1-2009

A Comprehensive Study for RFID Malwares on Mobile Devices

Qiang Yan

Yingjiu Li
Singapore Management University, yjli@smu.edu.sg

Tieyan Li

Robert Huijie DENG
Singapore Management University, robertdeng@smu.edu.sg

A Comprehensive Study for RFID Malwares on Mobile Devices

Qiang Yan[1], Yingjiu Li[1], Tieyan Li[2], and Robert H. Deng[1]

[1] School of Information Systems, Singapore Management University
[2] Institute for Infocomm Research, A*STAR, Singapore
{qiang.yan.2008,yjli,robertdeng}@smu.edu.sg,litieyan@i2r.a-star.edu.sg

Abstract. Radio Frequency Identification (RFID) technique has been widely accepted as wireless identification standard in the business world. While RFID technique enables efficient collection of identification information, it also introduces new security risk due to the emerging of RFID malwares. This risk becomes increasingly severe due to the adoption of internet in RFID applications (e.g., track and trace in EPCglobal network) and the use of mobile devices as RFID readers. The prior work to defend the threat of RFID malwares has mainly focused on the protection of front-end tag-reader communications and back-end database systems. Less work has been conducted to defend against RFID malwares in a systematic manner. In particular, no work has investigated RFID malwares on mobile devices that are connected to the internet. In this paper, we survey the state of the art in research on RFID and mobile malwares. The major challenges are identified in the research. To defend against RFID malwares on mobile devices, we propose an extended threat model, a basic anti-malware framework, and a list of intrusion detection techniques for future research.

1 Introduction

Radio Frequency Identification (RFID) is a contactless automatic identification and tracking technique, which has been widely accepted in the business world. As the replacement of traditional barcodes, RFID makes it more efficient to gather identification information about physical objects from a distance. On the other hand, RFID malwares have been recently expected to become a severe threat to RFID applications in the near future.

In the past, there used to be certain security myths about RFID malwares. One myth is that the limited storage capacity of RFID tag will make any harmful malware impossible to survive until one research team in Vrije University provides the first proof-of-concept malware design [1]. Their work shows that a harmful malware can be constructed without violating the capacity limitation of RFID Tag. Making the situation worse, the capacity limitation of RFID tag has been being relaxed with the development of IC techniques. Today, even some low-cost RFID tags have enough storage to hold certain common PC malwares; more powerful RFID tags will be emerging in the near future.

The new RFID standard, EPCglobal architecture [3] , aims to create a global network for sharing RFID-related product information between trading partners. To achieve high scalability and low cost, existing internet is used in EPCglobal architecture as backbone. The inherent security issues in internet makes RFID systems more vulnerable to malware attacks.

Due to the popularity of ubiquitous computing, integrating mobile devices with RFID readers exhibits an emerging trend in RFID applications. The use of mobile devices in RFID systems provides a flexible and efficient environment for information access and maintenance, but it also introduces new challenges for defending against RFID malwares.

The current research on RFID malwares has mainly focused on the protection of front-end tag-reader communications and back-end database systems. Relatively less effort has been made towards defending RFID malwares in a systematic manner. In particular, RFID malwares have not been investigated for RFID applications based on EPCglobal architecture and mobile devices. To facilitate research in this direction, we survey the state-of-the-art malwares for RFID and mobile systems. The major challenges are identified for defending against RFID malwares on mobile devices. To address the challenges, we propose an extended threat model, a basic anti-malware framework, and a list of intrusion detection techniques for future research.

The rest of this paper is organized as follows. The security challenges for defending against RFID malwares and mobile malwares are demonstrated in Section 2 and Section 3, respectively. The basic framework for defending RFID malwares on mobile devices is proposed in Section 4. Finally, a conclusion of this paper is given in Section 5.

