Ontology-based Mobile Malware Behavioral Analysis

Hsiu-Sen Chiang, Woei-Jiunn Tsaur

Department of Information Management
Da-Yeh University, Changhua, Taiwan, R.O.C.
chianghs@mail.dyu.edu.tw, wjtsaur@yahoo.com.tw

Abstract. Recently, Mobile malware such as Cabir, Duts, and Brador has caused harm by leaking of user privacy, depletion of battery power, and extra service charges by automatically sending expensive multimedia messages or making long-distance calls. Also, the convenience which can download programs from the Internet and share software with one another through short-range Bluetooth connections, worldwide multimedia messaging service (MMS) communications and memory cards has created new vulnerabilities. As we know, anti-malware software is to play an essential role in defending against mobile malware. The majority of detection software relies on an up-to-date malware signature database to detect malware. However, mobile phone networks have very different characteristics in terms of limited processing power, storage capacity and battery power. It is a challenge to distribute malware signatures files to mobile devices in a timely manner, and therefore limits the effectiveness of complex anti-malware solutions in battery-powered handsets. This paper proposes an ontology-based behavioral analysis for mobile malware, and further provides information about mobile malware for end users or organizations to help them use their mobile phones securely.

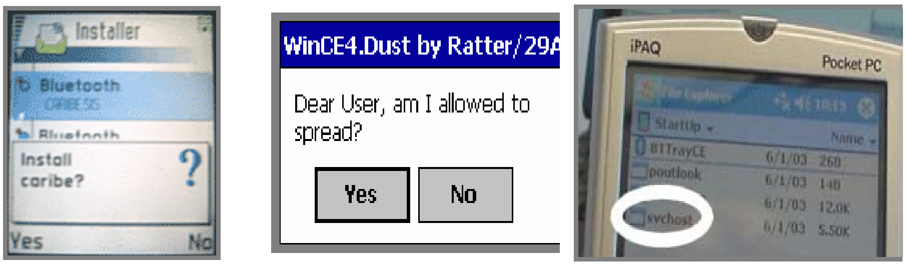
Keywords—Mobile malware, smart phone, ontology, behavioral analysis.

1 Introduction

At present, mobile devices have become convenient and often essential components assisting us in our everyday life, because they provide “all-in-one” convenience by integrating traditional mobile phones with handheld computing devices. As cell phones have evolved into smart phones, more and more people are using the devices to download programs from the Internet, and do e-mail, instant-messaging, worldwide short messaging service (SMS) and multimedia messaging service (MMS) communications. Unfortunately, mobile devices’ increasing popularity and its features have attracted the attention of malware writers and provided vulnerabilities for hackers to install malware or for users to run it inadvertently on a device. Cabir (Ferrie et al., 2004), the first mobile worm targeting Symbian operating system has been reported in June 2004, used Bluetooth channels to spread onto other mobile phones. As a worm, Cabir is very basic, because it simply makes copies of itself arriving to other phone and does not modify or attach itself to existing files. The first Windows CE virus called Duts is also reported in July of the same year, which is a true virus, and it inflects all the files in the devices' root directory that run Windows mobile by appending itself to them, after displaying the message: 'Dear user, am I allowed to spread?'. Furthermore, some mobile malware is not as rudimentary. In fact, as with the majority of PC malware, the attractions of Trojan horse are more than file-infecting viruses in mobile environments. Both WinCE.Brador and Symbian.Skuller are Trojan backdoor that does not replicate itself from a device to other ones but it relies on users to download and manually launch the Trojan applications (Chien, 2004). To illustrate these behaviors mentioned above, Table 1 summarizes them alongside a variety of other mobile malware (Gostev, 2006). From year 2004 to 2008, the number of types of mobile malware has increased significantly. As of March 2008, F-Secure has counted 401 different types of mobile malware in the world, and McAfee has counted 457 kinds of mobile malware, as shown in Fig. 1 (Lawton, 2008). Mobile malware has caused various harm such as leaking of user privacy, extra service charges by automatically sending expensive multimedia messages or making long-distance calls, and depletion of battery power. Currently, even at least 15 variants of Cabir may be found spreading in over 35 countries (Coursen, 2007), and 0.5~1.5% of MMS traffic in a Russian mobile network is made up of infected message, which is close to the fraction of malicious code in the email traffic (Yury, 2006).

Table 1. Behavior types of mobile malware

Behavior	Name	Date	Target OS	Functionality	Technology used	Number of variants
Internet Worm	Cabir	June 2004	Symbian	Spreading via Bluetooth	Bluetooth	15
Virus	Duts	July 2004	Windows CE	Infecting files	File API	1
Trojan Backdoor	Bardor	Aug. 2004	Windows CE	Providing remote network access	Network API	2
	Skuller	Nov. 2004	Symbian	Replacing files, icons and system applications	OS vulnerability	31



Install caribe?

Dear User, am I allowed to spread?

