leavitt, 2005).

Security threats make the battle against hackers tougher because vulnerabilities are not discovered until a period of time after they have been exploited by hackers; at which point they have already caused financial loss, damage, and disruption. This shows that fact that hackers are becoming more adept in directing their attacks toward mobile devices containing financial information such as bank account numbers, credit card numbers as well as social security numbers.

4. A Look at the Top 100 Free Google Play Apps

There is no denying the presence and popularity of the Android operating system (Android). Developed by

Google and released to the public on September 8th, 2008, Android accounts for 85.9% of the global smartphone market share as of 2017 (Statista, 2019). The Android operating system can also be found on television sets (Android TV), in many modern cars (Android Auto), smartwatches (Wear OS), and other consumer electronics such as personal computers, digital cameras, and video game consoles.

Android was designed from the ground up as an open source project. As such, Google created the Android Open Source Project (AOSP), a repository for developers that provides the source code necessary to create their own variants of Android (Google, 2019). This also allowed device manufacturers to make their own unique Android ROMs, providing unique software and hardware combinations to gain a competitive advantage. As of 2015, there are over 18,000 different types of Android devices on sale (Epstein, 2015). As of today, Google (2019) reports this number at over 24,000 different devices.

5. Evolving Threats and Challenges

Kharif,(2009).supports the argument that smart phones are opening doors for bigger security threats as those devices –such as I-Phones and Black Berries-are becoming capable of downloading many third party free applications via Internet without user's knowledge.

Some of the most imminent risks in this regard are normally encountered in the form of viruses, worms, spyware, and Trojan horses that usually penetrate the operating systems and applications programming interfaces (APIs) for smart phone users; those harmful applications, once executed and activated within the OS, they become capable of tracking user's web activity and implement malicious intentions.

Fraud is one of the most commonly encountered security issues associated with the use of smart phones, because many mobile users, nowadays, making deposits to their bank accounts using applications that run on operating system provided by smart phones, in which these smart devices are increasingly becoming more capable of processing such complex computational tasks, this in turn attracts high profile criminals to target aggressively those kinds of financial and personal information.

Channel (2009) indicates that hackers can access smart phones containing confidential and personally identifiable information by simply sending a text message from the phone's service provider. What really makes the risk extreme is the fact that attackers do not have to demonstrate any kind of special technical skills to launch attacks; in addition to a flaw, which many operating systems have that is exemplified by lack of capability to block installation or removal of third party software applications.

6. Smart Phone's Security Risks:

Smart phone's risk exposure is expected to grow bigger as more individuals and businesses increasingly rely on those devices to conduct business activities as well as personal applications such as e-mails, games, and SMS; what really derives people to using smart phones is smart phone's tempting and compelling features represented in processing power (such as downloading games and installing other software), storage capabilities, and increased bandwidth; this in turn, makes those smart devices a repository for personal and financial critical information such as credit card information, social security numbers, and contact details for other people.

Moreover; there are some hidden risks that can be exploited by hackers such as when downloading music files or games applications from trusted websites (such as Apple) in which the downloaded applications reveal (unbeknownst to the user) the list of contact details in smart phones and other confidential information stored in the phones. This creates an allure for cyber criminals

to effectively and relentlessly focus their efforts on attacking Smart phones to gain financial benefits and cause vandalism as well as disruption on both individual and organizational levels.

Category	Appearance	User interaction	Vector	Payload
Virus	Needs a host machine	Usually needed	File transport, file injection, exploit	Several, eg. Replication, modification
Worm	Independent program	Usually not needed	Exploit	Replication and remote access
Trojan horse	Malicious functionalities disguised	Usually needed	File transport, exploit	Remote access, destructive functionalities

Table 1: Viruses Source (Schmidt and Albayrak, 2008)

7. Smartphone Malware

Containing sensitive personal and financial information, Smart phones provide an enticing reason for hackers to produce malicious code that can attack the operating systems of hand-held devices in hopes of gaining unauthorized access to those devices and ultimately attain financial benefits. There are several ways for malicious software to enter the operating system of smart phones such as file injection, boot sector, or file transport. Once the malicious code is activated in the host device (smart phone), it can start executing malicious actions and thereby causing harm and disruption such as file deleting, disable certain critical applications (such as SMS and games), denial of service, and logging key strokes (Schmidt and Albayrak, 2008).

It's important to note that malicious software can appear in three categories: virus, worm, and Trojan horse. A virus is typically transferred to the victim's device via an executable file, once the virus is inside the victim's operating system, it starts executing malicious commands. A worm is an autonomous program used to take up residence in devices and deplete its resources (such as processor and memory) and can spread itself without user's interaction thus degrading the performance of other legitimate critical applications (Brookshear, 2009).