2 State-of-Art RFID Malwares

The first proof-of-concept RFID malware is proposed in 2006 by a research team at Vrije University. The publication of their paper [1] triggers significant attention from the media, for it demonstrates that RFID malwares are realistically feasible with limited resources of RFID tags. Since the physical limitations for RFID malwares have been relaxed largely in latest RFID products, more RFID malwares are expected to emerge in the near future. In this section, we summarize various aspects of RFID malwares and the current countermeasures for defending them.

2.1 Essence of RFID Malwares

Similar to the traditional PC malwares, RFID malwares exploit software vulnerabilities to make software work abnormally. Previously, RFID malwares were considered impractical because RFID tags can only hold limited amount of data (usually less than 1024 bits). Therefore, only the existing malwares that reside

[3] EPCglobal architecture, http://www.epcglobalinc.org

in a small amount of data may be migrated to RFID scenarios. This requirement made some people believe that RFID malwares attack was unrealistic.

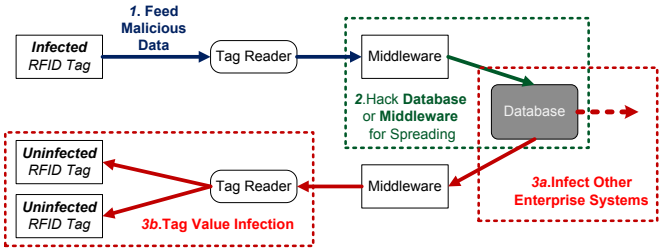

Fig. 1. Basic Threat Model for RFID Malwares

Figure 1 shows the basic threat model for RFID malwares given in [1]. Notice that the infected RFID tags can be common tags with limited resources or more powerful tags such as contactless smart cards. The basic threat model consists of the following steps: 1) The infected RFID Tag first feeds the tag reader with malicious data. 2) The malicious data are used to exploit the vulnerabilities of RFID middleware or database system. 3) If the middleware or database is successfully compromised, the malware can be spread by updating tag values with malicious data during regular tag updating. They can also infect other enterprise systems when they retrieve the malicious data from the database.

Three kinds of RFID malware attacks have been investigated before [1, 2]: SQL Injection, Code Insertion, and Buffer Overflow. **SQL Injection** for RFID is to encode malicious SQL fragments into tag values, which may hack into the backend database system to modify the data columns related to regular tag updating. **Code Insertion** to encode malicious script fragments into tag values, which may launch attacks such as Server Side Includes and XSS when the RFID system is managed by its administrator. **Buffer Overflow** is to feed tag readers with data whose size is larger than the expected length. This may cause buffer overflow as the middleware programmer may assume to process tag data of small size.

In addition, EPCglobal architectureallows using the internet infrastructure to achieve high scalability and cost-effectiveness for RFID middleware; therefore, RFID systems in EPCglobal network inherit the existing security vulnerabilities of the internet.

2.2 Capability of RFID Products

The major physical limitations for RFID malwares is the storage capacity of the RFID tags. Since a large number of tags are usually used in commercial RFID applications, the cost of RFID tag must be kept low to promote the adoption of RFID techniques. To reduce the cost of RFID tag, the storage capacity of

RFID tags is limited to hundreds or thousands bits in the previous low-cost tag products.

Table 1. Capability of Representative RFID Tags

Model	Price per tag	Tag ID (bit)	EPC ID (bit)	User Memory (byte)
RI-UHF-00001-01[a]	$0.09	32	96	N/A
Higgs-3[b]	$0.40	32	96(up to 480)	64
FBT-7400[c]	$5.00 (2006)	Unknown	Unknown	7.5K
LIME Tag[d]	$50.00 (2007)	128	96	512K

[a] Texas Instruments, http://www.ti.com
[b] Alien Technique, http://www.alientechnology.com
[c] Intelleflex, http://www.intelleflex.com
[d] SecureRF, http://www.securerf.com

With the development of IC technology, certain low-cost tags that are newly developed have relatively larger storage capacity that can even hold common PC malwares. Table 1 gives the product information of typical RFID Tags. The FBT-7400 tag has 7.5KB user memory and its price is only $5.00 per tag two years ago. [4] Moreover, the storage capacity of RFID tag is expected to keep increasing because this is essential to enable more applications of RFID techniques. Another motivation is that the deployment of sophisticated security mechanisms also demands large storage. In the near future, the storage capacity of RFID tags should no longer be a major limitation for RFID malwares.

