ACCEPTED FROM OPEN CALL

MOBILE APPLICATION SECURITY: MALWARE THREATS AND DEFENSES

DAOJING HE, SAMMY CHAN, AND MOHSEN GUIZANI

ABSTRACT

Due to the quantum leap in functionality, the rate of upgrading traditional mobile phones to smartphones is tremendous. One of the most attractive features of smartphones is the availability of a large number of apps for users to download and install. However, it also means hackers can easily distribute malware to smartphones, launching various attacks. This issue should be addressed by both preventive approaches and effective detection techniques. This article first discusses why smartphones are vulnerable to security attacks. Then it presents malicious behavior and threats of malware. Next, it reviews the existing malware prevention and detection techniques. Besides more research in these directions, it points out efforts from app developers, app store administrators, and users, who are also required to defend against such malware.

INTRODUCTION

Compared to traditional mobile phones, which mainly provide mobile telephony functions, smartphones are general-purpose handheld computing and communications devices that support multimedia communications and applications for entertainment and work. Due to this quantum jump in functionality, the rate of upgrading traditional mobile phones to smartphones is tremendous. According to the IDC (International Data Corporation) Worldwide Quarterly Mobile Phone Tracker, worldwide shipment of smartphones in 2013 surpassed one billion units, which is a record yearly shipment figure [1].

The rapid growth of the global smartphone market in the coming years will also be accelerated by the increasing business use of smartphones. Besides the traditional corporate-liable model, the new employee-liable BYOD (bring your own device) model is gaining acceptance in enterprises throughout the world. According to its studies, IDC believes that in 2013, 132.3 million and 61.4 million smartphones were used as employee-liable and corporate-liable devices, respectively. This is a 50.3 percent and 18.5 percent growth rate compared to the 2012 shipments for the two models. Moreover, shipment of employee-liable and corporate-liable smartphones in 2017 are expected to reach 328.4 and 88 million units, respectively [2].

One of the distinct features of smartphones is that they allow users to install and run third-party application programs, which are usually referred to as *apps*. They significantly broaden the functionality boundary of smartphones and hence enrich the user experience. These applications are officially distributed via online stores referred to as app markets — Apple App Store for the iOS platform and Google Play Store for the Android platform. These markets provide a convenient venue for app developers to distribute their apps and for users to explore and download new apps. This has driven the tremendous development rate of apps in recent years. For instance, by September 2012 the Google Play Store and Apple App Store were home to more than 650,000 and 700,000 apps, respectively.

Like other cyber systems, smartphones are also vulnerable to malware, which are malicious programs designed to run on infected systems without their owners' awareness. While users are keen on downloading apps from app markets, this provides hackers a convenient way to infect smartphones with malware. For example, they would repackage popular games with malware and distribute them in the app markets. Very often users are attracted to download the infected apps. A recent survey reported that 267,259 malware-infected apps have been found, among which 254,158 reside on the Android platform [3]. It also suggested that the number of malware in apps has increased by 614 percent since 2012. There are also a variety of other ways for malware to infect targets [4]. Some malware are disguised as the macros of files. Some are installed through certain known vulnerabilities existing in a network device or mobile platform. Some are installed in victims' smartphones when they click a multimedia messaging service (MMS) message or open an email attachment. In any case, malware can cause serious issues relating to information security and data privacy, with severe repercussions for users and even organizations.

In the remainder of this article we first discuss why smartphones are vulnerable to security attacks and then present malicious behavior and threats of malware. Then we review the existing malware prevention and detection techniques. We argue that efforts are required from app

Daojing He is with Shanghai Key Lab for Trustworthy Computing, East China Normal University and State Key Laboratory of Power Transmission Equipment & System Security and New Technology, Chongqing University.

Sammy Chan is with City University of Hong Kong.

Mohsen Guizani is with Qatar University.

1536-1284/15/$25.00 © 2015 IEEE

store administrators, app developers, researchers, and users to defend against such malware. Finally, we conclude with several outstanding security issues that need further research work.

Why Smartphones are Vulnerable?

There are a number of factors that make smartphones vulnerable to security attacks, and these are discussed below.