On the other side, a Trojan horse is a program that inserts itself to the operating system as a desirable and beneficial (from the users standpoint) application such as a game. Once the program is inside the system, Trojan horses start implementing malicious-coded activities and in some cases the Trojan horses will just reside inside the system inactive until time arrives for a preselected event. The table below is an excerpt from (Schmidt & Albayrak, 2008) and is used to depict some of malicious software discussed above and their format and appearance when targeting smart phone devices.

8. Attack Vectors and Techniques

The nature of Smart phone devices and the services they provide for their users create some propagation vectors such as SMS/MMS and radio proximity range (blue tooth); hackers can easily propagate Smart phone devices by sending text messages to users of smart phones and seemingly enticing them to open those messages without apparent malicious intentions. Moreover, because SMS and MMS are most widely and frequently used by Smart phone users, attackers are using them as effective infection vectors by sending messages to mobile phone users tempting them to dial a number masquerading as bank or credit card. SMS and MMS could also be used as gateways for spreading spam and propagating the operating systems of smart phones thereby causing financial loss as well as disruption to operating systems (Bose, 2008).

Attacker can also use social engineering techniques that have proven to be effective in trapping unwary users

into revealing their personal information such as phone numbers and e-mail addresses that can be used as pieces of the puzzle when exploiting vulnerabilities and launching vicious attacks.

SMS and MMS are indeed considered as one of the most effectively successful attack vectors because they have long been known as easy and soft attractive targets for high profile criminals. Furthermore, Roy (2008) cites that "Commwarrior, first detected in 2005, is a notable virus that spreads using MMS, The payload deleted users' addresses then propagated using MMS, replicating the application via the phone's Bluetooth wireless interface, Commwarrior also sent SMS and MMS to spam other users". This kind of attack strategy is intended to cause damage, harm, and some financial loss as well because it increases the user's bill when it sends MMS and SMS to other users and causes network traffic peak as well.

Security researchers think that smart phone's software platforms are becoming more vulnerable to attacks because they are flexible enough to provide an environment and a gateway for self-propagating malware. Moreover, smart phones such as Blackberries are available on the hands of teenagers who are very novice and know little or nothing about risks associated with the use of smart phones especially when surfing the Internet. These are factors that generate speculations and raise concerns that smart phones will be a priority target for hackers in the near future.

Antonpoulos (2010) says that the recent security incident happened around Christmas of 2009 when hackers started sending phishing application in the form of a worm that fooled users into installing it as a gateway to access banking websites; this worm application was intended to steal confidential and personal banking accounts information as well as credentials necessary to access back accounts and ultimately caused severe financial losses and identity theft. This incident along with many other security breaches that have happened recently-and are continuing to happen- evidently represent an emergence in malware targeting smart phones and therefore it will require an urgent need for further research and investigation.

It is noteworthy in that the attack vectors and techniques are only likely to increase and the ground battle will intensify because users are more heavily relying on Smart phones to conduct more complex computational tasks and activities, some of which are very attractive for hackers to target, having smart phones that are capable of handling and processing complex computational tasks that include the transaction of critical and personally identifiable information such as online banking, stock trading, and online bills pay all provides a financially lucrative lure for criminals.

One of the most underlying security threats that can be classified as an effective attack vector, associated with smart phone's use that attackers are always on the lookout for is the discouraging fact that Smart phone users are mostly careless and somewhat oblivious about the importance of purchasing and installing security protection software such as malware detection and encryption- those being some of the most basic protection measurements- to ensure appropriate defense and protect the integrity and confidentiality of critical information contained in Smart phone devices.

Given the popularity of Smart phones among users of different groups and ages-we see 12 year olds using I phones and PDAs- on both sides of the spectrum and given the obliviousness as well as lack of security awareness compounded with the dilemma of ineffective security strategies and defense measurements employed currently, to provide some security for smart phones, is certainly not sufficient to protect smart phones users from various kinds of attacks and threats. Therefore, there is an urgent need for further research and

implementation of effective, multilayered proactive protection strategies that take into consideration the emerging threats and evolving attacks. In the coming section, some of those proactive and integrated security approaches will be proposed for implementation.

9. Security Controls and Mitigations

Financial motives create an environment in which attacks on smart phones operating systems become inevitable due to the sensitive personal information in those hand-held devices. This in turn makes the case for some robust security and defense strategies to ensure appropriate protection of sensitive data; traditional protection measures such as anti-virus, anti-malware, encryption, and authentication techniques have not been able to live up to the tough challenges posed by cyber criminals in which they become more adept each day and launch new attacks in such innovative and effective manners.

