A Mobile Phone Malicious Software Detection Model with Behavior Checker

Teck Sung Yap and Hong Tat Ewe

Faculty of Information Technology,
Multimedia University, Malaysia

Abstract. There have been cases reported for the new threats from mobile phone technologies and it has raised the awareness among the technology and antivirus vendors. Malicious programs such as Viruses, Trojan, and Worms have been created and targeted at mobile phone. This paper discusses the possible attacking model on mobile phone adapted from malicious attack on computer. It also presents the types of attack and appropriate solution model for mobile phone. A prototype of the simulation of malicious software and detection software on mobile devices is developed and the results of applying this approach to simulated malicious software and detection software on mobile device are also presented.

1 Introduction

Computer viruses are well-known and dangerous risks to today's corporate computer environment. Related threats include other forms of destructive programs such as network worm, Trojan horse, Bacteria, Logic Bomb, Password Catcher, Trapdoors and war. Collectively, they are sometimes referred to as malicious program. Loss of data and crashed email servers are the main elements left in the wake of any virus attack [1], [2].

Another field, which could be affected by malicious program, is mobile phones. Incredibly fast development of wireless technology will soon turn them from an ordinary tool of voice transaction into a universal mobile communications portal with the rest of the world. Mobile phones will be powered with all features of modern PCs connected to the Internet. They will be equipped with operating system, text editors, spreadsheet editors and database processors similar to modern ones. Finally, users will have the ability to exchange with executable files. As exactly as it is with PCs, some of them may contain malicious programs [3], [4]. From previous research carried out by Gupta, V., & Gupta, S. [5], new wireless technology has opened up new exciting opportunities in the mobile e-commerce market such as financial transactions and online purchasing, with sensitive data transfer using mobile phones, thus security is one of the most important issues to be considered on this new service.

Viruses have been created to exploit vulnerabilities on mobile devices. The first mobile phone virus, a worm named Cabir, running on Symbian OS mobile phones, was discovered on 14th June 2004. Although this virus have not spread wildly, and are only a minor threat, they clearly demonstrate that mobile devices have become a

S. Shimojo et al. (Eds.): HSI 2005, LNCS 3597, pp. 57 – 65, 2005.

target for virus writers [6]. Subsequently, the finding of security flaws in Bluetooth enabled devices has explored the growing concern over the vulnerability of mobile phones. Bluejacking and bluesnarfing are the two forms of new intrusion. Bluejacking is a technique of sending anonymous messages to Bluetooth enabled device and bluesnarfing allows attackers to hack in and download data stored in mobile phones such as contact details and diary entries without leaving any trace [7].

The experts have warned that when mobile phones become more intelligent and powerful, the risk of mobile virus infecting mobile phones increases [3], [4], [8]. The development of standard technologies in mobile networks and the ability to constantly connect to the Internet, offer many Internet-based functionalities and services. It is anticipated that by 2005, mobile networks will be hit by a malicious program costing approximately $471 million for every five million users affected [9].

This paper discusses the potential threats of mobile phone and proposes an appropriate solution against malicious attack. It discusses the existing mobile phone threats including potential malicious attacks and suggests a solution model against the attacks. It also demonstrates the ease that certain types of malware (malicious software) can be implemented on a mobile phone and a proof-of-concept solution program is presented.

2 Present Mobile Phone Threats

The security challenges in the mobile environment are similar to the problems we have encountered in the PC world. Open platforms are becoming popular in smartphones, for example the Symbian operating system is used in more than 20 million mobile phones at the moment. Mobile phones are vulnerable to new forms of attack as they become more powerful in their capabilities.

Virus creators also exploit the vulnerabilities of Bluetooth enabled devices that could lead to explore others' personal data. Hacker can steal confidential data and retrieve the complete memory contents of the mobile phone including pictures and text messages. Bluetooth enabled mobile phones are easier to target because the system are designed to accept external connections from simple electronic devices. Bluejacking and Bluesnarfing are just 2 types of attacks on Bluetooth wireless technology.

Bluejacking is a technique of sending anonymous messages to other Bluetooth enabled device and receiving authentication response. The system becomes vulnerable as soon as the information exchange succeeds and all the data on the target device become available to the originator. On the other hand, bluesnarfing is an act of stealing and downloading data such as telephone number by hacker without alerting the owner of the target device. The undetected attack is affecting a number of popular models of mobile phones manufactured by Ericsson and Nokia.