First, personal data are often stored in smartphones. In particular, since more and more users carry out financial transactions such as online banking and shopping from their smartphones, some data can be very sensitive. Hackers can have substantial financial gain from such sensitive data and thus find smartphones to be lucrative targets.

Second, more and more smartphones are based on the Android platform. With Android's policy of open-source kernel, malware writers can gain a deeper understanding of the mobile platform. According to Google's marketing strategy, development of third-party apps is encouraged and publishing of apps is made easy to gain market share. As a result, there are many opportunities for hackers to create and publish malware. At the same time, as users are in the habit of downloading and installing apps for their smartphones, the chances of installing malwares increases as well.

Third, most users have the impression that their smartphones are just mobile phones that are installed with a wide variety of software for communications and entertainment. They are not sensitive to the fact that their smartphones are essentially handheld computers that are vulnerable to cyber attacks. As a result, not enough attention is paid to security measures.

In addition, with the advent of the hardware and operating systems of smartphones, malware writers are less constrained to implement their malicious actions. Moreover, sometimes it is convenient for adversaries to develop mobile malware; they simply migrate PC malware to smartphone platforms.

Malicious Behavior and Threats of Malware

Mobile malwares are characterized by their propagation behavior, remote control behavior, and malicious attack behavior [5]. The propagation behavior refers to how malware may be transmitted to the victims. The remote control behavior indicates how the mobile malware makes use of a remote server to further exploit the infected device. The attack behavior refers to how the malware, after infecting a victim's devices, attacks the devices via different communication channels (e.g. Bluetooth). A more detailed description of the threats posed by malware is provided as follows.

Once malware is installed on smartphones, it would try to gain access to the data stored in the devices, interfere with the normal functions of the devices, or open more security vulnerabilities such as enabling unauthorized remote access. In general, through malware, various types of attacks can be launched. Typically, threats include phishing, spyware, surveillance attacks, diallerware attacks, financial malware attacks, worm-based attacks, and botnets, as listed in Table 1.

Attack	Description
Phishing	Users' credentials such as account details and credit card numbers are collected by means of apps, emails, or SMS, which seem to be genuine.
Spyware	Users' activities on the smartphones are being monitored, which means personal information is extracted or inferred. Compared to surveillance attacks, spyware does not have specific targeted victims.
Surveillance attacks	A specific user is under surveillance by means of his/her infected smartphone, making use of the built-in sensors.
Diallerware attacks	Users' money is stolen using the malware that makes hidden calls to premium numbers or SMS services.
Financial malware attacks	Such attacks aim to steal users' credentials from the smartphones or perform man-in-the-middle attacks on financial applications.
Worm-based attacks	A worm is a malware that duplicates itself, typically propagating from one device to another, using different means through an existing network without users' intervention.
Botnets	A botnet is a set of zombie devices that are infected by malware so that a hacker can remotely control them.

Table 1. Typical attacks launched by malware.

Phishing Attacks — A phishing attack is a well-known threat for PC users. Since this type of attack does not need to attack the users' systems in any way, it is actually platform-independent and readily applicable to smartphones. The malware only needs to contain URLs of faked web sites, which masquerad as trusted web sites, to steal personal information such as credit card details. It has been found that approximately 25 percent of malware contains suspicious URLs.

There are several reasons for hackers to choose smartphones to phish users. First, it is easy to disguise infected apps as legitimate apps and distribute them in app markets. Second, smartphones tend to have a small screen, so it is easier to disguise trust cues on which users rely to decide whether it is risky to submit credentials, for example, cues that indicate whether the site is enabled by Secure Sockets Layer. Third, there are various channels in smartphones that hackers can use for phishing, e.g instant messaging, short message service (SMS), and so on. Fourth, users are often not aware that phishing can be a risk on smartphones. Also, many users trust their smartphones more than their PCs.

