Security Steps for Smartphone Users

Heloise Pieterse
Defence, Peace, Safety and Security
Council for Scientific and Industrial Research
Pretoria, South Africa
Email: hpieterse@csir.co.za

Martin S Olivier
Department of Computer Science
University of Pretoria
Pretoria, South Africa
Email: molivier@cs.up.ac.za

***Abstract*—Smartphones are an important asset for people living in the 21st century. With functionality similar to computers, smartphones have become all-in-one portable devices providing interconnectivity and device-to-device communication. Such continuous improvement in capabilities will cause the popularity of smartphones to constantly rise. Besides the popularity of smartphones there has also been a sharp increase in mobile malware. Most of the mobile malware recently discovered target Google's Android operating system. The ease of modifying and the simplicity of the design of the operating system are the aspects that are drawing malware developers towards Android smartphones. This study focus on the current state of mobile malware, the adequacy of mobile security applications and possible security steps smartphone users can take to prevent mobile malware attacks. To evaluate the adequacy of current mobile security applications a malicious Android application is developed and deployed on an Android smartphone. In addition, this new Android application is also evaluated against mobile security applications. From the results additional security steps are identified that users of smartphones can follow to prevent or detect possible mobile malware infections. The ultimate goal of this research is to eventually automate the identified steps in the form of an application rather than depending on the user to execute the steps.**

***Index Terms*—Smartphones, Malware, Security, Android.**

I. Introduction

Smartphones are an integral part of everyday living in the 21st century. With advance capabilities, high definition displays and millions of applications simply a click of a button away give smartphones the opportunity to become a prominent companion. Along with the popularity comes the increasing trend to attack smartphones by infecting applications with malicious content. During 2012 the motivation to attack smartphones continued to grow alongside the reliance users place on these devices to perform telephonic services, financial transactions and entertainment. These are just a few motivations behind the development of mobile malware with the preferred incentives being: novelty and amusement, selling user information, stealing credentials, performing premium rate calls or SMS spam [1].

Mobile malware comes in many forms but the vast majority can be classified into the following category: premium service abuser in the form of a SMS Trojan [2]. Mobile malware falling into this category will continuously send out SMS messages to premium rate numbers. These malicious activities are easily hidden within a legitimate application and smartphone users that download such applications are completely unaware of the hidden functionalities.

Mobile malware is on the rise and the compiled mobile malware statistics of 2012 supports this. According to Trend Micro Incorporated, 350 000 new Android malware variants were identified by the end of 2012 [2] and since 99% of all the mobile malware detected by Kaspersky labs during 2012 targets the Android operating system (OS) [3], this reveals a problematic situation. Unlike users of personal computers, smartphone users are not always aware of the potential threat they face when using these devices and therefore are not as cautious as when using a personal computer. Besides the lack of awareness surrounding mobile malware, there are also very few articles in literature focusing on potential countermeasures that smartphone users can follow to prevent and/or detect malware infections.

The purpose of this study is to evaluate available mobile security applications and determine to what extent they can protect smartphones against malicious applications. From this evaluation additional security steps are identified that smartphone users can employ as countermeasures against potential mobile malware threats.

This paper will start by evaluating the current state of mobile malware, looking at the growth of malware during 2012 and the targeted mobile operating system (Section 2). Furthermore, the adequacy of current mobile security applications will be explored by testing these applications against a simplistic but still malicious malware sample (Section 3). From the experiment a series of security steps is deduced that smartphone users can follow to possibly prevent mobile malware infections (Section 4). The final section concludes the paper and identifies future possibilities that can build on this research (Section 5).

II. Current State of Mobile Malware

The mobile threat landscape continues to grow and the popularity of smartphones are currently one of the main contributors. It is important to note that mobile malware have changed significantly since the arrival of the first mobile worm, Cabir, in 2004 [4]. With each passing year the level of sophistication of mobile malware improves, providing malware with the ability to accomplish more complex tasks. As of 2013, smartphones are facing the same kind of threats previously

seen on personal computers, but mobile malware achieved this level of sophistication much faster [2].

Malware developers are often drawn to smartphones due to the vast collection of information stored on these devices. Typical information stored by smartphone users include: contacts, SMS messages, personal photographs, emails, music, passwords and in some instances confidential data [5]. To obtain the above mentioned information malware developers will rather modify an existing piece of malicious code to perform the required actions than to develop a new malware design from scratch [5]. This saves both time and money, and have led to the exponential growth of mobile malware.