In June 2004, the world's first mobile worm called “cabir” has been discovered. The worm was developed by an international group of hackers and was anonymously sent to experts in various countries. It replicates on the Symbian operating system used in several models of mobile phones made by Nokia, Siemens and Ericsson. It shortens the device's battery life by constantly scanning for other Bluetooth enabled devices. Although the worm will not damage a phone or its software, it is anticipated that more similar or worse threats are just waiting to emerge.

3 Potential Mobile Phone Threats

To discover new threats to mobile phones, we should mirror the development of malware (malicious software) on computer, which can duplicate attacking model for mobile phones technologies. It is likely that we will also see new kinds of attacks: malicious program in games, screensavers and other applications, resulting in false billing, unwanted disclosure of stored information, and deleted or stolen user data.

3.1 Trojan

The primary concern of malicious attack is from Trojan applications. Nowadays, it is very common to find a computer Trojan that transmits spam emails to Internet user [10]. This will interrupt network performance and create lots of inconvenient issues to user, but generally involves no direct cost to the user. However, a similar Trojan on a phone could impose a heavy financial penalty on the consumer. In next section, it shows a Trojan application that sends SMS messages without any notification. These messages could be used to spam other users at random, or could be targeted at users stored in the phonebook. Such Trojans could be further developed, again requiring little programming effort, to send their messages to reverse billed numbers, generating revenue for the developers. For example, an application that sends messages at a rate of $1/sms, if the infected application runs for an average of 100 SMS/day, it would cost user $100/day. Consumers will only receive mobile billing after 30 days before the mobile owner realizes that his phone has been infected by malicious program.

3.2 Worm

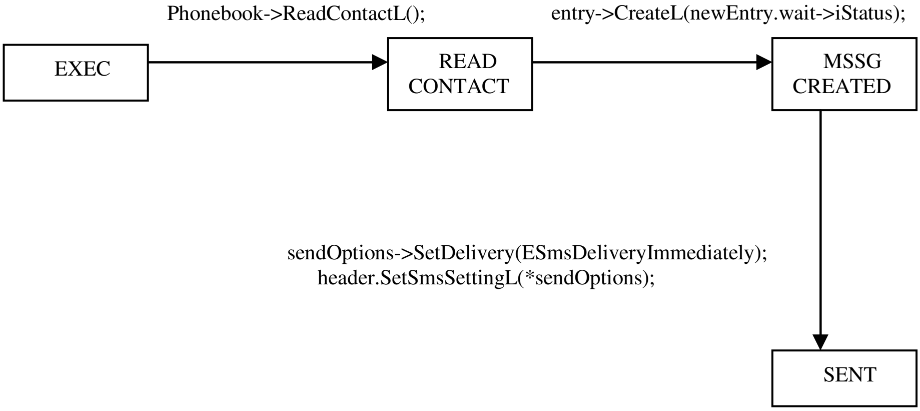
The second area of attack is to develop a self-replicating mobile application. This type of malicious program can be developed from a Trojan by attaching a copy of itself to the MMS messages. For such viruses to work, interaction with the message recipient is required. But one thing for sure is that MMS message service does not allow any application file to attach with it for this moment [10].

3.3 Virus

Virus is the most destructive program designed to damage files or otherwise interfere with the mobile phone's operation. Similar attacks can be developed for other nefarious reasons, such as copying the contents of the phone’s address book and sending them elsewhere, corrupting or deleting the numbers in the address book, blocking incoming call, and a whole host of other denial of service attacks [10].

4 Developing a Simple Mobile Phone Attack

For this section, we are not going to elaborate how to develop all of the malware application described in the previous section, but will outline the development of a simple Trojan implemented for the Symbian operating system, as an example of the ease with which such a form of malware can be developed. This application consists of a simple graphic user interface with a Trojan embedded within the code that sends an SMS to the first contact number in the phonebook when the function has been executed.



```
Phonebook->ReadContactL();
entry->CreateL(newEntry.wait->iStatus);
sendOptions->SetDelivery(ESmsDeliveryImmediately);
header.SetSmsSettingL(*sendOptions);
```

Diagram 1. Malware attack model

Diagram 1 is a pictorial representation of malware's behavior and attack model on Symbian operating system. When the Trojan application has been executed, "EXEC", it will retrieve the first contact from phonebook, "READ CONTACT", and create a SMS message entry for it, "MSSG CREATED". This message will be scheduled to send out for the contact owner.