Some of the traditionally used tools to protect Smart phones from malicious attacks include the virus scanner that is used to match the signature of applications against a list of signatures that are already in the system for malware such as viruses, worm, and Trojan horses. This tool cannot provide effective protection for Smart phones because it limits its benefit to a list of known malware and would not be able to detect nor prevent any malware that is not in that list.

Some of the basic defense measures that can be implemented to harden the security of Smart phones include enabling password protection at the start-up time, locking down Bluetooth connection by default to prevent connection with other unknown devices in the range, encrypting important data inside the device to prevent leakage if it were to be stolen, avoid the installation of third party applications from unknown sites, and downloading the latest security updates from the service provider's website to ensure appropriate protection against evolving Smart phone attacks and threats.

In order to accurately provide the needed protection for Smart phones, a combination of factors has to intertwine including: designing an integrated, multi-layered, real time, and proactive security strategy, improve security awareness for Smart phone users, implement enhanced password protection techniques, and use of malware detection software.

An effective approach is suggested by Schmidt and Albayrak (2008) in which an intrusion detection system or intrusion prevention system can be used to monitor network traffic for abnormal behavior during data transmission between Smart phones; so when suspected behavior of data activity is detected /noticed by network administrator, appropriate countermeasure can be applied such as port closing on the user side using Smart phone. In fact, intrusion prevention system can automatically take defensive actions against abusive network behavior or what is suspected to be malicious.

There have been some other solutions for Smart phones malware attacks such as virus scan software that can scan all data received in the hand help device; such virus scanner can automatically and constantly scan the device for all data transmissions. Once suspected data is identified, user gets alerts and is offered to delete the data containing threats or even save it as quarantine.

Albawaba (2008) presents the latest ESET Smart phone anti-virus produced by ESEST as one of the most innovative security solutions for mobile devices; this anti-virus (as cited by albawaba (2008)) provides an effective approach for proactively detecting the most sophisticated malware attacks without reducing the hand set device's performance.

This anti-virus software is capable of providing heuristic detection for present and future risks via ESET'S threat engine, folder scanning feature, and most

important, ESET mobile anti-virus, unlike any previous mobile anti-virus, is capable of decoding and analyzing executable code in a virtual environment in real time thereby differentiating malicious code from legitimate one. This technology is considered to be very pioneering and advanced because it's the only one of its kind to provide such innovative technique for real time protection against most-cleverly designed malware attacks.

One of the other mitigations that can be considered as a good protection practice is the use of encryption techniques to encrypt sensitive data being transmitted during transactions such as when doing online banking or online shopping; using encryption tools will also support the authentication process necessary to ensure that only authorized users can access critical data on smart phones operating systems.

It's important to note that many of the protection approaches and defense strategies are based on using some kind of protection platform such as an Intrusion Detection System or Anomaly Detection System are achieved on the server side and this could undermine the robustness of smart phones security because best and most appropriate protection can be provided in real time and that is when it's being done on the smart phone side.

In short, there is a critical need to develop some kind of defense strategy in which protection can be provided on multiple layers in real time with robust security controls so that suspicious behavior for malware intentions can be detected and prevented with minimal effect while preserving the performance and processing capabilities of Smart phone devices.

The open marketplace philosophy of the Google Play store, while enticing to new developers and those without the resources to develop for Apple's app store, is an easy target for malicious actors. With a significant lead in market share adoption, the threat of mobile malware on the Google Play store will only increase. Knowing this, Google built a malware scanner called Google Play protect that uses machine learning to improve detection. However, in the case of these apps, Hello Launcher was downloaded enough times to be on the top 100 free app list before Google detected the app and removed it from the Google Play store. As such, a scanner acting as oversight to an app' activity is not enough of a barrier to prevent malware from distributing on the Google Play store.

The researchers suggest that Google, like Apple, curates a verified-safe top 100 list instead of relying on the number of times an application has been downloaded and reviewed.

10. Results

Since Android is a free, open-source platform, it allows any developer to submit and upload apps to the Android Market with no restrictions enforced to determine the legitimacy of those apps. On one hand, this is a great benefit of having an open-source system that encourages developers and users to interact and exploit the advantages of this platform. On the other hand, this provides an opportunity for hackers to mask their malicious apps and submit them to the Android Market as benign and legitimate apps and make some of them freely available for download by end users.

The central issue lies at the heart of the Android permission mechanism, which is not capable of blocking malicious apps from accessing sensitive phone resources (contact info, browsing history credentials, and bank login credentials). The current permission technique either allows or disallows apps from accessing the resources requested by the app at the installation time, but it fails to reverse the granted permission if the underlying app was deemed malicious or illegitimate. It must be noted, however, that Android's sandboxing mechanism makes Android one of the more secure

platforms by separating applications and processes from each other and enforcing each app to be executed in its own sandbox, thereby minimizing the risk of unauthorized access by other apps to sensitive phone resources.