During 2012 many mobile malware samples terrorized smartphone users. There were however 5 specific mobile malware samples that have been identified as the most dangerous, sophisticated and prolific pieces of mobile malware of 2012. The first is FakeInst, a SMS Trojan that disguised itself as popular applications while in the background it sends out SMS messages to premium-rate numbers. SMSZombie was located in third-party markets in China and exploited China Mobile's online payment system. Once installed this malware obtained administrative privileges which makes it difficult to remove after installation. NotCompatible, discovered by Lookout Mobile Security, is the first mobile malware to use websites as a distribution method, infecting smartphones when the device visits a specific website. Android.Bmaster, a mobile botnet, was bundled with legitimate applications and generated a daily revenue that ranged between 10 000 and 30 000 US dollars. Lastly, LuckyCat targeted the aerospace and energy industries in Japan, causing a backdoor to be opened on the infected device. All of the above mentioned mobile malware samples are examples of Android malware [6].

The explosive growth of mobile malware mirrors the growth of the Android Operating System (OS) over the last few years [2]. As of the fourth quarter of 2012 Android held 69.7% of the smartphone market share, well ahead of iOS (at 20.9%) and Research in Motion (at 3.5%) [7]. The Android OS, developed by Google, is a mobile OS that places strong emphasis on the openness of the OS design. This however gave malware developers the opportunity to explore the inner workings of the OS, allowing for the creation of more advanced mobile malware.

Figure 1 shows that Android malware have risen exponentially from 1 000 samples at the start of 2012 to 350 000 samples by year end [2]. Most of the Android malware samples appear in one of the following forms: Adware, Click fraudster, Data Stealer, Malicious downloader, Premium service abuser or Rooter [2]. More than 70% of all the Android malware samples belong either to premium service abuser or adware, as can be seen in Figure 2 [2]. Google is however taking steps to boost the security surrounding the Android OS. Their efforts include the following: adding mitigation features and an optional application verification feature [8].

Even though Google are making attempts to improve the security surrounding the Android OS, mobile malware will continue to grow as smartphones continue to become popular and less expensive. It is therefore necessary for smartphone users to take precautionary steps to protect their devices against mobile malware infections.

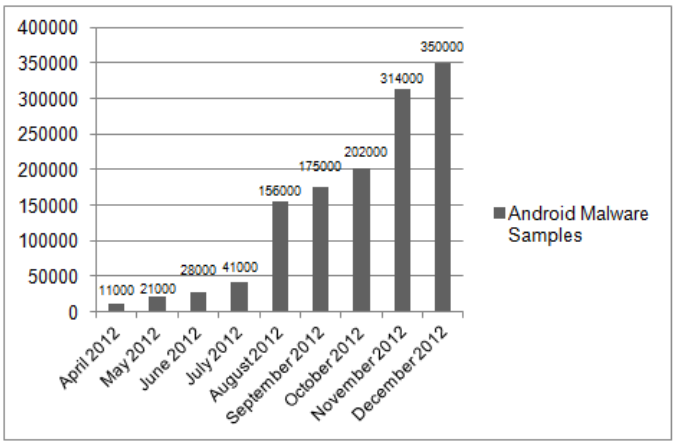

Fig. 1. Android Malware Samples for 2012 [2]

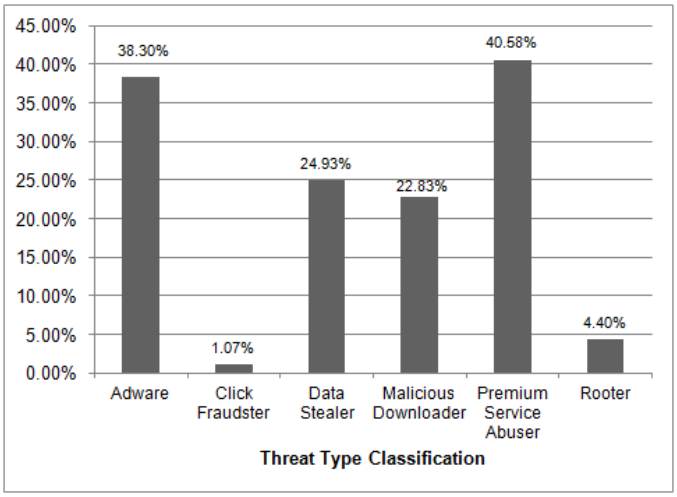

Fig. 2. Classification of the Android Malware Samples [2]

III. Detection of New Malware by Mobile Security Applications

The previous section revealed that mobile malware is indeed a real threat and that the Android operating system is currently the most popular platform for mobile malware. Due to the popularity of the Android OS as an attacking platform, it has been selected as the testing platform.