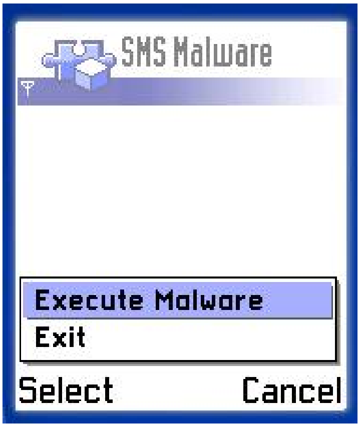
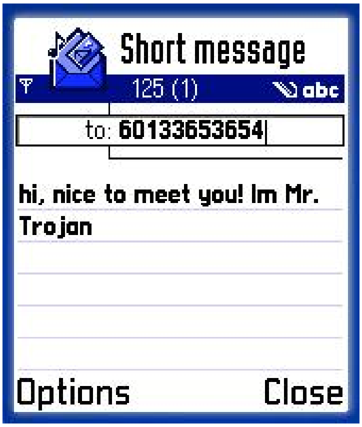


Fig. 1. Malware interface



to: 60133653654

hi, nice to meet you! Im Mr. Trojan

Fig. 2. SMS message

Figure 1 and 2 illustrate the Trojan application interface and the sent message as it appears in the Sent Message folder after it has been scheduled to send out.

This application can hide behind any program or software, when it has been triggered, similar malicious activity will happen. As discussed in previous section, a more malicious attack is the one that continually sends messages without user acknowledgment; which will bring high financial cost to the user.

5 Proposed Solution Against Mobile Phone Attack

The security issue about mobile phones' threats has awakened the awareness of security software provider and also the mobile phone manufacturer. At present, at least three software companies have released personal security software for emerging smartphones, which are exposed to the attack of a new wave of phone viruses. F-Secure is one such firm, selling antivirus and encryption software for smartphone operating systems made by Palm, Microsoft and the Symbian platform common in Europe.

5.1 Antivirus Techniques

In order to propose a good solution for mobile phone attack, we should examine how the current computer antivirus software works. We'll start with some common antivirus techniques and find an appropriate solution for this case. Three different antivirus techniques that are used to locate and eliminate viruses will be discussed. These include scanning, behavior checking and integrity checking. Basically, the scanner searches for specific code, which is believed to indicate the presence of a virus, behavior checkers look for programs that do things that viruses normally do and integrity checkers monitor for changes in files [10].

Scanning. Scanning for viruses is the oldest and most popular method for locating viruses. Back in the late 80's, when there were only a few viruses floating around, writing a scanner was fairly easy. Today, with thousands of viruses and many new ones being written every year, keeping scanner up to date is a major task. For this reason, many professional computer security scanners are obsolete and not useful. However, scanners have important advantages over other type of virus protections as they allow one to catch a virus before it ever executes in your computer [10].

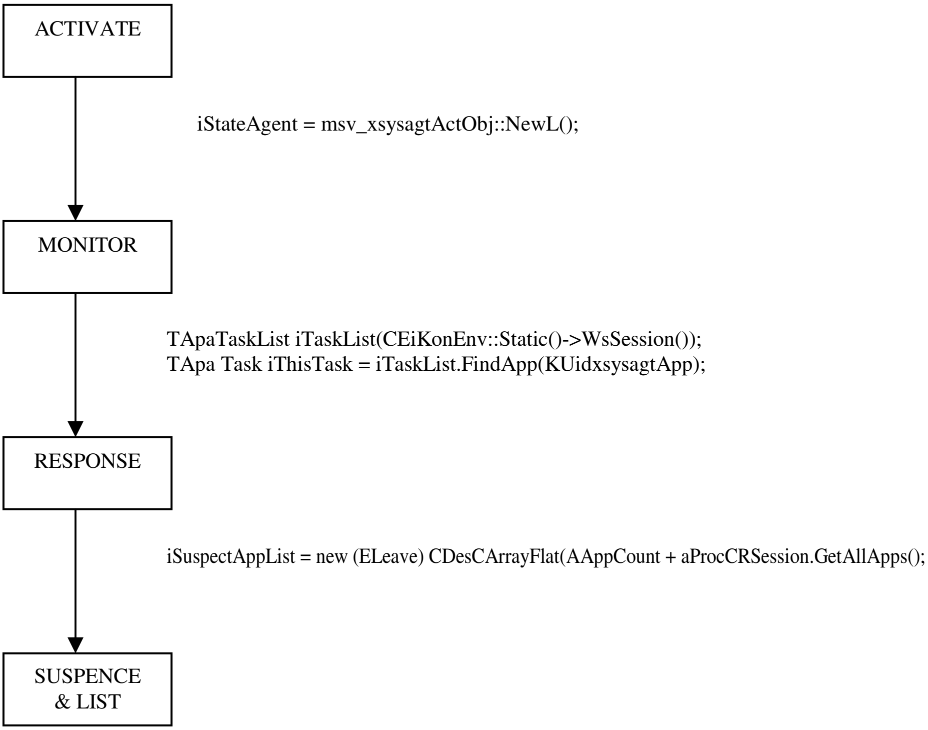
Behavior Checker. Behavior checkers watch your computer for virus-like activity, and alert you when it takes place. Typically, a behavior checker is a memory resident program that a user loads in the AUTOEXEC.BAT file and then resides in the background looking for unusual behavior [10].