Table 2. Capability of Representative RFID Readers

Model	Platform	Interface	RAM (byte)	Flash (byte)
ALR-9900 reader[a]	Linux, Java & .Net	LAN TCP/IP, RS232	64M	64M
MC9090-G handheld reader[b]	Windows Mobile 5.0	802.11a/b/g, Bluetooth v1.2	128M	64M
UHF Interrogator CF Card[c]	Windows and Linux	CF Type 1	N/A	N/A

[a] Alien Technique, http://www.alientechnology.com
[b] Motorola, http://www.motorola.com
[c] GAO RFID Inc, http://www.gaorfid.com

From the product information of typical RFID readers shown in Table 2, we can see that most of the RFID readers work on mainstream platforms. The RFID readers have become common peripheral devices for computer systems and they can be considered as another wireless interface like Wi-Fi and Bluetooth. The high integration of RFID devices with current computation environment means RFID systems will not only enjoy the power but also suffer from the vulnerabilities of the current computation environment.

[4] Some of the prices are estimated from the old reports. The current prices should be lower than the estimation. The publication year of those reports are labeled with their prices.

2.3 Practices of RFID Malwares

We now examine two events related to RFID malwares. Although no all technical details are available in the reports of the events, we can still learn valuable lessons from these events.

Event 1: Announcement of first proof-of-concept RFID malware (2006)

Rieback, Crispo, and Tanenbaum proposed the first artificial SQL/Script injection and buffer overflow examples together with a basic propagation model for RFID malwares [1]. They figured out that the malicious data stored in a small number of bits can be used to launch a SQL/Script injection attack that contains short malicious commands such as system shutdown. The RFID malware can be propagated by modifying the backend database for many tag values. Their malwares are experimented on an artificial RFID system with 256 KB Texas Instruments ISO-15693 compliant RFID tags. Their malwares require insecure database configuration which should be easy to prevent in practice.

Lesson 1: *It is enough to construct a RFID malware with the malicious data stored in a small number of bits without violating the capacity limitation of a RFID tag. RFID malwares can spread itself by modifying the backend database for many tag values.*

Event 2: Cracking of RFID enabled e-passport system (2007)

Lukas Grunwald started his cracking work for RFID systems in 2006. He has shown how to clone, extract, and modify information of RFID enabled e-passport in the top hacker conference defcon-14 in 2006 [5]. It took only weeks to forge an e-passport with his technique. This attack can be applied to any country's e-passport systems that adhere to the same International Civil Aviation Organization (ICAO) standard in the case that the access key printed on a passport page can be read. In 2007, he showed how to construct a malicious JPEG2000 image file that contains an e-passport photo to crash RFID middleware by exploiting the buffer overflow vulnerability in an off-the-shelf JPEG library [6]. Although the JPEG data is protected with digital signature, an attacker is still able to crash the system by loading malicious data. It is suggested that the vendors should choose off-the-shelf software/library carefully to avoid common vulnerabilities. Since the e-passport system is critically important for national security, many security experts claimed that RFID is the wrong type of technology for personal identification.

