Mobile Malware and Smart Device Security: Trends, Challenges and Solutions

ARABO, Abdullahi and PRANGGONO, Bernardi <http://orcid.org/0000-0002-2992-697X>

Mobile Malware and Smart Device Security: Trends, Challenges and Solutions

Abdullahi Arabo[α] and Bernardi Pranggono[β]
[α]*The Oxford Internet Institute (OII), Oxford University, Oxford, OX1 3JS, U.K.*
[β]*School of Engineering and Built Environment, Glasgow Caledonian University, Glasgow, G4 0BA, U.K.*

Abstract **— This work is part of the research to study trends and challenges of cyber security to smart devices in smart homes. We have seen the development and demand for seamless interconnectivity of smart devices to provide various functionality and abilities to users. While these devices provide more features and functionality, they also introduce new risks and threats. Subsequently, current cyber security issues related to smart devices are discussed and analyzed. The paper begins with related background and motivation. We identified mobile malware as one of the main issue in the smart devices' security. In the near future, mobile smart device users can expect to see a striking increase in malware and notable advancements in malware-related attacks, particularly on the Android platform as the user base has grown exponentially. We discuss and analyzed mobile malware in details and identified challenges and future trends in this area. Then we propose and discuss an integrated security solution for cyber security in smart devices to tackle the issue.**

Index **— Botnet, cyber security, mobile malware, security framework, smart device security**

I. INTRODUCTION

The Internet is one of the most remarkable developments to have happened to mankind in the last 100 years. The development of ubiquitous computing makes things even more interesting as it has given us the possibility to utilise devices and technology in unusual ways. We have seen the development and demand for seamless interconnectivity of smart devices to provide various functionalities and abilities to users. But we also know the vulnerabilities that exist within this ecosystem. However, these vulnerabilities are normally considered for larger infrastructures and little attention has been paid to the cyber security threats from the usage and power of smart devices as a result of the Internet of Things (IoT) technologies. In the IoT vision, every physical object has a virtual component that can produce and consume services. Smart spaces are becoming interconnected with powerful smart devices (smartphones, tablets, etc.). On the other hand, we also have the backbone, the power grid that powers our nations. These two phenomena are coming at the same time. The increased usage of smart meters in our homes or businesses provides an avenue of connectivity as well as powerful home services or interconnected powerful smart devices. The example of the smart grid also provides the means of controlling and monitoring smart grid infrastructures via the use of portable smart devices.

The vulnerability of the connected home and developments within the energy industry's new wireless smart grid are exposed to the wrong people; it will inevitably lead to lights out for everyone. This will eventually uncover the multitude of interconnected smart devices in the IoT as a hotbed for cyber-attacks or robot networks (botnets) and a security nightmare for smart space users and possibly for national infrastructures as a whole.

The latest research has reported that on average people own three internet-connected smart devices such as smartphones and tablets [1]. Therefore, as a result of the ubiquity of smart devices, and their evolution as computing platforms, as well as the powerful processors embedded in smart devices, has made them suitable objects for inclusion in a botnet. Botnets of mobile devices (also known as mobile botnets) are a group of compromised smart devices that are remotely controlled by bot-masters via command-and-control (C&C) channels. Mobile botnets have different characteristics in several aspects as compared to PC-based botnets, such as their C&C channels medium.

PC-based botnets are seen as the most common platforms for security attacks, and mobile botnets are seen as less of a threat in comparison to their counterparts. This is so for different reasons, such as limited battery power, resource issues, and Internet access constraints, etc. Therefore, the efforts directed to both the manifestation of operating mobile botnets and corresponding research and development endeavours are not as wide as for PC-based botnets. However, this development could change with the recent surge in popularity and use of smart devices. Smart devices are now widely used by billions of users due to their enhanced computing ability, practicality and efficient Internet access, thanks to advancement in solid-state technologies.

Moreover, smart devices typically contain a large amount of sensitive personal and corporate data and are often used in online payments and other sensitive transactions. The wide spread use of open-source smart device platforms such as Android and third-party applications made available to the public also provides more opportunities and attractions for malware creators. Therefore, for now and the near future smart devices will become one of the most lucrative targets for cybercriminals.

