Mobile Security: A Literature Review

Cassandra Beyer
SA IT Services
1950 Roswell Rd
Marietta, GA 30068

ABSTRACT

The following paper is a literature review on the topic of Mobile Security. The topic has been chosen due to the rise in mobile applications and the insufficient rise in the topic of the security within those applications.

For the purposes of this paper, mobile devices are considered as *tablet and cell phones which run a mobile Operating System (OS)*. More specifically, these are Android (Google), iOS (Apple), or BlackBerry OS (RIM). While it is important to note these terms, this literature review is focused primarily on the Android OS security vulnerabilities. Polymorphic is defined as malware that transforms to be somewhat different than the one before. The automated modifications in code do not modify the malware's functionality, but they can render conventional anti-virus detection technology ineffective against them. An attack vector is most basically described as the approach utilized to assault a specific technology (i.e. a path taken to compromise a system). A botnet is a collection of "zombies" which are remotely controlled for malicious or financial gains [1]. A single botnet often contains hundreds or thousands of devices. When the term "vulnerability" is being utilized within this paper, it is a weak spot which allows an attacker to decrease a system's security. A vulnerability occurs when three elements intersect, including a system weakness or flaw, attacker *access* to the flaw, and attacker competence to exploit the flaw [2].

Keywords

Mobile, Security, polymorphic, smartphones, Android, IOS, Blackberry, Google, Anti-virus, BYOD, Botnet, Vulnerability, Information Technology, ISA

1. INTRODUCTION

Mobile device security has become more critical as businesses begin to rely on these devices for everyday processes. Nonetheless, the security for these devices has been established as nonexistent. On average, only 10% of the approximately 86 million devices in use today are secured [3]. The securing of these mobile devices for both personal and business use has become a frequent hot button topic in the news, but little to no research has been presented on how to solve this problem. In particular, Android security has been a topic of discussion as Android devices have risen drastically in the last few years. In the last year alone, device activations have risen 250% and app downloads from Google's "Play" market have topped 11 billion and counting [4].

2. IMPORTANCE OF MOBILE SECURITY

According to the journal's 2012 Strategic Security Survey, 69% of respondents believe that mobile devices present a current threat to the corporate environment, where 21% believe it has the potential to pose a threat in the future [5]. Two major concerns came up, both device loss/theft that could compromise due to the data held on it, and the network being compromised by an infected device being brought into the network. The policies that manage BYOD (bring your own device) vary greatly by company, but most (86%) of survey takers allow personally owned devices in the network [5]. It is unclear who the respondents to the survey are (IT managers, CTO's, CEO's etc.?). Regardless, the information establishes proof of importance that mobile device security is a current, if not future, concern.

On the same topic, mobile device security is an increasing topic of concern for enterprise networks. Phones have the capability to be "locked down" but corporations rarely do so due to employee complaints and upkeep. BYOD is an ongoing security concern, due to the fact that the devices can't be fully secured, and user intervention can easily overcome many locking mechanisms and applications. Network Access Control is usually considered the "best" way to control these devices but this also has significant faults. Surprisingly, college and academic campuses have been encountering – and conquering – the BYOD world long before enterprises have suffered its effects, suggesting we should look to them – *not enterprises* – for answers [5].

To understand the impact of a lack of mobile security, we need to understand how smartphones are most commonly being used. Smartphone usage has become so varied it would be near impossible to document every available usage of the mobile phone. As previously noted, the "Google Play" market has over 11 million apps [4]. However, it is considered common knowledge that mobile banking is available through many major (and some smaller) banking industries. When we consider mobile payments and the security that is required before a user should trust a mobile smartphone or tablet with their personal data, especially payment information, we must consider current saturation levels of mobile payment methods in usage today [6]. The dynamic way in which mobile payments have been utilized and depends largely on non-mathematical data, such as how a user "feels" about a subject and/or their current time availabilities [6]. In addition, whether another option is presented can greatly impact whether a user accepts the pathway of mobile payments. Regardless, this remains to be a large security concern for mobile usage which has gone largely undiscussed in the academic world.

3. MOBILE SECURITY: A LITERATURE REVIEW

3.1 Overview

Utilizing EBSCO and ProQuest, a search of scholarly publications (journal articles and dissertations) that contain "mobile security" in its title returns 231 results, a surprisingly low number. 33% of these (76 articles) were written in the last year, which suggests a significant rise in the research of mobile security. Even more surprising, a search of scholarly publications containing "Android Security" in the title results in a 154% increase of articles, with 356 articles returned, and 87% (310 articles) being written in the last year. Intriguingly, not one of these articles searched claim any security benefits to Android security, rather all articles discuss vulnerabilities.