Lesson 2: *Data level protection mechanisms such as encryption and integrity checking may not provide complete protection against RFID malwares. We need more sophisticated system level protection against RFID malwares.*

2.4 Academic Research on RFID Malwares

The prior research on RFID malwares is based on the basic threat model proposed in [1]. The first work in this area [1] demonstrated the basic design principles for RFID malwares that exploit SQL-Injection and Server Side Including

[5] Defcon, http://www.defcon.org

[6] E-passport, http://www.wired.com/politics/security/news/2007/08/epassport

vulnerabilities. More examples for RFID malwares, including a simple buffer overflow attack, are provided in [2]. Sulaiman, Mukkamala, and Sung [3] reported platform test results for SQL Injection attacks in RFID systems. They [4] also proposed a new attack paradigm called fragmentation attack to break the capacity limitation for RFID malwares. In this paradigm, an RFID malware can be decomposed into multiple fragments that can be stored into resource-limited tags; the fragments can later be combined to form a functional malware under certain conditions so as to attack a target system. Recently, Rotter [5] analyzed the security and privacy risks of RFID systems in a systematic manner. However, none of the previous work on RFID malwares addresses the security challenges of adopting EPCglobal standards and mobile devices in RFID applications.

Among many working groups on RFID Security, it is worthwhile to mention MIT Auto-ID Lab [7]and RFID CUSP (i.e., RFID ConsortiUm for Security and Privacy) [8].

2.5 Industrial Efforts against RFID Malwares

Many companies run business on RFID security, eleven of which formed an alliance called "RFID Security Alliance" [9]. Most of the companies on RFID security commit themselves to anti-cloning and anti-counterfeiting of RFID tags, while one company, NeoCatena Networks, Inc. [10]provides anti-malware solutions for RFID systems. The security suite of NeoCatena Networks consists of three components, *RF-Audit*, *RF-Wall*, and *RF-Manager*. RF-Audit is a network monitor that analyzes network events to detect denial of service attacks and triggers early alarms for unexpected RFID network traffic. RF-Wall provides network security with RFID data encryption and digital signatures. RF-Manager is a management interface for the security suite. To defend against malware attacks, the security suite employs two techniques: one is content and format validation for tag data, and the other is pattern-based RFID traffic analysis.

Figure 2 provides an overview of the RFID malware countermeasures used in current industrial products. Due to the resource limitation of RFID tags, the computationally intense operations in performing the countermeasures are assigned to middleware or back-end systems. Current anti-malware solutions mainly focus on protecting middleware and backend database systems, more work needs to be done to protect front-end devices such as (mobile) RFID readers. Systematic solution is needed to guarantee security for every component in RFID systems.

3 State-of-Art Mobile Malwares

The first proof-of-concept mobile malware "Cabir" is proposed in 2004 by a virus writer named Vallez, a member of international group of virus writers known as

[7] MIT Auto-ID Labs, http://autoid.mit.edu
[8] RFID CUSP, http://www.rfid-cusp.org
[9] RFID Security Alliance, http://www.rfidsa.com
[10] NeoCatena Networks, Inc, http://www.neocatena.com

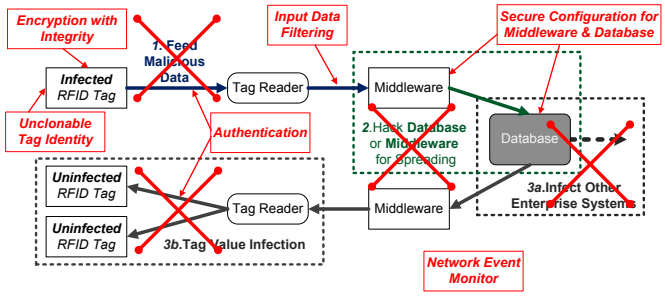

Fig. 2. Common countermeasures in industrial products

29A. This event was said to lift the curtain on a new era of mobile malwares [11]. However, the past four years didn't see any major outbreak of mobile malwares. Until now, the total number of mobile malwares is known to be hundreds, which is small if compared to millions of PC malwares [12]. Nonetheless, the popularity of smart phones and other mobile devices open up new opportunities for mobile malwares.