On the Google Play Store there are more than 1000 antivirus applications available for download but unlike personal computers, users of smartphones have not yet adopted the culture of using security applications. To show that this is indeed the case, a quick comparison of the installation estimates between security applications and general applications is performed. All of the applications were randomly selected.

The following security applications were selected:

- AVG Antivirus
- Avast Mobile Security

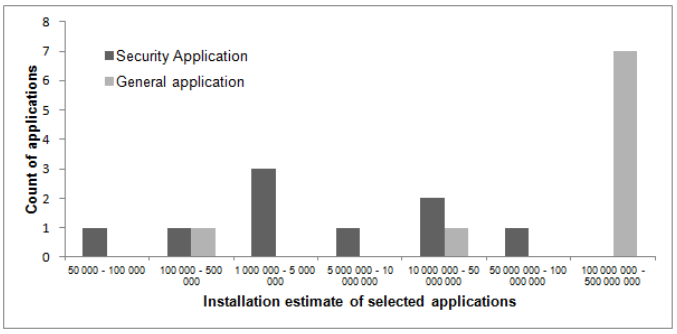

Fig. 3. Comparison between installation estimates of security and general applications

- Lookout Security & Antivirus
- Android Antivirus
- Norton Security & Antivirus
- TrustGo Antivirus & Mobile Security
- Sophos Security & Antivirus
- Kaspersky Mobile Security Lite
- Comodo Antivirus

The following general applications were selected:

- Whatsapp
- Facebook
- Skype
- Twitter
- Adobe Reader
- Chrome
- Gmail
- Mxit
- Angry Birds

Figure 3 shows the comparison between the installation of security applications and general applications. Concluding from the comparison reveals that the installation estimate of general applications often falls between 100 000 000 and 500 000 000 installations while with security applications the installation estimate is about 5 000 000.

The lack of using security applications is twofold. Firstly, the lack of awareness surrounding mobile malware has caused smartphones users to not invest in security applications because they believe it is unnecessary. Secondly, mobile security applications have not yet reached the same potential as that of security applications for personal computers and therefore are not often used by smartphone users.

This section will now focus on evaluating the adequacy of current mobile security applications by testing these applications against a new Android malware, called the SMS Inflictor. The SMS Inflictor is a SMS Trojan, created by the authors and designed specifically for the Android platform. The SMS Inflictor is embedded within a classic Tic Tac Toe game to allow for easy propagation within the Google Play Store. The technical details of the SMS Inflictor are described below:

- Testing platform: Galaxy S2, Android version 2.3.4
- Malware classification: SMS Trojan
- Android version affected: Version 2.3
- Capability: Intercept all incoming SMS messages, transport the messages to a central server and send SMS messages to specified premium-rate numbers.
- Permissions:
  - Send SMS messages
  - Receive SMS messages
  - Write new SMS messages
  - Allow Internet connections
- Revenue generation: The SMS Trojan sends SMS messages to specified premium-rate numbers.

Firstly, before the installation of the Tic Tac Toe game, all of the above mentioned security applications perform a scan of the Android device to ensure there is no malicious activity taking place. To verify that the original Tic Tac Toe game does not contain any malicious content, the game without the embedded malware is installed on the Android device and all of the installed security applications perform an internal scan. The last experiment is to test the security applications against the SMS Inflictor malware. The results of the experiments are shown in Table 1.

Out of the 9 security applications installed on the Android device, only one, the Avast Mobile Security application, detected the newly installed malware. Avast identified the new application as the malware Android.Jifake, a Trojan horse for Android devices. The Android.Jifake malware sends out SMS messages to premium rate numbers and was first detected by Symantec on July 30, 2012 [9]. Avast was thus able to identify a specific part of the malware (the sending of SMS messages to premium rate numbers) but not the interception of incoming SMS messages. Although Avast identified the SMS Inflictor malware incorrectly, it was still able to identify this new application as malware while all the other security applications failed to do so.