(a) Internet Worm – Cabir

(b) Virus – Duts

(c) Trojan Backdoor – Brador

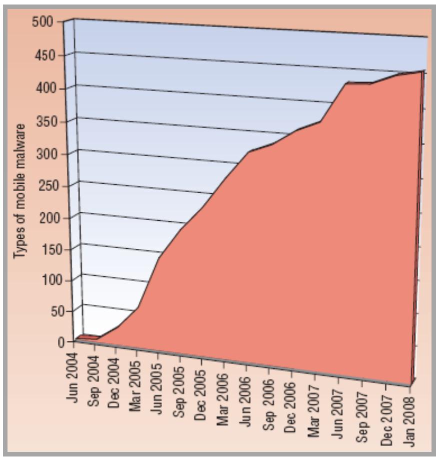


Fig. 1. The growth of mobile malware.

Currently, in response to this increasing threat, security vendors such as F-security, Kaspersky Lab, McAfee, and Symantec have released mobile anti-virus, firewall, and encryption products. As desktop environments, anti- malware solutions are the major mechanism against mobile malware. Such a mechanism relies on an up-to-date malware signature database and scanning engine to detect them. However, several important differences exist between mobile and traditional desktop environments. First, a mobile device typically has only limited processing power, storage capacity and battery power. Although mobile devices' CPU speed and memory capacity have been increasing rapidly at low cost in recent years, they are still much less than their desktop counterpart. In particular, energy-efficiency is the most critical requirement that limits the effectiveness of complex anti-malware solutions in battery-powered mobile devices. Second, mobile malware can spread without the reliance on the network infrastructure, e.g., through Bluetooth interfaces. This can happen when a new malware emerges and the anti-malware researchers have not yet identified its signature. As a result, even when the malware signature is available, the mobile device may not be able to obtain it in a timely manner. If the signature of a malware is outdated, its effectiveness will diminish. Lastly, a mobile device is highly mobile and always has a greater degree of difficulty in quarantining the malware in a local region.

Malware disasters and incidents have organizational ramifications beyond the money, resources, and effort required to recover from such incidents. This paper proposes an ontology-based behavioral analysis for mobile malware, and further provides information about mobile malware for end users or organizations to help them use their mobile phones securely. Ontology theory is a research methodology which gives us the design rationale of a knowledge base, kernel conceptualization of the world of interest, semantic constraints of concepts together with sophisticated theories and technologies enabling accumulation of knowledge which is dispensable for knowledge processing in the real world. Furthermore, ontologies also provide a mechanism to allow inferenceing on the data, such that an inference engine, in combination with rules, can derive new facts and conclusions implicitly represented in the data. Thus, the ontology theory is adopted to support the behavioral description and the knowledge management of mobile malware. In the future, this work will be applied to develop a detection framework that overcomes the limitations of signature-based detection while addressing unique features and constraints of mobile handsets.

The rest of the paper is organized as follows. Section 2 reviews related work and lists major technologies and methodologies for mobile malware detection in mobile environments. In Section 3, we have a brief description of ontology theory that will be used for analyzing the behaviors of mobile malware. The process of mobile malware' ontology knowledge representation is described in Section 4. We conclude by presenting our plans for future work in the last section.

2 Related Work

Internet worms and computer viruses have been plaguing computer environment for many years and led to the widespread investigation of malware propagation on the internet. Traditionally, the detection of malware is handled by anti-malware software. The most commonly-used technique for malware mitigation is signature-based methods. Typically, a signature-based method is picked to illustrate the distinct properties of a specific malicious executable. A unique detection signature is extracted by an expert in the field or using static information and a code value for each malware program so that future examples of it can be correctly classified with a small error rate. Therefore, this type of detected method must rely on a signature database to analyze each malware. In other words, signature-based detection cannot detect an attack from unknown malware or its variant (Christodorescu et al., 2005; Morales et al., 2006). Protection from unknown malware is the major issue of the day in computer virology. The anti-malware community relies heavily on known signatures to detect malicious programs but all efforts still haven't solved the key problem until behavior based method appeared. The behavioral detection method is based on an in-depth understanding of malware' nature, characteristics, and dynamic behavior. The runtime behavior of an application is monitored and compared against malicious and normal behavior profiles. Behavioral detection is more resilient to polymorphic worms and code obfuscation, because it assesses the effects of an application based on more than just specific payload signatures. Moreover, behavioral detection has potential for detecting new virus and zero-day worms (Wang et al., 2005), because new virus are often constructed by adding new behaviors to existing malware or replacing the obsolete modules with fresh ones, indicating that they share similar behavior patterns with existing malware (Christodorescu et al., 2005). In addition, Signature-based detection methods do not be efficient for resource-limited mobile devices because they must check if each derived signature of an application matches in the virus database. Moreover, due to the high mobility of devices and the relatively closed nature of cellular networks, constructing network signature of mobile malware is very difficult. Thus a lightweight and novel detection method is required.