Spyware Attacks — Malware that covertly collects users' various information stored in their infected smartphones are referred to as spyware. The

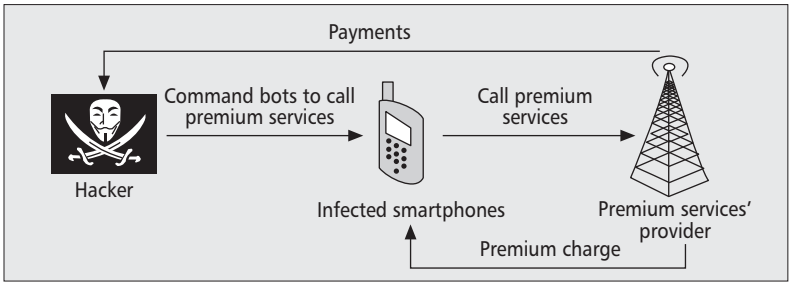

Figure 1. Diallerware attacks.

amount of personal data and sensitive information stored in and processed by smartphones makes them attractive targets for spyware. Moreover, covert channels are available in smartphones for returning collected information to hackers. Sometimes, even when an app seems to have a legitimate need to send data to the outside world, the permission settings of smartphones may not be granular enough to prevent abuse of such a permission. For example, a weather app can have the permission to send location data to some weather information servers, but if it is implanted with spyware, it can abuse the permission by sending the same location data to advertisement servers for spamming marketing information [6].

Depending on the type of information being collected, different levels of damage can be incurred. In the above example where users' location information is used to trigger spam messages, users are only annoyed. However, if more sensitive information is collected, more serious damage can be done. For example, a recent spyware in the Android platform, Zitmo, is more dangerous than other common spyware. It intercepts confirmation SMS sent by banks. Such a SMS message may contain credentials of the owner of the spied smartphone for Internet banking. Using such information, the hacker can carry out fraudulent transactions [7].

Surveillance Attacks — Smartphones are commonly equipped with sensors such as a Global Positioning System (GPS) sensor, accelerometer, microphone, and camera. Combined with the fact that they are closely associated with their owners, smartphones infected with suitable spyware can be used to keep targeted users under surveillance [6]. In particular, the GPS sensor is particularly useful as it can provide highly sensitive personal information. There are already examples of legitimate apps that are exploited by hackers to keep the targeted users under surveillance. Moreover, even apps that are not originally designed as spyware may be covertly configured to support tracking.

Diallerware Attacks — As shown in Fig. 1, hackers can incur financial charges to smartphone users by diallerwares, which send premium-rate SMS messages without users' awareness. The original purpose of premium-rate SMS messages and calls were to provide value-added services such as news and stock quotes, with the cost being charged in the users' phone bills. Premium-rate calls are abused for the hacker's profit under this attack. Hackers lure owners of infected smartphones into signing up premium-rate services controlled by themselves. For example, HippoSMS is an Android malware that sends SMS messages to a premium-rated number. It blocks SMS messages from service providers so that users are not aware of the unwanted additional charges [7].

Financial Malware Attacks — Financial malware aims to steal credentials from the smartphones or perform man-in-the-middle attacks on financial applications. Similar to PCs, smartphones are also vulnerable to financial malware. Financial malware may simply be a key-logger that collects credit card numbers. In a more sophisticated form, it may be an app impersonating a real banking app. If users download and run the app, the hacker can launch a man-in-the-middle attack for banking transactions.

Worm-Based Attacks — A worm can damage and compromise the security of smartphones. Moreover, it duplicates itself, typically propagating from one device to another, using different means through an existing network without the users' intervention. In fact, worms can be easily spread by just one click to infect smartphones in any part of the world with a large chance of success. Moreover, as network function virtualization will be introduced into next generation mobile networks to reduce capital and operating expenditures [8], worm-based attacks to the virtualization environment and hence to smartphones are expected to increase.

Botnets — A botnet is a set of zombie devices that are infected by malware so that hackers can remotely control them. When a number of smartphones are compromised and remotely controlled, a mobile botnet is formed. Botnets impose serious security threats to the Internet, and most of them are used in organized crime, launching attacks to gain money. Some examples include sending spam, Denial-of-Service attacks, or collecting information that can be used for illegal purposes. Once a smartphone is infected, it becomes a zombie for cyber attacks.

Challenges

Compared to PCs, smartphones have very different security principles. In particular, the security problems on smartphones originate from the integration of multiple technologies to access the Internet. The following three factors distinguish mobile security from traditional computer security:

- Mobility: devices are carried by their owners and have high mobility. Therefore, they are subject to the risk of being stolen or physically tampered with.
- Strong personalization: normally, the device owner is also its unique user.
- Strong connectivity: smartphones enable users to access various Internet services. As a result, devices can be infected by malware through different channels.