These experiments revealed that most of the available mobile security applications are unable to detect new malware. This is because most of the available mobile security applications rely heavily on signature-based detection mechanisms. Thus by changing or adding a single component in previously detected mobile malware will possibly allow this new malware variant to bypass security applications. Since mobile security applications are not always able to detect new malware, the next section introduces security steps that users of smartphones can follow to possibly detect and remove hidden malware.

IV. Security Steps for Users of Smartphones

Mobile malware is a real threat and can severely impact the end users, either financially or simply emotionally. Protection measures to defend against mobile malware have not yet evolved to the point where it is as efficient as those measures used to defend against malware targeting personal computers. The most basic step that smartphone users can take to protect themselves against mobile malware attacks is to install anti-virus and security applications. Such applications can only detect previously identified mobile malware and will not always detect newly designed malware as shown by the

TABLE I
DETECTION OF MALWARE BY MOBILE SECURITY APPLICATIONS

	Before Game Installation	After Game Installation	After Malware Infection
AVG Antivirus	No Threats Found	No Threats Found	No Threats Found
Avast Mobile Security	No Threats Found	No Threats Found	Threat Found
Lookout Security & Antivirus	No Threats Found	No Threats Found	No Threats Found
Android Antivirus	No Threats Found	No Threats Found	No Threats Found
Norton Security & Antivirus	No Threats Found	No Threats Found	No Threats Found
TrustGo Antivirus & Mobile Security	No Threats Found	No Threats Found	No Threats Found
Sophos Security & Antivirus	No Threats Found	No Threats Found	No Threats Found
Kaspersky Mobile Security Lite	No Threats Found	No Threats Found	No Threats Found
Comodo Antivirus	No Threats Found	No Threats Found	No Threats Found

experiments in the previous section. Users of mobile devices must therefore take additional steps in order to protect their smartphones against malware infections.

A. Step 1: Caution

The first step involves caution, and therefore users of smartphones must take the necessary precautionary steps to avoid danger or common mistakes. Protection of smartphones starts with the installation of anti-virus and security applications. Even if these applications are not capable of detecting new threats, it still provides the user with valuable services to secure the device if it ever gets lost or stolen. Such services include locating the device by using the GPS functionality, remotely locking the device via the Internet and remotely wiping the device, which will delete most of the personal information stored on the mobile device such as contacts, text messages and photos. So besides their shortcomings, anti-virus and security applications still offer many beneficial services for smartphone users.

Many users today are rooting their Android devices. This allows a user the ability to obtain superuser privileges, which then allow the user to alter certain system settings that would otherwise not have been possible. To root a smartphone is a complex process and if not performed correctly users can end up bricking their devices which renders it into an unusable state. Furthermore, some companies today state that if a user should root a smartphone, the warranty associated with that specific device becomes void. The user will thus not be able to find any assistance from the company if anything should go wrong with the smartphone. Lastly and most importantly, by giving the smartphone superuser privileges also allow the malware the ability to use these privileges and can therefore cause much more harm to the device. So to protect the smartphone, it is recommended not to root the device.

Smartphones have become popular due to their ability to host various applications. Such applications can either be downloaded from trustworthy market stores, such as Google's Play Store, or from third party market stores. It is the responsibility of the user to decide where the applications are downloaded from and it is therefore important to know that malicious applications are mostly found on third party market stores. In order to run a lower risk of getting infected by malware, users should only download applications from trusted market stores.

Malware are known to use networking technologies, such as Bluetooth, to propagate and perform command dissemination [10]. It will not be long before mobile malware also start exploiting NFC and Wi-Fi technologies in order to improve their growing potential. Users who continuously enable Bluetooth, Wi-Fi and/or NFC are at a higher risk of getting infected by mobile malware. To protect their smartphones, users should keep Bluetooth, Wi-Fi and NFC turned off whenever possible. If the user requires any of these technologies, he or she must carefully select the network to which the device will connect to. With Wi-Fi the user must only connect to secure Wi-Fi networks and regularly monitor the connection. Whenever possible, such as during night time, the user should turn off the data network. This will prevent any Internet activities from taking place and should malware infect the smartphone, this will limit the malware's ability to communicate beyond the smartphone. Another step users can take to protect their smartphones is to manage the location settings. If the user wants to keep their location a secret and prevent malware from exploiting the location data, users must turn off all forms of location assessment whenever possible.