The main focus of this paper is threefold: firstly to highlight the possible threats and vulnerability of smart devices, secondly to analyse the challenges involved in detecting mobile malware in smart devices and finally to propose a general security solution that will facilitate solving or addressing such threats. The rest of the paper is organized as follows. In section II we provide a detailed analysis of the security threats on smart

devices and their links with cyber security. We have identified mobile malware as one of the main issues and we discuss it in more detail in Section III. Section IV provides our proposed security solution that will be able to deter the problems of mobile malware. The paper is concluded in section V.

II. Security Threats on Smart Devices

The weakest link in any IT security chain is the user. The human factor is the most challenging aspect of mobile device security. Home users generally assume that everything will work just as it should, relying on a device's default settings without referring to complex technical manuals. Therefore service content providers and hardware vendors need to be aware of their responsibilities in maintaining network security and content management on the devices they provide. Service providers might also have the opportunity to provide add-on security services to complement the weaknesses of the devices.

The issue of cyber security is much closer to the home environment than has been usually understood; hence, the problem of cyber security extends beyond computers it is also a threat to portable devices. Many electronic devices used at home are practically as powerful as a computer - from mobile phones, video consoles, game consoles and car navigation systems. While these devices are portable, provide more features and functionality, they also introduce new risks.

These devices previously considered as secure can be an easy target for assailants. The information stored and managed within such devices and home networks forms part of an individual's Critical Information Infrastructure (CII) [2] as identified by the POSTnote on cyber security in the UK. For example, an attacker may be able to compromise a smart device with a virus, to access the data on the device. Not only do these activities have implications for personal information, but they could also have serious consequences if corporate information were also stored on the smart device.

The use of mobile devices in healthcare is also more common these days, such as in mobile-health. A typical example is having a health device connected to the home network, which is capable of transmitting data wirelessly to hospitals and other relevant parties. Most of the manufacturers of these devices do not put much effort in trying to make sure that the devices are secure. If these devices are compromised not only will the information and privacy of the user of the device be compromised, but the attacker can even change the settings of the devices, which could lead to harmful consequences. It has been shown that it is possible to hack into a pacemaker and read the details of data stored in the device such as names and medical data without having direct access to the devices simply by standing nearby [3].

Therefore, it is also possible to reconfigure the parameters of the device. This is not only applicable to medical devices, but also to any devices that are used within the home network for any purpose.

According to the Juniper Networks report [4], 76 percent of mobile users depend on their mobile devices to access their most sensitive personal information, such as online banking or personal medical information. This trend is even more noticeable with those who also use their personal mobile devices for business purposes. Nearly nine in ten (89 percent) business users report that they use their mobile device to access sensitive work-related information.

Another more worrying impact is when cybercriminals use the vast resources of the network to turn it into a botnet and launch a cyber-attack on national critical infrastructures. There are some Android applications that when downloaded from a third party market (not the Android market) are capable of accessing the root functionality of devices ("rooted") and turning them into botnet soldiers without the user's explicit consent.

People could easily and unwittingly download malware to their smart devices or fall prey to "man-in-the-middle" attacks where cyber-criminals pose as a legitimate body, intercept and harvest sensitive information for malicious use. In 2011, there was a mix of Android applications removed from the Android Market because they contained malware. There were over 50 infected applications - these applications were copies of "legitimate" applications from legitimate publishers that were modified to include two root exploits and a rogue application downloader.

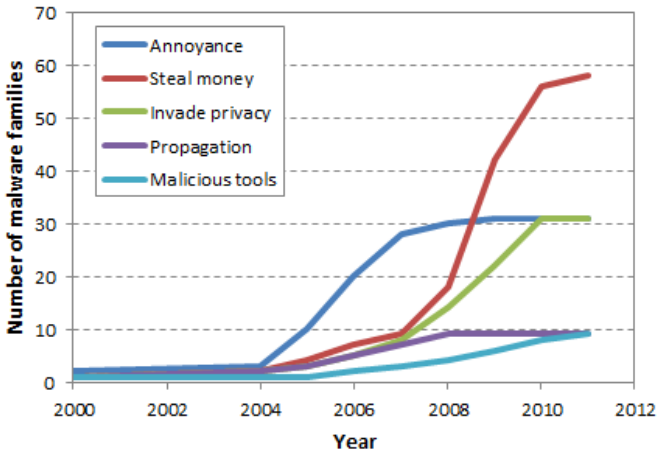

Figure 1. Number of malware families in 2000-2011 (source: Fortinet)