Also, the limited resources of smartphones are the most obvious difference from a PC. Limited CPU power, memory, and battery life

restrict the sophistication of possible security solutions. For example, complex intrusion detection algorithms are not suitable for smartphones as they require excessive CPU power.

Defense Methodology

To defend against malware, a two-level strategy can be deployed. The first level aims to prevent malware from getting into smartphones. The second level relies on tools to pro-actively detect the existence of malware. Once it is detected, it is removed and the smartphone systems are cleaned up. Below we first discuss this strategy for general scenarios. Then we will focus on some specific types of attacks.

General Scenarios

Preventive Measures — To prevent attacks from malware residing in smartphones, as shown in Fig. 2, it is essential to have co-operation among the stake holders [9].

Application Developers — Application developers should ensure that their apps abide by the policies governing secure coding and privacy and do not access unnecessary information. Then it would be difficult for malware that exploits the security weaknesses of another app to launch attacks. For example, developers can use a unique identifier instead of the IMEI number. Also, sensitive information stored locally or sent to remote servers should be encrypted. If third-party libraries are used in the development of apps, they should be vetted by appropriate mechanisms.

Moreover, while Android apps have about 100 built-in permissions that control operations such as dialing the phone and sending short messages, the use of such permissions should be minimized. For example, an app should not ask for full Internet access permission unless it is essential for it to work properly. Since smartphone users generally just use the default settings, careful use of built-in permissions by application developers is particularly important. Furthermore, application developers may provide add-on security services to complement the weaknesses of the devices or resist the attacks from malware.

App Market Administrators — Administrators of app markets should strictly vet every uploaded app, and remove suspicious apps. Recently, server-side vetting processes have been developed to detect and then remove malicious apps from app markets with varying levels of success [10]. Moreover, it is helpful to developers if administrators have a well defined security policy. For example, apps have to conform to Apple's security rules before they can be distributed via the App Store. Apple approves apps by code signing with encryption keys. Downloading the apps from the App store is the only way for iPhones to install apps. This ensures that only those apps satisfying Apple's security policy can be distributed to iPhones. Google has introduced a new mobile malware detector *Bouncer* to scan apps before they are released in the Google Play Store. Bouncer checks if an app attempts to send SMS messages to malicious sites [11].

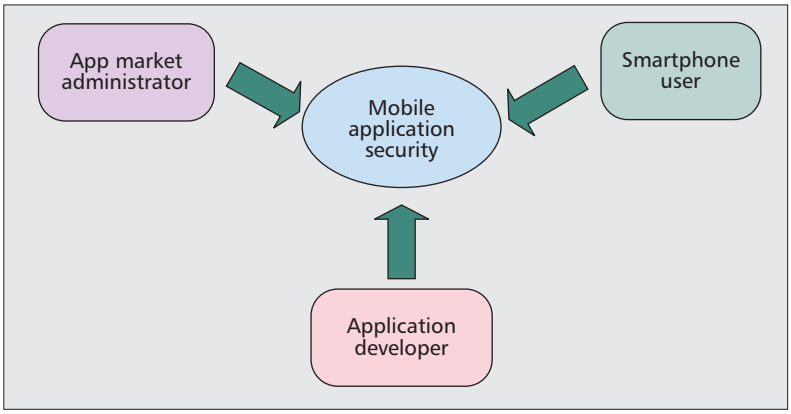

Figure 2. Co-operation among the stake holders.

Smartphone Users — Users should implement a good anti-malware framework (e.g. a personal firewall is a possible element) that can protect and alert them for any suspicious events. Besides, they should only download apps from trusted app markets. Before installing an app, its reviews should be consulted. When approving the permissions requested by apps, it should be done in a cautious manner.

If the networking functions such as WiFi or Bluetooth are not in use, they should be turned off to prevent the smartphone from contracting proximity malware, which is malware that can propagate by proximity contact such as direct peer-to-peer communication technologies.

Detection Techniques — Fundamentally, mobile malware detection techniques are either signature-based or anomaly-based. With signature-based techniques, the malicious behaviors of known malware are captured as their signatures. The malware is detected when one of its signatures is identified. With anomaly-based techniques, the normal system behavior is modeled first. Then the malware is detected whenever the system behavior deviates from the modeled normal behavior.