3.1 Vulnerabilities on Mobile Devices

The vulnerabilities on mobile devices can be classified into two categories: (i) *Basic implementation errors or design flaws*. This type of vulnerabilities usually results from improper assumptions on input parameters or program behaviors. For example, unrecognized codes in SMS and Caller ID may crash certain mobile phones. Insecure exception handlers for hardware failures may also be exploited by mobile malwares. (ii) *Lack of permission control*. Most mobile systems are single-user systems, where each process on a mobile device runs in a high privilege. Once a mobile malware is launched on such device, it can do anything in a high privilege if it is not explicitly forbidden by the mobile OS. To address this problem, the permission protection mechanism for system files is available, but only at v9 and above in the latest Symbian OS. Figure 3 shows the distribution of software vulnerabilities on mobile systems in CVE (Common Vulnerabilities and Exposures) database [13]. It can be observed that Symbian has less vulnerabilities than Windows Mobile and iphone.

The mobile malware attacks can be categorized into: (i) *Denial of service*, which crashes mobile phone and reboots it. Most of proof-of-concept denial of service attacks exploit the codes available on the internet. An advanced form of this attack uses Trojan horses to launch distributed denial of service for some specific phone numbers [6]. (ii) *Destruction*, which deletes system files or user data. The destruction attacks may be common for Mobile OS without permission protection for critical files. (iii) *Information stealing*, which forwards user

[11] Viruslist, www.viruslist.com/en/analysis?pubid=200119916
[12] Symantec, http://www.symantec.com/business/theme.jsp?themeid=threatreport
[13] CVE database, http://cve.mitre.org

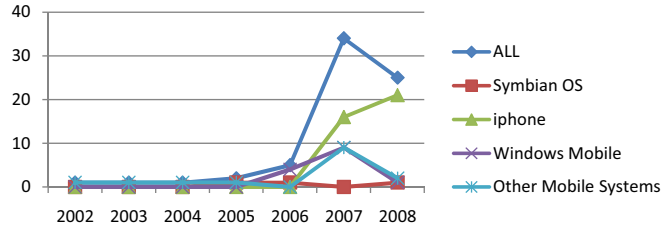

Fig. 3. The distribution of software vulnerabilities on mobile systems

data by SMS/MMS/Email without user prompt, or opens a backdoor for hacker [6]. Mobile malwares can be propagated through all available communication measures including SMS, MMS, Email, Blue Tooth, Wi-Fi, Flash Card, even RFID.

Nowadays, a barrier for mobile malwares to propagate is that user interaction must be involved for those non-crash-purpose malwares. None of today's mobile malwares can install themselves without the users accepting the standard security warnings[14]. Social engineering techniques, such as pretending to be a theme, a system patch, or a game installation, are widely used to tempt users to run malwares on mobile systems. The latest cell-phone malwares report from F-Secure as shown in Figure 4 indicates that 364 out of 373 malwares are designed for the most popular mobile OS, Symbian (57.1% market share in Q2 2008), which however has only three vulnerability records in the CVE database. All infection involves user download.

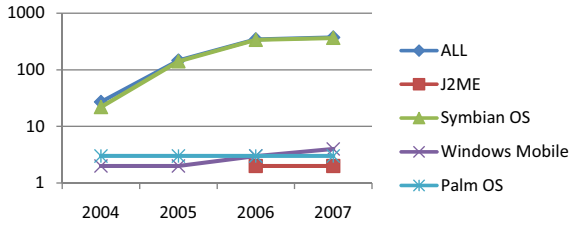

Fig. 4. Malwares per Platform by Year

3.2 Malware Trend on Mobile Systems

The phenomenon that there has been no major mobile malware breaks can be explained by the following reasons:

[14] Mikko Hypponen: Mobile Malware. Invited talk at the 16th USENIX Security Symposium, Boston, 2007. http://www.usenix.org/events/sec07/tech/

– Most mobile devices have limited functions that do not support installing many user softwares. Even if the installation is supported, mobile malwares may not be installed without user interactions.
– Most mobile devices cannot provide enough network capability to support the internet connection that is necessary for malware propagation. Only local propagations of mobile malwares are allowed through Bluetooth in most cases.
– Most people only use the phone or email functions of mobile devices such that infecting mobile devices may not lead to high potential profit.