Integrity Checker. Typically, an integrity checker will build a log that contains the names of all the files on a computer and some type of characterization of those files. That characterization may consist of basic data like the file size and date/time stamp, as well as a checksum. Each time the user runs the integrity checker; it examines each file on the system and compares it with the characterization it made earlier [10].

5.2 Proposed Solution

In this paper, behavior checker will be the proposed technique to apply in the mobile phone platform where it can detect malicious activities appeared in the system. Over the years, this technique has evolved when antivirus vendors moved their direction into behavior checker technique to overcome the limitation of current antivirus software [11]. Behavior checker does not require virus pattern for detection but it monitors activities or behavior of application running in the system. Misuse detection method will be used for the above-mentioned solution where it detects attacks as instances of attack behavior [12], [13]. This approach can detect known attacks accurately and generate low false alarm rate. So, misuse detection needs to package with a list of known attack behaviors in a particular system. This method is efficient because mobile phone features are quite limited and it is easy to compile a potential attack behavior list for detection purpose.

We will present a proof-of concept solution program based on the malware behavior created in previous section. Both the program will be tested in Nokia Mobile Phone running Symbian operating system. Symbian OS uses message type modules (MTM) to define message types. Each MTM is composed of four classes that are used as base classes for specific message handling implementation. Whenever any application wants to use any of the messaging functionality it needs to create a session with the message server. A detector application can observe all the sessions that have been created with the message server and then monitor all the message events that take place in a session.



```
iStateAgent = msv_xsysagtActObj::NewL();
```

```
TApaTaskList iTaskList(CEiKonEnv::Static()->WsSession());
TApa Task iThisTask = iTaskList.FindApp(KUidxsysagtApp);
```

```
iSuspectAppList = new (ELeave) CDesCArrayFlat(AAppCount + aProcCRSession.GetAllApps();
```

Diagram 2. Simplified Malware Detection Model

Diagram 2 is a pictorial representation of detection model for proposed solution for mobile phone. When detector application has been activated, "ACTIVATE", the detector engine will be started and sits behind the system to monitor activities within the message server, "MONITOR". The detector application is notified of every event that takes place within the session. The message event of interest is "EmsvEntryCreated", which is used to create new entry in any of the folders such as the Inbox, Outbox and Sent Items. Whenever "EmsvEntryCreated" events are inherited by unauthorized program and detected by the detector, "RESPONSE", the activity session will be suspended and the user will be alerted with a list of suspected malware, "SUSPEND & LIST". It shows that when the event is misused by any application, the solution should be able to provide fast response on it.

In Figures 3 and 4, it shows the application interface of detector engine and a list of suspected malicious programs for user further actions.