From the perspective of where malware detection is executed, malware detection techniques can be divided into two domains, client detection and network detection, as shown in Fig. 3. Generally, techniques for client detection can be either host-based or cloud-based. The techniques that run locally in smartphones are referred to as host-based techniques. On the other hand, the intense computation involved can be offloaded to a remote server in order to improve the efficiency; this type of detection techniques is regarded as cloud-based. Most mobile versions of antivirus software currently offered by security vendors basically implement similar functions as their desktop counterparts. Hence, only limited detection capability is provided while significant resources are required. Such an approach may not be effective. Most of the malware detection tools for mobile devices use signature-based detection techniques. The efficacy of these techniques depends on the availability of an up-to-date signature database. Often it requires the device to store a huge signature database for static scanning. One possible way to reduce the size of the database is to use

In a situation relating to financial transactions, users should confirm with their financial institution. Any email that asks a user to log in from the link provided in the email should be treated with suspicion. Also, users should look for secure symbols in browsers, for example, the lock in the address bar.

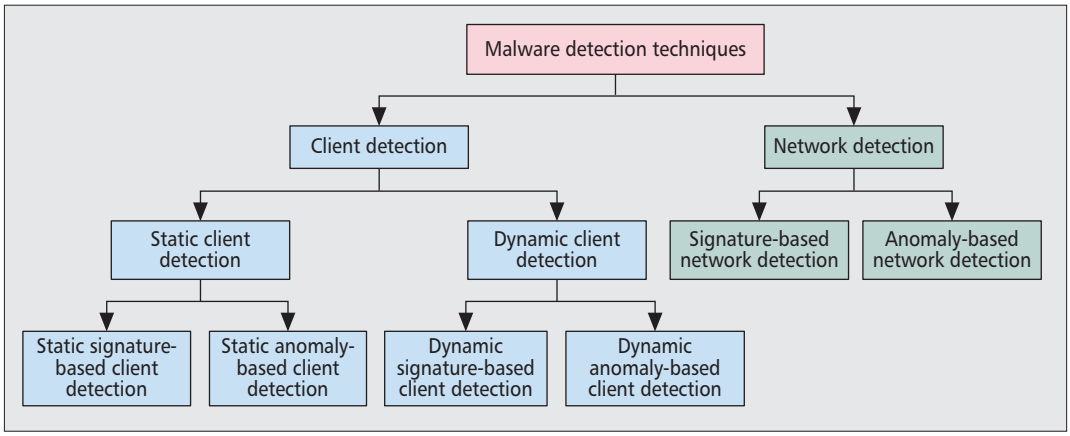

Figure 3. Classification of mobile malware detection techniques.

the same signature for all variants of the same malware. In any case, susceptibility to obfuscation is a major drawback of signature-based detection techniques. Malware creators may use polymorphism and metamorphism techniques to evade detection by static detection techniques.

To overcome this, the cloud-based approach should be used. By offloading intensive computations to the cloud, efficient detection for heterogeneous devices are enabled [9].

As shown in Fig. 4, a cloud-based malware detection server has multiple scan engines for signature or anomaly detection. For example, Zonouz *et al.* [12] developed Secloud, which is a cloud-based security solution for smartphones. It emulates a registered smartphone in the system by continuously feeding the device inputs and network connections to the cloud. In this manner, resource-intensive security analyses on the emulated device becomes feasible.

Alternatively, if a user is not aware of the need, or is not willing to install mobile malware detection software, protection can be sought from network detection schemes. These schemes aim to detect malware in the mobile Internet by capturing the network traffic and monitoring malicious events arising from smartphones. For example, Nadji *et al.* [13] designed and implemented a prototype called Airmid that can automatically detect and respond to malware infection in smartphones.

Detection can be achieved based on either static analysis or dynamic analysis. In static analysis, codes or apps are analysed without being executed. It consists of three steps: unpacking, disassembling, and analyzing. It is generally fast and simple. Dynamic analysis means that the behavior of apps is continuously monitored in an isolated environment. This technique collects and analyzes runtime information of an app, e.g. events and system calls. Static analysis techniques focus on what is being accessed, while dynamic analysis focuses on why certain suspicious operations are performed and how often they are performed [9].