The Juniper Networks Mobile Threat Centre (MTC) reported that in 2011 there was an unparalleled increase in mobile malware attacks, with a 155 percent increase from the previous year across all platforms [5]. It is also reported that Android malware experienced an increase of 3,325 percent in 2011. Notable in these findings is a significant number of malware samples obtained from third-party applications which do not enjoy the benefit or protection Google Play Store scanning techniques. Previously, an Android developer could post an application to the official Android Market and have it available immediately, without inspection or vetting to block pirated or malicious applications.

This increase in malware is mainly due to the combination of Google Android's dominant market share in smartphone (68.8 percent in 2012) and the lack of security control over the applications appearing in the various Android application markets. It was reported recently that Google Play store, which

has more than 700,000 apps just passed 15 billion downloads. Security firm Fortinet estimated that money-stealing malware has increased exponentially in 2006-2011 as shown in Figure 1. Based on an estimation by Kaspersky Lab, cybercriminals who target smart devices like smartphones earn from $1,000 to $5,000 per day per person. Mobile phone hacking is also getting more attractive with the rise of the Near-Field Communication technology (NFC), which expands the use of smart devices as e-wallet or helps people to read product information.

In December 2011 alone, Kaspersky Lab discovered more than 1,000 new Trojans targeting smartphones. That is more than all the smartphone viruses spotted during 2003-2010. This trend is continuing; in 2012, the number of cyber-attacks targeting mobile devices increased exponentially during the first quarter, as reported by security firm Trend Micro [6].

Their report identified approximately 5,000 new malicious Android applications in just the first three months of the year, mainly due to the increase of the Android user base. The research also pointed out a marked escalation in the number of active advanced persistent threat (APT) campaigns currently being mounted against companies and governments. APT is a cyber-attack launched by a group of sophisticated, determined, and coordinated attackers who systematically compromise the network of a specific target or entity for a prolonged period. Security researchers see APT in different ways, while some researchers regard APT as different type of attack; others just categorize it as a more organized botnet with more resources behind it.

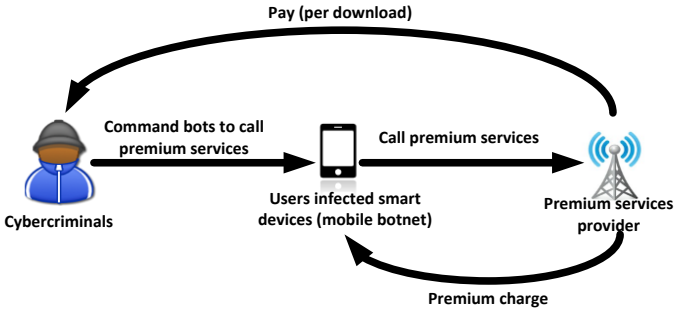

Figure 2. Premium calls abuse

Malware developments that targets smart home devices have several known monetization factors. Most malwares are aimed at mobile pick pocketing (short message service (SMS) or call fraud) or the ability to charge premium bills via SMS or calls, as illustrated in Figure 2. Some malware are used as part of botnet creations. Malwares like DreamDroid (or DroidDream) [7] have integrated thousands of mobile devices into extensive botnets. Some of the malwares are developed to exploit vulnerabilities on either the operating systems (OS), installed applications, or just to create trouble to user information.

Home devices and general consumer electronics are progressively becoming more advanced and are capable of connecting with other devices over a network. While it may sound unreal, devices such as TVs, digital picture frames, smart meters and e-readers are quite vulnerable and absolutely capable of causing problems on your network. The next few years will provide opportunities for various types of malware developers to explore unlikely methods of achieving their goals. Smartphones are not invulnerable and Macs can get malware, such as the CVE-2012-0507 vulnerability [8].