However, this situation may change due to the fast development of mobile technology. With the popularity of smart phones, the device functionality may no longer be a limitation for propagating mobile malwares. Wi-Fi has been incorporated in the latest mobile devices, which allows malwares to obtain stabler and faster connections to the internet. Many people, including businessmen and college students, get used to storing sensitive or private data on their mobile devices. All these new trends inspire strong motivations for attackers to launch mobile malware attacks.

3.3 Academic Research on Mobile Malwares

Academic research on mobile malwares has focuses on investigating malware propagation and malware detection. For malware propagation, many stochastic models are proposed to characterize malware propagation behavior through Bluetooth or SMS/MMS [7–11]. On the other hand, the malware detection research can be considered as an extension of the malware detection on the PC platform. The solution is similar to the signature-based detection, which is adjusted for resource-constrained mobile computation environment.

Bose and Shin [6] provided a survey of mobile malwares from 2004, the first year when mobile malware was reported, to 2006, the year when the paper was published. The basic malware signatures provided in Bose and Shin's work is still valuable for today's mobile malwares. A high-level signature detection scheme is introduced later for mobile device based on the malware detection approach on PC platform [12]. In addition, Cheng et al. [13] presented a firewall solution between cellular network and internet to filter malicious data transferal.

3.4 Industrial Efforts against Mobile Malwares

Most anti-virus vendors offer the mobile versions of their anti-virus softwares. However, their solutions may not work extremely well due to the following reasons: (i) *Limited resources* are available on mobile devices for anti-virus softwares to consume. (ii) *Timely update on anti-virus softwares* may be guaranteed since internet connection is not always available on mobile devices. (iii) *Social engineering attacks* may tempt users to skip the warnings provided by anti-virus softwares. Once malwares are launched, anti-virus softwares could be neutralized due to poor runtime privilege control on mobile systems. The conclusion is that

anti-virus softwares on mobile devices are not mature and the current mobile anti-virus solutions are useful mostly for post-infection cleanup [12].

4 Anti-Malware Framework for RFID Systems with Mobile Devices

The threats of RFID malwares will become more immediate and severe in the near future due to the following two reasons. First, RFID systems will be widely deployed in business and industry (e.g., supply chain management, electronic payment, and access control). The high return on breaking such systems (e.g., forging credit cards and e-passports) will motivate attackers to launch attacks. The internet connections provided in EPCglobal network may facilitate the propagation of RFID malwares. The resource limitations for RFID malwares will be relaxed in new RFID tags due to the fast development of IC technology. Second, the integration of RFID readers and mobile devices opens more vulnerabilities for RFID malwares than their non-portable readers. The limited resources on mobile devices prohibit sophisticate anti-virus mechanisms from migrated from PC platform to mobile devices. To mitigate these threats, systematic solution should be designed to protect every component in RFID systems. In this section, we propose an extended threat model for RFID malwares, and then discuss anti-malware solutions for RFID systems with mobile readers.

4.1 Extended Threat Model

We extend the basic threat model proposed in [1] by including mobile devices and EPCglobal network (See Figure 5). The whole RFID system is partitioned into three domains: EPC core domain, company domain, and public domain. The EPC core domain contains the EPCglobal network, which should be maintained under the most strict security policies to establish trust among multiple involving parties. The company domain contains mobile devices, middleware, edge servers, and enterprise database systems. The company domain encapsulates business logic in RFID applications. The public domain contains RFID readers and tags, which is the weakest link in terms of information security. The malicious data carried by RFID tags can be malware entities, malware triggers, or malware fragments that can be later re-assembled into malware entities or triggers.