Specific Attacks

Phishing — Users can play an active role to avoid being phished on their smartphones. They should be careful with emails containing hyperlinks. When they read an email, they should carefully check the sender and the details of the message. The content of the email should help them decide if it is legitimate. It helps to look for spelling mistakes and grammatical errors. Many phishing scams originate from senders whose first language is not English. In a situation relating to financial transactions, users should consult with their financial institution. Any email that asks a user to log in from the link provided in the email should be treated with suspicion. Also, users should look for secure symbols in browsers, for example, the lock in the address bar. In summary, users should be as vigilant as possible.

Furthermore, there are tools available to help users. For example, users can download an app to check every site they visit with real-time protection against phishing. Other tools to mitigate phishing attacks include filtering on the browser and toolbar, anti-virus, and anti-phishing. There are advantages and disadvantages of each of these techniques. For example, anti-phishing software requires the phishing signatures to be updated frequently. However, the advantages are that they are widely used and easily updated. Some common detection techniques are:

- Content based filtering, which has been shown to successfully detect phishing attacks in email.
- Blacklist, a method that requires human verification. Since this technique has a very low false positive rate, it is widely applied as anti-phishing in the toolbar.
- Whitelist, a method that is different from blacklist in that it needs to maintain records of all websites in the cyber world.

Mobile network operators can also participate in combatting phishing attacks. They can scan incoming and outgoing SMS and MMS messages in the mobile network and filter those containing phishing links by using anti-malware software. Moreover, they can establish global partnerships with other operators to prevent propagation of mobile malware by exchanging database information.

Spyware — Similar to phishing, users can play an active role to defend against spyware.

Adjust browser security settings: Most browsers allow users to adjust their security levels, usually with a scale from “high” to “low”.

Users should make use of these options so the browsers can stop unwanted operations.

Be very wary of pop-ups: Advertisements are often displayed in pop-up windows that might mask deceptive purposes. Some might pretend to provide a virus infection alert. Users should never click "yes." Instead, users should practice skeptical computing and always assume that any new program is potentially harmful unless it is proven otherwise. Users should keep in mind that answering "yes" to a prompt they do not understand can allow spyware to be loaded.

Always read the terms and conditions: Legitimate software vendors would disclose details about how they collect and use collected user information in the terms and conditions. Unfortunately, most users do not bother to read them. If users are particularly adamant about protecting their online privacy, it is better for them to know exactly what they are signing up for.

Use anti-spyware scanners: Users can deploy anti-spyware programs to scan their smartphones to detect malicious tracking software. Removing spyware from smartphones can be tricky, but it can always be quarantined so it is no longer used. Most anti-spyware programs provide ongoing protection by scanning incoming traffic and blocking any potential threats. Certainly, anti-spyware tools need to be updated regularly to remain fully effective.

Botnets — There are signs that would indicate a smartphone has been compromised as a zombie. The smartphone might seem a bit slower than usual. It may freeze occasionally or reboot itself. From these signs, users should be alerted. Another way to spot botnet activity is to check if the device is actively sending or receiving data, even when no related apps are running. Other signs include unwanted behaviors and degradation of system performance. Being a zombie can consume CPU capacity, disk usage, and network traffic. Users need to be alert to unusual behavior exhibited by their smartphones.

Botnets have been actively researched in recent years, primarily focussing on detection, measurement, tracking, mitigation, and future botnet prediction. Based on this research, effective tools are expected to be available to help smartphone users protect their devices from being compromised as a zombie. For example, Wang *et al.* [14] proposed a lightweight approach to detect malware. It introduces phantom contacts in the device to capture messages sent by malware. Based on the captured messages, further analysis is carried out to identify a signature of the message, or even a signature of the malware.

Conclusion and Future Work

In summary, the market penetration of smartphones will be increasing. Distribution of malware into smartphones is also expected to escalate. Efforts are required from app store administrators, app developers, researchers, and users to defend against malware. This article has summarized the major attacks caused by malware in smartphones and possible preventive approaches and detection mechanisms.