Luigi Auriemma in [9] has uncovered a vulnerability in a Samsung D6000 high definition (HD) TV that caused it to get stuck in an endless loop of restarts. Auriemma's report followed another denial-of-service (DoS) vulnerability in Sony Bravia TVs uncovered by Gabriel Menezes Nunes [10] which stops users from changing the volume, channels or access any functions.

In the 2012 first quarterly report from Trend Micro [11], it was pointed out that the large diffusion of mobile devices and the increase in awareness of the principal cyber threats have resulted in an increase in the interest of cybercrime in the mobile sector. Another significant interest is concentrated on the threat in terms of the rapid spread of botnets based on mobile devices, favored by the total almost absence of protection and the difficulty of tracing the agents composing the network. If these exploits are targeted by well-established hacker groups such as Anonymous, it will pose a bigger threat to organizations and smart environments that protect highly sensitive data, targeting companies and individuals for various political and financial reasons.

III. MOBILE MALWARE

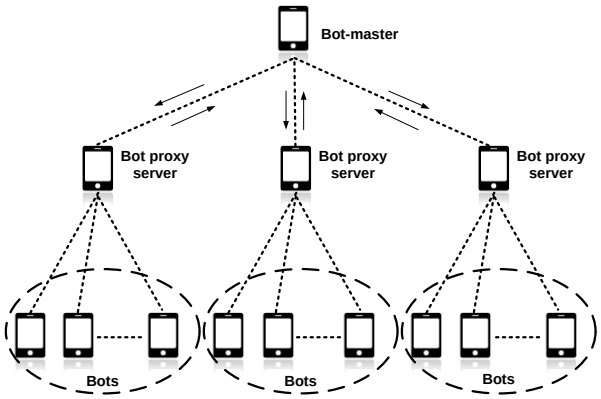

Figure 3. Botnet Command & Control

One of the major and most common problems in today's Internet is malware. Among these malware, Botnets are considered as the biggest challenge. Botnets are used to send email spam, carry out distributed denial of services (DDoS) attacks, and for hosting phishing and malware sites. Botnets are slowly moving towards smart devices since those devices are now basically everywhere, powerful enough to run a bot and offer additional gains for a bot-master such as financial gains as discussed earlier. With PC-based botnets, cybercriminals often use zombies within botnets to launch DDoS attacks. Even though there have been no major mobile DDoS incidents, with current trends we can expect to see this in the near future.

Botnets are maintained by malicious actors commonly referred to as "bot-masters" that can access and manage the botnet remotely or via bot proxy servers as illustrated in **Error! Reference source not found.**. The bots are then programmed and instructed by the bot-master to perform a variety of

cyber-attacks, including attacks involving the further distribution and installation of malware on other information systems.

In PC-based botnets, botnet master controllers typically use http requests with normal port 80 to transmit and receive their messages. In mobile-based botnets, the bot-master also uses similar http techniques to distribute their commands but also exploits SMS, Bluetooth, etc. The bot-master exploits operating system and configuration vulnerabilities to compromise smart devices and to install the bot software.

The first mobile malware, known as Cabir, was discovered in 2004 and was also known as the first mobile worm. The first mobile botnet was discovered around July 2009, when a security researcher found SymbOS.Yxes or SymbOS.Exy.C (aka Sexy Space) [12] targeting Symbian devices and using simple HTTP-based Command-and-Control (C&C).

Later the same year, a security researcher discovered Ikee.B [13], which targets jailbroken iPhones using a similar mechanism to SymbOS.Yxes. Geinimi, which is considered to be the first Android botnet, was discovered in China in December 2010. Geinimi also implements similar HTTP-based C&C with the added feature of encrypted communications. Geinimi steals the device's international mobile equipment identity (IMEI), international mobile subscriber identity (IMSI), GPS coordinate, SMS, contact list, etc. and forwards it to the bot-master.

Although advanced mobile botnets have not been observed in the main population of smartphones, we believe it is just a matter of time. As shown in [14], mobile botnets are obviously serious threats for both end users and cellular networks. Threats imposed by botnets will continue to increase. As more people use smart devices, it is essential to analyze and explore the mechanisms of mobile botnets and develop security solutions in regard to smart devices.