4.2 Anti-Malware Architecture for RFID Systems with Mobile Devices

To provide systematic protection for RFID systems with mobile devices, we propose to arm the mobile devices with an intrusion prevention system (IPS) and an intrusion detection system (IDS). Figure 6 shows this anti-malware architecture.

The IPS system works as a firewall on RFID readers and mobile devices that can monitor RFID traffics sending between RFID tags and middlewares. It checks the format and content according to RFID data specifications so as to

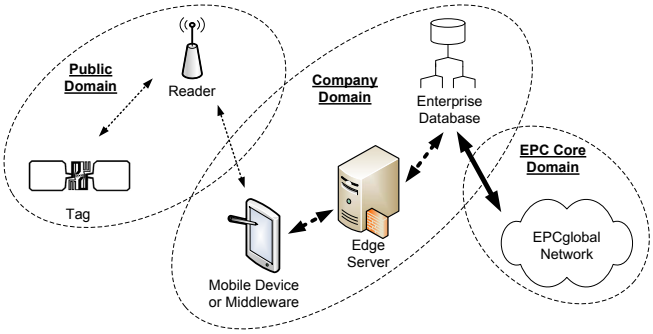

Fig. 5. Extended Threat Model for RFID Malwares

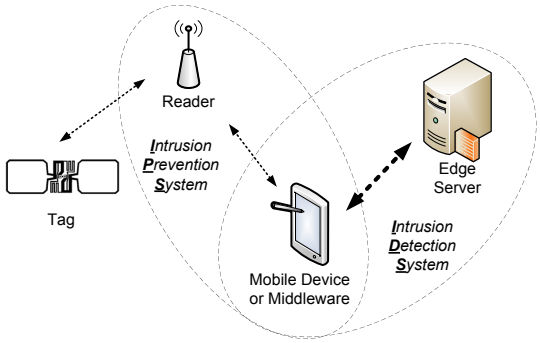

Fig. 6. Anti-malware Architecture for Mobile Devices

defend against DoS attack, SQL/Script injection, and shell code in text input. The IPS system may also check digital signatures of RFID data so as to prevent unexpected crash caused by loading malicious data payload.

Since the IPS system cannot filter out all malware attacks due to the constraint of limited resources at RFID readers and mobile devices, the remaining protection is handled by the IDS system. The IDS system will detect RFID malwares by monitoring the track between mobile device and edge server. The purpose is to thwart unexpected attacks such as buffer overflow attacks. A significant challenge for deploying IDS system on mobile devices is how to make the IDS system practical on resource-limited mobile devices. The IDS solutions developed for PC platforms cannot be directly applied on mobile devices since such IDS solutions are mostly resource demanding.

4.3 Potential Techniques for Practical IDS on Mobile Devices

To address the challenges of deploying IDS on mobile devices against RFID malwares, we discuss some potential pratical techniques for future study. The first technique is *good signature checking*. The huge size of signature database is

the major obstacle for IDS system to achieve practical performance on limited resources. In traditional signature-based solutions on PC platform, it is common to query a signature database with a half million records, each characterizing a malware's behavior. The complex program behaviors on PC platform make it difficult, if not impossible, to maintain signatures for malware-free programs. For convenience, we call the signatures for malware-free programs "good signatures." Considering that the functionalities of RFID readers on mobile devices are much simpler than general purpose PC systems, it is practically meaningful to use good signatures to detect RFID malwares on mobile devices.

The good signature based checking may have the following problems. The first problem is how to automatically generate efficient good signatures? Many related researches have been conducted for extracting behavior signatures by machine learning and static program analysis; however, most programs are still be analyzed manually by anti-virus experts. The second problem is how to secure the good signature database and IDS monitor? The latest mobile OS is still a single-user system, which provides little protection for IDS software. The IDS software may be neutralized once certain RFID malwares have chances to run. Some runtime privilege control mechanisms should be proposed to augment mobile OSs.