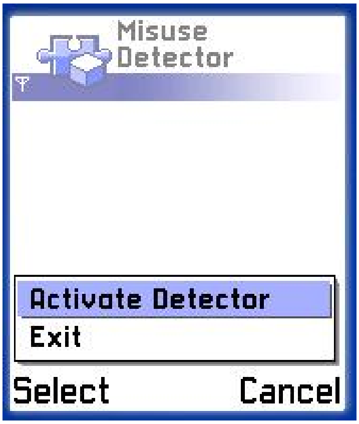
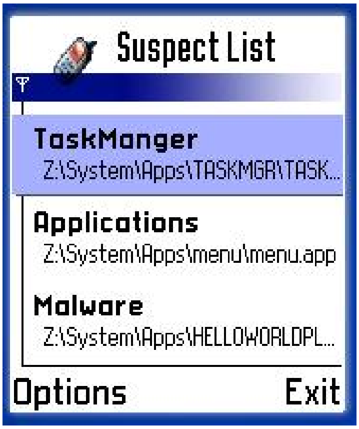


Fig. 3. Misuse Detector



TaskManger
Z:\System\Apps\TASKMGR\TASK...

Applications
Z:\System\Apps\menu\menu.app

Malware
Z:\System\Apps\HELLOWORLDPL...

Fig. 4. Suspected Application List

Detection Specification. This proof-of-concept program has shown the detection concept based on specific attack behaviors to monitor all malicious activities within the message server. Thus, we can detect all the malicious activities occurred. The attack behaviors for this program are:

- monitor any application using message server service without user authorization
- monitor "EmsvEntryCreated" event within message server sessions

Any program with this attack behavior will be suspended for further action. This solution has proven to provide an accurate detection to any malicious program, which tends to send SMS without notification. This solution model can be extended to monitor a sequence of events within a session and it can provide a more comprehensive detection engine for mobile phone system.

6 Conclusion

Security impact is an important issue to mobile phone technology in the near future. As mobile devices continue to become more prevalent and packed with greater processing power and wireless capabilities, they will become a more enticing target of choice for virus creators.

This paper has demonstrated the ease with which malware application can be developed and discussed potential threats on mobile phone. The Trojan application implemented for Symbian operating system shows its destructive action by sending anonymous SMS. From the experiment, the SMS is successfully sent and no security protection exists for such malicious activities.

This paper has proposed an appropriate security solution model on mobile phone for future security development. Misuse detection method based on behavior checker technique has been applied to a solution program to detect above-mentioned Trojan application. This solution has proven to provide an accurate detection to any malicious program, which tends to send SMS without notification. Based on a very similar solution model, we can add more modules, which help in tracking other malicious activity related to the file-system, the contacts database and even the phone module.

References

1. Davis, R. “Exploring computer viruses”, Aerospace Computer Security Applications Conference, Fourth, Pages: 7/11, 12-16 Dec. 1988
2. Slade, R. (1996). Guide to computer viruses (2nd ed.). New York: Springer-Verlag.
3. Jamaluddin, J.; Zotou, N.; Coulton, P., “Mobile phone vulnerabilities: a new generation of malware,” Consumer Electronics, 2004 IEEE International Symposium Pages:199 - 202, Sept. 1-3, 2004
4. Dagon, D.; Martin, T.; Starner, T., “Mobile Phones as Computing Devices: The Viruses are Coming!”, Pervasive Computing, IEEE , Volume: 3 , Issue: 4, Pages:11 - 15, Oct-Dec 2004
5. Gupta, V., & Gupta, S., “Securing the wireless internet”, IEEE Communication Magazine, Vol 39, No.12, 2001, pp 68-74
6. eFinland (1 Nov 2004). Preparing for Mobile Phone Viruses [Online] Available: http://www.e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=29431 [2004, November 1]
7. BluejackQ (No Date). What is Bluejacking [Online]. Available: http://www.bluejackq.com/what-is-bluejacking.shtml
8. BBC News World Edition. “Mobile Virus Threat Looms Large” [Online] Available: http://news.bbc.co.uk/2/hi/technology/2690253.stm
9. Belson, Ken. “A Brand New Worry: Mobile Phone Viruses”, International Herald Tribune: The IHT Online Available: http://www.iht.com/cgibin/generic.cgi?template=articleprint.tmplh&ArticleID=119373
10. Mark A. Ludwig (1995). Black Book of Computer Viruses. American Eagle Publication, Inc.
11. Ellen, M.(2002, February 1). Behavior blocking repels new viruses [Online] Available: http://www.nwfusion.com/news/2002/0128antivirus.html

12. D. Denning, “An Intrusion-Detection Model,” IEEE Transactions on Software Engineering 13(2), pp. 222-232 (Feb. 1987)
13. H. Teng, K. Chen, and S. Lu, “Adaptive Real-Time Anomaly Detection Using Inductively Generated Sequential Patterns,” Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, pp. 278-284 (May 1990)