The use of C&C for a mobile botnet stipulates additional challenges that differentiate it from well-known PC-based botnets. Some of these main challenges include, among others: computational power, seamless connectivity, inter-connectivity with other secure platforms/networks, portability and amount of stored sensitive data, and computational power. PC-based botnets also use an IRC-channel as the main C&C communication channel.

The impact of SMS-based C&C, IP-based C&C, and Bluetooth-based C&C has been addressed in detail in [15], while P2P-based C&C mobile botnets are analyzed and discussed in [16].

As a result of the abilities of smart devices in terms of placing i.e. calls, use of SMS and MMS amongst others, the burdens for mobile botnets are very interesting and challenging as it opens the door for easy financial gain for a bot-master. Additionally, since mobile phones interact with operators and other networks, attacks against the critical infrastructure are also possible.

Hence, it is possible to launch sophisticated cyber-attacks on the mobile phone network that will be very hard to prevent.

Detecting and preventing malware is not a trivial task as malware developers adopt and invent new strategies to infiltrate mobile devices. Malware developers employ advanced techniques such as obfuscation and encryption to camouflage the signs of malware and thereby undermine anti-malware software.

Some of the main reasons why mobile malware are an attractive point for viruses and malware developers are:

1. The ubiquity of smart devices such as smartphones in general.
2. The increasing computational powers of smart devices. Whose they are becoming virtually as powerful as desktop systems.
3. The lack of awareness of the threats and the risk attached to smart devices from the end-user's perspective.
4. The growing uses of jailbreak/rooted devices both on iOS and Android devices.
5. Each smart device really is an expression of the owner. It provides a means to track the user's activity, hence serves as a single gateway to our digital identity and activities.
6. Most of the widely used smart devices operate on an open platform such as Android, which encourages developers and download of applications from both trusted applications markets and third party markets.

IV. Potential Security Solutions

Considering the above threats and challenges, a new security solution is essential for cyber security for smart devices in smart homes. More specifically, several key research tasks are required: 1) investigate new secure system architecture for smart devices in smart homes; 2) re-evaluate and enhance security system architecture for smart devices in smart homes.

Android OS has four layers: Linux kernel, libraries (+Android runtime), application solution and applications layers (see Figure 4). So, basically Android runtime is a kind of "glue" between the Linux kernel and the applications.

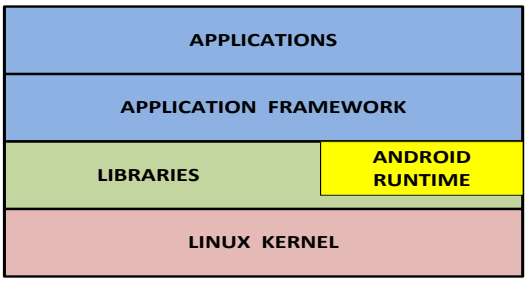

Figure 4. Android OS layers

The main security features common to Android involve process and file system isolation; application or code signing; ROM, firmware, and factory restore; and kill switches.

However, the main security issue with Android OS is it relies heavily to the end-user to decide whether an application is safe or not. Even though Google's just adding one piece of the security layer by scanning an applications in the Google Play, the end users still needs to analyze and make the final decision themselves whether to continue with the installation or not. Until now, the end-users cannot rely on the operating system to protect themselves from malware.

As part of Google's marketing strategy to gain market share as big as possible by offering applications as many as possible, the Android application publishing process makes it easy for developers to develop Android applications, but also provides too much space for malicious application creators.

Malicious applications have successfully infected Android market before, one example being a malware application called droid09 which allowed users to carry out banking transactions. The application needs the user to provide the bank's details and tricks the user by masquerading a legitimate login of a bank website (phishing).

Malware applications have become more sophisticated these days; they find new ways and techniques to enter the system by exploiting software vulnerabilities or by just tricking the users.

We propose a multi-layers integrated security solution for mobile smart devices as illustrated in Figure 5.

End-user: It is always essential for the end-user to be aware of the security measures of their mobile device. End-users should be aware of at least the following measures:

- Install anti-virus and anti-malware solutions to protect the device against malware and viruses. Also ensure to turn on the automatic update. It is been shown that installing anti-virus and anti-malware is very effective to protect mobile devices from malicious applications [5, 6, 17].
- Install a personal firewall to protect mobile device interfaces from direct attack and illegal access. The effectiveness of mobile firewalls to increase a mobile device's security is shown in [18].