Even though the existing preventive approaches and detection tools can help prevent some of the attacks, the behavior of malware is changing rapidly and malware developers always have new ways to infiltrate smartphones. Therefore, more sophisticated tools need to be developed. Moreover, the limited resources in mobile devices should be taken into account in the design of such tools. It is envisioned that in the future the task of mitigating malware attacks on smartphones will be shared between the cloud and the device. The computationally intensive tasks should be carried out in the cloud, while detection by reduced classification schemes can be carried out locally by the device. We conclude this article by suggesting the following future research directions.

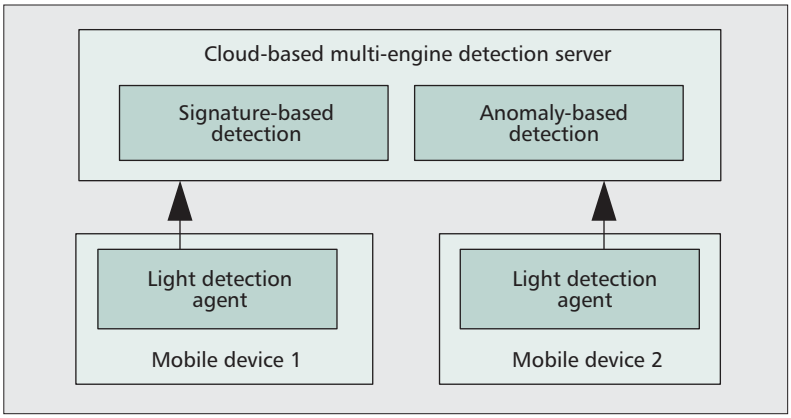

Figure 4. A cloud-based detection system.

First, more attention should be focused on how to collect the data of emerging malware systematically as they are usually hidden in apps distributed by different third-party markets. Due to competition, security companies are rather reluctant to make their malware database available to the public. As a result, researchers only have access to small samples of malware. Therefore, how to automate a systematic process to collect these malicious applications should be investigated.

Second, as described above, the key of signature-based detection is how to associate a malware with existing ones in order to carry out security analysis. Currently, cryptographic hash or package name are commonly used as identifiers. Unfortunately, they are not effective methods because hackers can change them easily. Often, security analysts can only discover malicious functions and structure by laborious reverse engineering processes. Thus, future work should focus on developing efficient methods to associate new malware with those in the database.

Third, mobile malware is evolving rapidly to avoid detection by existing detection techniques. Therefore, novel approaches are needed for timely discovery of new malware. Recently, some researchers suggested using machine learning approaches based on Bayesian classification for uncovering unknown malware on the Android platform [15].

Fourth, what is needed is a paradigm shift. So far, when security systems are designed, much effort is spent to find and eliminate all possible vulnerabilities to achieve perfect security. Other-

Even though the existing preventive approaches and detection tools can help prevent some of the attacks, behavior of malware is changing rapidly and malware developers always have new ways to infiltrate smartphones. Therefore, more sophisticated tools need to be developed.

wise, even a single vulnerability is sufficient for adversaries to dismantle the entire system. This imposes great difficulties on the design process. However, if such a single point of failure problem can be shifted from defenders to adversaries, then it is the adversary who needs to fight against any factor that prevents it from achieving its attack goals. Hence, future work should explore the single point of failure of adversaries.

Acknowledgment

This research is supported by a strategic research grant from City University of Hong Kong [Project No. 7004225], the Pearl River Nova Program of Guangzhou (No. 2014J2200051), the National Science Foundation of China (Grants: 51477056 and 61321064), the Shanghai Knowledge Service Platform for Trustworthy Internet of Things "(No. ZF1213), the Shanghai Rising-Star Program (No. 15QA1401700), a visiting scholar project of the State Key Laboratory of Power Transmission Equipment & System Security and New Technology (No. 2007DA10512713406), and the Specialized Research Fund for the Doctoral Program of Higher Education. D. He is the corresponding author of this article.

References

[1] IDC, "Worldwide Smartphone Shipments Top One Billion Units for the First Time, According to IDC," press release, 27 Jan. 2014; https://www.idc.com/getdoc.jsp?containerId=prUS24645514

[2] IDC, "Worldwide business use smartphone 2013-2017 forecast update," press release, 04 Dec. 2013; http://www.idc.com/getdoc.jsp?containerId=244840

[3] "254,158 Android apps are 'malicious' as mobile malware skyrockets 614 percent, Juniper says," June 26, 2013, http://venturebeat.com/2013/06/26/254158-android-apps-are-malicious-as-mobile-malware-skyrockets-614/

[4] M. La Polla, F. Martinelli, and D. Sgandurra,, "A Survey on Security for Mobile Devices," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 1, First Quarter 2013, pp. 446–71.