Another potential technique is *cooperative mode*. Since internet connection is guaranteed in EPCglobal network, it is not necessary for mobile devices to work alone in RFID systems. The mobile devices can shift part or all of the intrusion detection workload to cooperative servers, which can leverage on more resources to alleviate the bottleneck of RFID firewall on mobile devices.

The cooperative mode technique may have the following problems. First, which portion of IDS workload should be shifted to cooperative servers? This portion of workload should be determined carefully so as to guarantee both good-enough security and practically efficient performance. One possible solution is to dynamically adjust the work load to avoid the mobile device or any cooperative server from becoming the performance bottleneck. Another problem is how to cope with the situation in which the connection to the cooperative server is lost? It is possible that an attacker launches a DoS attack and blocks the communication channel between the mobile device and its cooperative server. The most conservative response is to stop any transactions, roll back to a pervious secure point, and report the event by certain backup channels. An alternative way is to process the safe transactions only that the mobile device can decide itself.

5 Conclusion

In this paper, we survey the state-of-the-art malwares and countermeasures for RFID systems and mobile systems. We propose an extended threat model to capture the malwares threats to RFID systems with mobile devices. We also discuss some potential techniques to defend against malware threats to RFID systems with mobile devices. In the future, we will deepen our analysis on RFID malwares and provide more technical details on anti-malware solutions.

References

1. Rieback, M.R., Crispo, B., Tanenbaum, A.S.: Is your cat infected with a computer virus? In: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications. (2006) 169–179
2. Rieback, M.R., Simpson, P.N., Crispo., B., Tanenbaum, A.S.: Rfid malware: Design principles and examples. Pervasive and Mobile Computing **2**(4) (2006) 405–426
3. Sulaiman, A., Mukkamala, S., Sung, A.: Sql infections through rfid. In: Proceedings of the 6th European Conference on Information Warfare & Security. (2007) 263–272
4. Suliman, A., Shankarapani, M., Mukkamala, S., Sung, A.: Rfid malware fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems. (2008) 533–539
5. Rotter, P.: A framework for assessing rfid system security and privacy risks. IEEE Pervasive Computing **7**(2) (2008) 70–77
6. Bose, A., Shin, K.G.: On mobile viruses exploiting messaging and bluetooth services. In: Securecomm and Workshops. (2006) 1–10
7. Mickens, J.W., Noble, B.D.: Modeling epidemic spreading in mobile environments. In: Proceedings of the 4th ACM workshop on Wireless security. (2005) 77–86
8. Su, J., Chan, K.K.W., Miklas, A.G., Po, K., Akhavan, A., Saroiu, S., de Lara, E., Goel, A.: A preliminary investigation of worm infections in a bluetooth environment. In: Proceedings of the 4th ACM workshop on Recurring malcode. (2006) 9–16
9. Yan, G., Eidenbenz, S.: Modeling propagation dynamics of bluetooth worms. In: Proceedings of the 27th International Conference on Distributed Computing Systems. (2007) 42
10. Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G.M., Mehes, A.: Can you infect me now?: malware propagation in mobile phone networks. In: Proceedings of the 2007 ACM workshop on Recurring malcode. (2007) 61–68
11. Meng, X., Zerfos, P., Samanta, V., Wong, S., Lu, S.: Analysis of the reliability of a nationwide short message service. In: 26th IEEE International Conference on Computer Communications. (2007) 1811–1819
12. Bose, A., Hu, X., Shin, K.G., Park, T.: Behavioral detection of malware on mobile handsets. In: Proceeding of the 6th international conference on Mobile systems, applications, and services. (2008) 225–238
13. Cheng, J., Wong, S.H., Yang, H., Lu, S.: Smartsiren: virus detection and alert for smartphones. In: Proceedings of the 5th international conference on Mobile systems, applications and services. (2007) 258–271