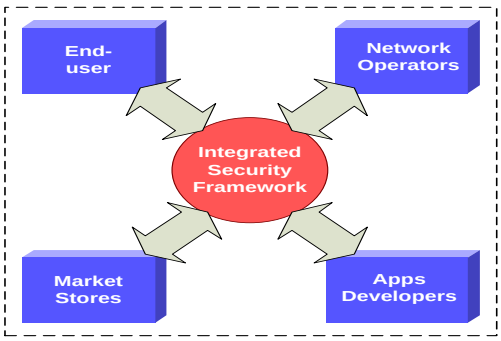

Figure 5. Integrated security solution for smart devices

- Install only applications from trusted sources that have legitimate contact information and a website. As the current Android Market (Google Play) does not adopt a certification process for applications, it is up to the end-user to make sure he/she only installs trusted applications from trusted developers.
- Install only applications from the official and original developer (for example, if you are installing Instagram applications, make sure you download it from Instagram Inc.).
- Check the permissions carefully when the application is prompting you during the installation phase. For example, when you install a wallpaper application, do you think it really needs full Internet access?
- Ensure your OS and software's always up-to-date with the latest versions and security patches need to be installed.
- Install remote locate, track, lock, wipe, backup and restore software to retrieve, protect or restore a lost or stolen mobile device and the personal data on the device.
- Only install applications that have a high number of downloads and positive reviews.
- Never view sensitive data over public wireless networks which have no passwords or encryption.
- Should be alert to anomaly behaviours and activities in their devices.
- Should be careful when clicking links on social network sites. Malicious links on social networks can be a very effective method to spread malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites.

Mobile Network Operators (MNOs): MNO also has responsibility to create a more secure environment for their customers. MNOs need to install anti-virus and anti-malware software to scan outgoing and incoming SMS and MMS to the mobile network, as many malwares use SMS/MMS to propagate and contact the bot-master. MNO should also build a global partnership with related agencies such as other MNOs to prevent mobile malware propagation by exchanging information, knowledge, database and expertise.

Apps Developers: Developers also need to take care of the security measures implemented in their application. They should ensure that private data is not being sent via an unencrypted channel; the data must be sent through HTTPS or TLS networks.

Developers should minimize the use of built-in permissions in their applications, for example do not ask for full Internet access permission, `INTERNET`, unless it is essential for your applications to work properly. Android has about 100 built-in permissions that control operations such as dialing the phone (`CALL_PHONE`), sending shot message (`SEND_SMS`), etc.

In Android, there are three main " security protection levels" for permission labels: a "normal" permission is granted to any application that requests it; a "dangerous" permission is only granted after user approval at install-time; and a "signature" permission is only granted to applications signed by the same developer key as the application defining the permission label.

This "signature" protection level is integral in ensuring that third-party applications do not gain access affecting the Android's trusted computing base (TCB)'s integrity.

Furthermore, applications developers need only collect data which is essential and required for the application otherwise it will be tampered by the attackers. This is also useful to minimize repackaging attacks. Repackaging attacks are a very common approach, in which a malware developer downloads a legitimate application, modifies it to include malicious code and then republishes it to an application market or download site.

It is shown that the repackaging technique is highly effective mainly because it is often difficult for end-users to tell the difference between a legitimate application and its malicious repackaged form. In fact, repackaging was the most prevalent

type of social engineering attack used by Android malware developers in the first two quarters of 2011 [17].

One of the characteristics of Android malware is typically it is specifically developed for a specific group of users. It is very unlikely for an Android user from Russia to be infected by Chinese malware for example. Android malware is typically created by cybercriminals with users in specific countries as their target, which is usually their own compatriot.

Market Store: The store needs to vet and rigorously screen new mobile applications before they can be put in the market. Google (Google Play) recently made a significant improvement in their security by screening new applications before they were put in the market. Applications store providers also should consider certification for each application before it can be published in the marketplace. The effectiveness of such certification process is shown in [19]. Applications should be rigorously reviewed to ensure that applications are safe from malicious codes, reliable, perform as expected, and are also free of explicit and offensive material.