Furthermore, survey results showed that many Android users download and install apps on a regular daily basis, and they reported a level of uncertainty about their confidence in the security of apps they download. The current permission mechanism is discretionary in nature, meaning that Android users have to decide whether to grant apps the permissions they need to be installed, which increases the security burden on users.

The rapid increase in the number of apps downloaded every day makes the current security system unable to cope with the malware risks, and therefore, it becomes very easy for hackers to develop and distribute malicious content that seems to be in its infancy stage. Although mobile malware that targets smartphones has been around since 2004, there have not been any major malware outbreaks yet. However, there have been many security incidents targeting Android phones recently, and since business organizations, government agencies, and academia are increasingly allowing their employees to access network resources using smartphones as a tool to enable productivity, this will certainly appeal to hackers and motivate them to shift their efforts towards this growing and rich industry.

It is noteworthy that survey findings also highlighted some points that were inconsistent with the literature in that only about 8% of respondents stated that they had experienced issues with their Android smartphones (e.g., unable to access the internet or send/receive SMS) after downloading apps. Maybe this is ascribed to the fact that users do understand and realize the security implications of downloading and installing apps; this was apparent in their responses to a survey question where 76% did confirm that they carefully read and understand the permissions granted to apps before installing them on their Android smartphones.

11. Conclusion

The forgone discussion has explored extensively the security aspects of Smart phones including the various threats and risks associated with their use as well as the mitigations and controls necessary to stop attacks launched by a community of cyber high profile hackers who are versed in the attack vector and understand the nature of vulnerabilities existed in the operating systems of Smart phones. Current defense strategies such as traditional virus scanner and ineffective authentication techniques are not capable of withstanding attacks because they do not provide any kind of proactive approach to protect critical financial information contained in Smart phones; also lack of security awareness by users of Smart phones further increases the dilemma of ensuring appropriate protection is deployed. Therefore, the results have been severe financial losses in thousands of dollars, disruption in operating systems and applications as well as vandalism. To mitigate this issue, proactive, integrated, and real time security approach needs to be implemented such as real time virus scanners, to detect threats in real time and fend them off as well as intrusion detection system to detect suspicious data activities and take actions to prevent attacks.

References

1. Antonopoulos, A. (2010). "Mobile malware will test Android and iPhone." Network World **27**(2): 18-18.
2. Bose, A 2008. "*Propagation, detection and containment of mobile malware*". Ph.D. dissertation, University of Michigan, United States -- Michigan. Retrieved February 7, 2010, from www.phoenic.edu/apololibrary.Full Text.(Publication No. AAT 3328771)
3. Brookshear, J (2009). "*Computer science, an overview*" . Boston, Addison-Wesley Computing. 10th Edition.

4. Channel (2009). "Hacking Threat Faces Mobile Phone Users, Experts Say." Retrieved Feb 3rd, 2010, from Channel Insider: 1-1.
5. ESET Launched Antivirus For Smart phones. (2008, June 18). Al Bawaba. Retrieved February 21, 2010, from ABI/INFORM Trade & Industry. (Document ID: 1496481391).
6. 6-Kharif, O. (2009). "Smart phones: A Bigger Target for Security Threats." BusinessWeek Online: 11-11.
7. Leavitt (2005), Mobile Phones: " *The Next Frontier for Hackers?".* Retrieved Feb 3rd , 2010, from IEEE Computer 38(4)(2005)20-30.
8. Schmidt & Albayrak (2008). "*Malicious Software for Smart phones*" retrieved Feb 2nd, 2010, from http://web.ebscohost.com.ezproxy.apollolibrary.com.
9. Schmidt, A.-D., F. Peters, et al. (2009). "Monitoring Smart phones for Anomaly Detection." Retrieved Feb 3rd, 2010, from Mobile Networks and Applications **14**(1): 92-106.
10. Epstein, Z. (2015, April 15). 500? 1,000? You'll never guess how many different Android devices are available. Retrieved from https://bgr.com/2015/04/15/android-sales-2015-smartphones-tablets-smartwatches/
11. Google. (2019). Android Open Source Project. Retrieved May 17, 2019, from https://source.android.com/
12. Google. (2019). Devices. Retrieved May 17, 2019, from https://www.android.com/devices/
13. Statista. (2019). Global market share held by smartphone operating systems from 2009 to 2017. Retrieved May 17, 2019, from https://www-statista-com.saintleo.idm.oclc.org/statistics/263453/global-market-share-held-by-smartphone-operating-systems/