The idea of information at our fingertips anytime and anywhere can be highly appealing. Due to the nature of apps behaving in swarms (i.e. checking in regularly) most apps behave in the same way as a bot would on a computer. Therefore detection mechanisms used to detect bots on computers are irrelevant to mobile phones. In today's day and age, where 230,000 open source SourceForge mobile software development projects have been used since 2009, it seems as though we don't ask the question "At what cost?" [7].

3.2 Android Security… A closer look.

There are two primary attack vectors for mobile phones. The first is when a mobile phone connects the internet; the second is when a mobile phone connects to a network. Because so much personal and financial data is being fielded on a phone, this is making the mobile phone environment more and more appealing to hackers. In 2010, McAfee labs reported a 46% increase in mobile phone security, and more than 55,000 new mobile malware strains are being found every day at the labs [8]. While PC's are steadily being utilized to launch mobile botnets, the primary focus of mobile malware is inclined toward stealing money and private data [8].

Similarly, the rise of android botnets has been an ongoing issue that has risen in discussion over the last year [9]. The above referenced author, Marko, accurately relates the idea of an Android botnet to a traveling salesman with tuberculosis, due to the itinerant nature of smartphones. Lastly, and perhaps more seriously, it is not uncommon for these mobile devices to then join a corporate network, expanding their capabilities and bandwidth beyond that of a mobile network [9]. There are very apparent security risks being taken without proper realization that it is a consequence of this "information at our fingertips" service being rendered by mobile device usage. There are a few *current* Android threats, as discussed in the following paragraphs.

Symantec investigator Mario Ballano stated he has found a new attack vector on Android, similar to Windows DLL hijacking [10]. This isn't a fault in the OS as much as susceptibility in some apps that load code dynamically using the Android classes Public Constructors and DexClassLoader. Ballano stated he has informed Google regarding the small number of apps he discovered that are vulnerable to this method. It is currently unclear as to Google's reaction to the vulnerability and it has not yet been patched as of November 2012.

False online "Google Play" stores are another attack vector for Android phones. Lookout software engineer Tim Wyatt tells us that software infected with the GGtracker Trojan, dispersed through the false online stores, is able to enroll victims in premium-rate SMS services without asking for permission, or even notifying the user that the transaction has occurred [10].

While it's been proven that malware can send and receive malware messages without the user ever knowing (see above), a new study at TrendMicro Labs tells us that a new strain of malware is utilizing Android phones as SMS relays [11]. This can then be utilized to enroll the user in premium services, or as a spy to upload all messages sent to the phone to also be uploaded to an offsite server. Trend Micro's report doesn't go into detail on perhaps the most frightening use of this vulnerability… this can be utilized as a sort of "proxy server" to send SMS messages… kidnappers, terrorists or even C&C type malware can all receive these text messages safely without ever being able to trace where they came from.

Cloned apps are another attack vector within Android Security. There is little to no information regarding how Android app repackaging could be utilized as an attack vector, but a recent report from F-secure sheds a little light on the issue. Reverse engineering Android applications is not necessarily hard, as Java is inherently transparent, so concern for "fake" android programs has been a hot topic for security often [12]. You hear it warned often that phones should not download apps from outside of the Google "Play" store. Unfortunately, Android apps can repackage to "look" and feel and even use the same base code as friendly apps – but are actually repackaged to include malware. The most common non-malicious repackaging is to reproduce "new" applications that are similar but slightly different than the original (i.e. "paid" versions of free apps or free versions of paid apps) [12]. There is not a known case where an application was repackaged to include malicious code, but the possibility has been demonstrated to exist.

Finally and perhaps the most threatening attack vector: a physical attack on a mobile Android device can be performed with little to no "hacker" skills. Within 30 seconds, the security of the phone can be compromised, grabbing passwords as well as personal information, then pushing a covert app onto the phone to perform security holes at a later date [13]. The "vulnerabilities" created use nothing more than the Android ADM framework's innate abilities to perform the attack.

4. SOLUTIONS PRESENTED

There are no clear solutions presented to the Android Security issues above. All cryptology (or security protection of information) is based on two factors: something you know and something you own. An access card and a password are perfect depictions of this scenario. Many times, just one of these items is needed, and sometimes in the most secure of places, both are needed. With mobile computing has become a storehouse for all things personal (from bank accounts to email addresses and phone numbers), the need for a simple but effective biometric solution has risen exponentially [14]. In addition malware detection services currently use a higher battery footprint than most applications, causing users to disable any security that had been previously implemented [15]. If malware protection was more energy aware and used less battery, it is more likely users would leave these protection services on.