Users must always use a password or pattern to lock their smartphone and so prevent an unauthorized person from accessing the device. Avoid weak passwords or patterns that can easily be guessed or enumerated. Furthermore, users must avoid storing sensitive information on their smartphones and if not possible, sensitive information must be encrypted by using a secure encryption algorithm. Should an unauthorized person gain access to the smartphone, such a person will not be able to view the sensitive information.

The last cautionary step that users of smartphones can take is to restrict usage of their devices. Users must never leave their smartphones unattended or lend it out to strangers. By ignoring the cautionary steps set out in this section will give malware developers an opportunity to infect the smartphone.

B. Step 2: Investigate

The second step involves the investigation of a smartphone. It is the responsibility of the user to regularly check the account associated with the particular smartphone. By investi-

gating the accounts regularly, the user will be able to determine if there is any malicious activity taking place on the device. The first indication of potential malicious activities can be a sharp increase in the bill. If this is indeed the case, the user must search for specific activities such as the sending of SMS messages or phone calls to premium rate numbers. By detecting malicious activities frequently can possibly save the user money and frustration.

As stated before, applications are an integral aspect of smartphones. The popularity of applications has caused them to be used for malicious purposes such as aiding the propagation of a mobile botnet. It is therefore necessary for users to properly check the permissions of applications. The user must do this before and after the installation of an application. When installing an application, the user must thoroughly read through all the permissions before continuing with the installation. For each permission, the user must ask whether this particular permission is really necessary and if it applies to the functionality provided by the application. If the user finds any suspicious permissions, the installation of the application must immediately be halted. By carefully evaluating the permissions of applications can equip the user with the necessary knowledge to prevent malware infections on their smartphones.

Users must systematically check the applications and files stored on their smartphones. Most mobile malware are known to install additional applications and files as required by the malware in order to operate successfully. The user must therefore be aware of all the applications and files stored on the device in order to be able to detect any malicious content. In addition, users must also check the settings of their smartphones and any settings that malware can potentially exploit must be turned off.

By investigating their smartphones on frequent occasions can equip the user with the necessary awareness to detect potential mobile malware.

C. Step 3: Monitor

For smartphone users, simply being cautious and checking the applications is not enough. Users must also continuously monitor their devices for any potential malicious activities. To monitor a smartphone, users must start with the evaluation of data consumption and battery life. Mobile malware, such as mobile botnets, are known to consume data since the botnet must connect to a command and control server from time to time. Even though such consumption might be insignificant on a daily basis, the increase of data usage after a monthly period can be more severe. It is therefore the responsibility of the user to regularly monitor the consumption of data and to be aware of the average consumption of data on a monthly or weekly basis. Should there be a sudden increase in data consumption over a specific period, the user must repeat the first two steps in order to check for potential malicious content.

The consumption of battery power is also a significant tool for the detection of mobile malware. Mobile malware often continuously execute activities in the background without alerting the smartphone user. Such activities, depending on their frequency, will consume battery power. Most smartphones on average have a battery life of approximately 9 hours, but this will differ from person to person as each person uses their smartphone differently. It therefore once again the responsibility of the smartphone user to frequently monitor the consumption of battery power. Should the user notice a sudden decrease in battery power, it can be that one of the latest installed applications or files contain malicious content. Such detection of mobile malware will only be possible if the user regularly monitors the battery consumption of the smartphone.

It is important to frequently monitor applications and the actions they perform. The user must do this after the installation of an application as well as after each update. Although most malicious activities occur in the background, it can have a negative influence on the infected application. It is the responsibility of the user to look out for abnormalities in applications. Such abnormalities can include: applications that continuously crash, slow performing applications, functionality of the applications hindered and the crashing of the smartphone. All of the above mentioned abnormalities are possible characteristics of a malicious application.

The user must also monitor Wi-Fi and Bluetooth connections and regularly check the connections made to Wi-Fi networks and Bluetooth devices. Should the user locate any suspicious connections to unknown networks or devices, it can be an indication of potential malicious content installed on the device that is exploiting these technologies. To discover the malicious content, the user must revisit each application and carefully check the permissions associated with an application.

Users must frequently monitor the data consumption, battery life and applications installed on the smartphone. Such knowledge can aid the user of a smartphone with malware detections and infections.