[5] D. Guo, A. Sui, and T. Guo, "A Behavior Analysis Based Mobile Malware Defense System," *Proc. ICSPCS*, pp. 1–6, 2012.

[6] G. Hogben and M. Dekker, "Smartphones: Information Security Risks, Opportunities and Recommendations for Users," Dec. 10, 2010, https://enisa.europa.eu/smartphonesecurity

[7] S.-H. Seoa *et al.*, "Detecting Mobile Malware Threats to Homeland Security Through Static Analysis," *J. Network and Computer Applications*, vol. 38, Feb. 2014, pp. 43–53.

[8] H. Hawilo *et al.*, "NFV: State of the Art, Challenges and Implementation in Next Generation Mobile Networks (vEPC)," *IEEE Network*, vol. 28, no. 6, Nov./Dec.2014, pp. 18–26.

[9] S. Ramu, "Mobile Malware Evolution, Detection and Defence," Term Survey paper, April 2012, http://blogs.ubc.ca/computersecurity/files/2012/04/SRamu_EECE572_SurveyPaper-SrikanthRamu.pdf.

[10] C. Wu *et al.*, "AirBag: Boosting Smartphone Resistance to Malware Infection," *Proc. NDSS*, 2014.

[11] N. Penning *et al.*, "Mobile Malware Security Challeges and Cloud-Based Detection," *Proc. CTS*, 2014, pp. 181–88.

[12] S. Zonouz *et al.*, "Secloud: A Cloud-Based Comprehensive and Lightweight Security Solution for Smartphones," *Computers & Security*, vol. 37, Sept. 2013, pp. 215–27.

[13] Y. Nadji, J. Giffin, and P. Traynor, "Automated Remote Repair for Mobile Malware," *Proc. ACSAC*, 2011, pp. 413–22.

[14] W. Wang *et al.*, "What You See Predicts What You Get — Lightweight Agent-Based Malware Detection," *Security and Communication Networks*, vol. 6, no. 1, Jan. 2013, pp. 33–48.

[15] S. Yerima, S. Sezer, and G. McWilliams, "Analysis of Bayesian classification-based approaches for Android malware detection," *IET Information Security*, vol. 8, no. 1, Jan. 2014, pp. 25–36.

Biographies

DAOJING HE [S'07-M'13] (hedaojinghit@gmail.com) received B.Eng.(2007) and M. Eng. (2009) degrees from Harbin Institute of Technology (China) and a Ph.D. degree (2012) from Zhejiang University (China), all in computer science. He is currently a professor in the Software Engineering Institute, East China Normal University, P.R. China. His research interests include network and systems security. He is an associate editor or on the editorial board of several international journals such as *IEEE Communications Magazine* and *IEEE/KICS Journal of Communications and Networks*.

SAMMY CHAN [S'87-M'89] (eeschan@cityu.edu.hk) received his B.E. and M.Eng.Sc. degrees in electrical engineering from the University of Melbourne, Australia, in 1988 and 1990, respectively, and a Ph.D. degree in communication engineering from the Royal Melbourne Institute of Technology, Australia, in 1995. He is an associate professor in the Department of Electronic Engineering, City University of Hong Kong.

MOHSEN GUIZANI [S'85-M'89-SM'99-F'09] is currently a professor and the associate vice president for graduate studies at Qatar University, Qatar. He received his B.S. (with distinction) and M.S. degrees in electrical engineering, and M.S. and Ph.D. degrees in computer engineering in 1984, 1986, 1987, and 1990, respectively, from Syracuse University, Syracuse, New York. His research interests include computer networks, wireless communications and mobile computing, and optical networking. He currently serves on the editorial boards of six technical journals, and is the founder and EIC of *Wireless Communications and Mobile Computing*, published by John Wiley (http://www.interscience.wiley.com/jpages/1530-8669/). He is an IEEE Fellow and a Senior Member of ACM.