Polymorphic malware has an infamous rep in the PC world, with new algorithms being drawn up seemingly every month to detect and stop malware strains. The issue of categorizing polymorphic malware is a consistent, ongoing challenge. As new methods are developed to thwart polymorphic malware, new ideas are conceptualized on how to thwart the new detection methods. A recent dissertation presented on polymorphic malware presents some conclusive findings on detection of polymorphic malware on the PC [16]. It is conclusive due to the fact it took 645 features of both clean and "dirty" programs and refined it down to seven carefully selected features. This allows for a significantly higher rate of successful classification (both in classifying dirty programs as dirty as well as classification of clean programs as clean). Unfortunately, this research is very narrow and therefore presents a disadvantage due to the results only being applicable in the specific scenarios presented (i.e. *polymorphic malware on a PC*). Because mobile apps behave “naturally” in swarms, with frequent updates and code changes, all current research on polymorphic malware is not likely to be applicable to the mobile platform environment.

While no clear solutions are being presented, it is clear that there is a need for more data. When security breaches happen, there are no current mandates that require the reporting of these breaches. In fact, in January 2012 alone there was 213 security breaches reported, yet only 78 of those reported one or more attributes about the data being stolen [17]. This means we have no data about the breach, rendering the reporting itself nearly pointless. It is clear that with a lack of a required national reporting mandates, that many data breaches will still be unreported, or under-reported, and it would seem that the state of affairs is continuing to grow worse. The breaches where data *was* reported contain interesting data. Healthcare breaches have increased from 17% to 27% of data breeches, banking industry breaches have dropped from 8% to 4%, and subcontracting breaches have doubled, from 7% to 14% [17]. The report also indicates hacking-based attacks have increased, while insider theft is down. This indicates the hacking industry is on the rise, which means if the increase continues at the current rate, it will be a record high in the category. No mobile breaches have been officially reported, although it can be speculated that they exist within the 76% of unattributed breaches [17].

5. CONCLUSION

There appears to be a distinct lack of literature regarding Android security, especially polymorphic and botnet related security. The number of articles written has risen significantly, but not as much as would be expected considering the rise in mobile smartphone usage worldwide. Lastly, there are no clear solutions presented to the Android Security issues, which leaves an area clear of opportunity for future scholarly research.

6. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards this paper, especially toward Capella University for providing editing services as well as an electronic resource database with which to perform the literature review.

7. REFERENCES

[1] “Glossary,” May 2005. [Online]. Available: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00333.html. [Accessed 4 November 2012].

[2] “The Three Tenents of Cyber Security,” n.d.. [Online]. Available: http://www.spi.dod.mil/tenets.htm. [Accessed 4 November 2012].

[3] T. Blitz, "Decoding mobile device security," *Security,* vol. 5, no. 42, pp. 46-47, 2005.

[4] Google Mobile Blog, “Android and Security,” 2 February 2012. [Online]. Available: http://googlemobile.blogspot.com/2012/02/android-and-security.html. [Accessed 4 November 2012].

[5] M. Finneran, "Mobile security gaps abound," *InformationWeek,* vol. 1333, pp. 26-29, 2012.

[6] N. Mallat, "Exploring consumer adoption of mobile payment - A qualitative study," *The Journal of Strategic Information Systems,* vol. 16, no. 4, pp. 413-432, Decmeber 2007.

[7] G. Hurlburt, J. Voas and K. W. Miller, "Mobile-app addiction: Threat to security?," *IT Professional Magazine,* vol. 6, no. 13, pp. 9-11, 2011.

[8] N. Leavitt, "Mobile security: Finally a serious problem," *Computer,* vol. 6, no. 44, pp. 11-14, 2011.

[9] K. Marko, "Rise of android botnets.," *Informationweek - Online,* 2011.

[10] "More mobile security glitches," *Computer Fraud & Security,* no. 7, p. 3, 2011.

[11] M. Balanza, "Android malware acts as an SMS relay," Trend Micro Labs, 2011.

[12] ThreatInsight, "Cloned Android Apps: Symbiosis or Parasitic?," F-Secure, 2011.

[13] Hak5, "Extreme android and google auth hacking with kos," Hak5, 2012.

[14] J. Hu, V. Bhagavatula, M. Bennamoun and K. Toh, "Biometric security for mobile computing," *Security & Communication Networks,* vol. 5, no. 4, pp. 483-486, 2011.

[15] J. E. Bickford, "Rootkits on smart phones: Attacks, implications, and energy-aware defense techniques," Rutgers The State University of New Jersey, New Brunswick, 2012.

[16] K. Raman, "Towards classification of polymorphic malware," University of California, Irvine, 2011.

[17] The Identity Theft Resource Center, "Breaches: Knowing less and less about less and less," The Identity Theft Resource Center, 2012.