D. Step 4: Update

Most mobile OSs have been plagued with exploits. The Android operating system is often targeted by premium service abusers or adware [2]. Malware developers are the front runners of discovering vulnerabilities and successfully exploiting them in the execution of the malware. It is only when researchers discover the malware that the vulnerability becomes publicly known. Developers of the mobile OS, with which the vulnerability is associated with, must quickly fix the vulnerability and release a patch to the end users.

In order to protect against malware infections, the user must keep the mobile OS of their devices updated. This will require the downloading and installation of patches and new versions on a regular basis. Besides the mobile OS, users must also keep the installed anti-virus and security applications updated. Anti-virus and security applications can only protect smartphones from known malware infections. If such applications are not updated frequently, previously detected malware can possibly slip onto the smartphone.

To ease the process of regularly updating the software and applications of the device, users can enable auto update. This will automatically update the mobile OS and other applications should new patches or versions become available.

If users are able to frequently update the software of their smartphone, malicious content will not easily find their way onto the device.

E. Step 5: Remove

The last step involves the removal of applications and files that are no longer being used or are potentially malicious. Malware can only cause damage as long as it remains undiscovered. Once located, the user must immediately remove the infected application or file from the device. If a user discovers any suspicious applications or files on the device that were either not installed by the user or not there previously, such an application or file must also immediately be removed.

Any applications or files that were previously installed or added by the user but are no longer being used must also be removed from the device. It is possible for malware developers to hide malicious content in other applications or files. To minimize the impact of mobile malware, users must regularly check their smartphones and remove applications and files that are no longer in use.

This removal of unwanted software from a smartphone is the final step that users can take to protect their smartphones against potential mobile malware infections.

V. Conclusion

Mobile malware goes hand in hand with technology and will continue to grow as smartphones popularity continuously improves. As long as users make use of smartphones, they will continue to be targets for mobile malware. Although there are protective mechanisms, such as security applications, available to smartphone users, these mechanisms are infrequently used and often provide inadequate protection against new mobile malware. The inadequacy of security applications were shown by testing these applications against a simple malicious application. This reveals the responsibility the user has in terms of being constantly aware of the activities taking place on their smartphone. This poor performance of security applications has led to the identification of security steps smartphone users can follow for additional protection. These five steps, if performed regularly, will allow smartphone users to be in complete control of their devices and provide them with the necessary knowledge to identify malicious activities. These steps however doesn't guarentee complete protection against malware infections but can create awareness about how to protect against future malware threats. Future research will include the refining of the five security steps and also exploring the possibility of adding additional steps. The future goal of this research is to automate these steps in the form of an application instead of relying on the user to execute these steps regularly. In the end, all the power lies with the user and the decisions they make will eventually impact their smartphones.

References

[1] A. P. Felt *et al.*, "A survey of mobile malware in the wild," in *SPSM'11 Proceedings of the 1st ACM workshop on Security and privacy in Smartphones and Mobile Devices*, 2011, pp. 3–14.

[2] "Evolved threats in a post-pc world," Trend Micro Incorporated, Tech. Rep., 2013.

[3] D. Maslennikov and Y. Namestnikov. (2013) Kaspersky security buletin 2012. the overall statistics for 2012. [Online]. Available: http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012

[4] S. Furnell, "Handheld hazards: The rise of malware on mobile devices," *Computer Fraud and Security*, vol. Volume 2005, no. 5, pp. 4–8, 2005.

[5] "Trends for 2013," ESET Latin America's Lab, Tech. Rep., 2013.

[6] B. Prince. (2012) Top 5 deadliest mobile malware threats of 2012. [Online]. Available: http://www.darkreading.com/mobile-security/167901113/security/news/240006056/top-5-deadliest-mobile-malware-threats-of-2012.html

[7] Gartner. (2013) Gartner says worldwide mobile phone sales declined 1.7 percent in 2012. [Online]. Available: http://www.gartner.com/newsroom/id/2335616

[8] "Threat report h2 2012," F-Secure, Tech. Rep., 2013.

[9] Symantec. (2012) Android.jifake. [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2012-073021-4247-99

[10] G. Yan, "Bluetooth worms: models, dynamics, and defense implications," in *Computer security applications conference, 2006, ACSAC'06*, 2006, pp. 245–256.