Detecting and preventing malware in mobile device need comprehensive and multi-level approaches. Based on our initial finding it is essential that all four components in the security solution work complementary to tackle the alarming increase in mobile malware issues in mobile networks.

V. Conclusion

The paper discussed a development of security solution to handle the challenges of cyber security to smart devices in smart homes. The IoT technologies may be able to extend anywhere computing to almost anything, but there are fundamental security issues that need to be properly addressed.

In the near future, mobile smart device users can expect to see a striking increase in malware and notable advancements in malware-related attacks, particularly on the Android platform as the user base has grown exponentially. Today's users utilize their mobile smart devices for everything from accessing emails to sensitive transactions such as online banking and payments. As users become more dependent on their mobile devices as digital wallets, this creates a very lucrative target for cybercriminals. Mobile smart device users can expect to see a significant malware increase on finance related applications, such as mobile Internet banking. Detecting and preventing malware in mobile device need comprehensive and multi-level approaches.

This work is part of ongoing research to design and implement a security model for smart devices in the smart home environment. For the future work we plan to implement and assess the security solution proposed in the test-bed environment which includes a honeynet for mobile malware.

References

[1] Juniper, "Trusted Mobility Index," Juniper, http://www.juniper.net/us/en/local/pdf/additional-resources/7100155-en.pdf 27/02/2013 2012.

[2] "Cyber Security in the UK," Houses of Parliament September 2011 2011.

[3] J. Blumberg, "Cybersecurity, Health Care, and Mobile Devices," in *Dartmouth Now*, 2011.

[4] Juniper, "Trusted Mobility Index," 2012.

[5] Juniper, "Juniper Networks 2011 Mobile Threats Report," Juniper Networks Mobile Threat Center (MTC), 2012.

[6] TrendMicro, "Security in the Age of Mobility," Trend Micro 2012.

[7] W. Dong, L. Yan, M. Jafari, P. M. Skare, and K. Rohde, "Protecting Smart Grid Automation Systems Against Cyberattacks," *Smart Grid, IEEE Transactions on*, vol. 2, pp. 782-795, 2011.

[8] McAfee, "Variant of Mac Flashback Malware Making the Rounds," 2012.

[9] L. Auriemma, "Samsung devices with support for remote controllers," *http://aluigi.org/adv/samsux_1-adv.txt*, 26/04/2012.

[10] G. M. Nunes, "Sony Bravia Remote Denial of Service " *http://archives.neohapsis.com/archives/bugtraq/2012-04/0043.html* , Apr 05 2012.

[11] TrendMicro, "Security in the Age of Mobility - Quarterly Security Roundup," *http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_security_in_the_age_of_mobility.pdf*, 2012.

[12] A. Apvrille, "Symbian worm Yxes: Towards mobile botnets?," presented at 19th EICAR Annual Conference, Paris, France, 2010.

[13] P. A. Porras, H. Saidi, and V. Yegneswaran, "An Analysis of the iKee.B iPhone Botnet," presented at 2nd International ICST Conference on Security and Privacy on Mobile Information and Communications Systems (Mobisec), 2010.

[14] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, T. L. Porta, and P. McDaniel, "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core," presented at ACM Conference on Computer and Communications Security (CCS), 2009.

[15] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, "Evaluating Bluetooth as a Medium for Botnet Command and Control," presented at International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), 2010.

[16] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. H. Kang, and D. Dagon, "Peer-to-peer botnets: Overview and case study," presented at Proceedings of the Workshop on Hot Topics in Understanding Botnets, 2007.

[17] Lookout, "Lookout Mobile Threat Report 2011," Lookout, 2011.

[18] H. C. Tan, J. Zhou, and Y. Qiu, "A mobile firewall framework-design and implementation," presented at IEEE WCNC, Hong Kong, 2007.

[19] W. Enck, M. Ongtang, and P. McDaniel, "On lightweight mobile phone application certification," presented at Proceedings of the 16th ACM conference on Computer and Communications Security, Chicago, Illinois, USA, 2009.