There have been recent studies to model propagation of such malware in cellular and ad-hoc networks. Most previous works of mobile malware propagation are focused on Bluetooth worms. Generic worm propagation model is based on behavioral signatures that describe aspects of any particular worm's behavior such as sending similar data from one machine to another, the propagation pattern, and the change of a server into a client (Ellis et al., 2004). Khayam and Radha (2005) developed a topologically-aware worm propagation model for stationary wireless sensor networks. They incorporate MAC layer interference into this model by specifying a constant infection rate when a worm spreads itself onto its neighbors. Mickens and Noble (2005) observed that traditional epidemic models fail to characterize worm propagation in mobile networks, so they modified traditional analytic models to create a probabilistic queuing technique that accounted for movement and traffic patterns over various time durations. Zheng et al. (2004) focused on modeling population distribution density, Bluetooth radius, and node velocity. Statistical Monitoring observed that the logical ordering of an application's actions over time. Cheng et al. (2007) present SmartSiren, a collaborative virus detection and alert system for smart-phones. In order to detect viruses, SmartSiren collects the communication activity information from the smart-phones, and performs joint analysis to detect both single-device and system-wide abnormal behaviors. Taejoon and Shin (2005) proposed a File system Monitoring method that can be monitored by checking file integrity, file attributes, or file access attempts. In checking for file integrity, the agent yields messages digests or cryptographic checksums for critical files, compare them against reference values, and verified their differences. Power-monitoring malware-detection framework that monitors detects and analyzes previously unknown energy-depletion threats. Kim et al. (2008) characterize power consumption patterns of events and designed two important system components to perform a comprehensive analysis of the detection accuracy for pinpointing the identify of events, as well as classifying them as malicious or normal. SMS/MMS and Bluetooth vulnerabilities analysis identified the vulnerabilities in Bluetooth and SMS/MMS messaging systems that may be exploited by future mobile malware. By analyzing existing mobile malware to extract a set of their common behavior vector can be used to develop mobile malware detection and containment algorithm. Bose and Shin (2006) investigated the propagation of mobile worms and viruses that spread primarily via SMS/MMS messages and Bluetooth. First, they analyze these propagated vulnerabilities in-depth so that appropriate malware behavior models can be developed. Next, they study the propagation of a mobile malware similar to Commwarrior in a cellular network. This result reveal that hybrid worms that use SMS/MMS and proximity scanning (via Bluetooth) can spread rapidly within a cellular network, making them potential threats in public meeting places such as sports stadiums, train stations, and airports. Ruitenbeek et al. (2007) also investigate propagation of MMS/SMS malware and various responses, although within only a small user population with an unconstrained messaging server. Bose et al. (2008) presented a behavioral detection framework for viruses, worms and Trojans that increasingly target mobile handsets, and used the technique of support vector machines (SVMs) to train a classifier from normal and malicious data. Schmidt et al. (2009) demonstrate how to monitor a smart-phone running Symbian OS. In order to extract features that can be used by anomaly detection methods, this research analyzed the normal and abnormal behaviors of mobile malware. Quarantine defense can be used against Bluetooth worms. Quarantine-based systems prevent a suspicious or infected client from sending or receiving messages. If Bluetooth worms are found on cell phones located at a specific area, quarantine tools can prevent them from spreading to other places. Recent industry initiatives such as Network Admission Control (NAC) (Cheng et al., 2007) and Network VirusWall (Trend Micro, 2004) are intended to enforce established security policies to endpoint devices as they enter a protected network. A wide variety of used methods for detecting mobile malware are listed in Table 2.

Table 2. The researchs of mobile malware detection

Authors	Methods of classification	Limits of energy-efficiency	Unknown malware detection
Mickens and Noble, 2005; Zheng et al., 2004; Ellis et al., 2004; Khayam and Radha, 2005	Generic worm propagation model	Yes	No
Cheng et al., 2007	Statistical monitoring	Yes	No
Taejoon and Shin, 2005	File-system monitoring	Yes	No
Kim et al., 2008; Flinn and Satyanarayanan, 1999	Power-monitoring	No	No
Bose and Shin, 2006; Ruitenbeek et al., 2007	SMS/MMS and Bluetooth vulnerabilities analysis	Yes	No
Bose et al., 2008	Support Vector Machines	Yes	No
Schmidt et al., 2008	Anomaly-based detection and monitoring	No	No
Cisco; Trend Micro	Quarantine defense	Yes	No

3 Methodology

The importance of capturing and representing real world knowledge in information systems has long been recognized in artificial intelligence, software reuse and database management. According to the past studies, ontology is defined as “a formal specification of a shared conceptualization”. An ontology can be considered as a model capable of providing required formalization and powerful constructs that include machine-interpretable definitions of the concepts within a specific domain and the relation between them. In practical terms, ontology is a hierarchy of concepts with attributes and relations that defines a terminology in consensus semantic networks of inter-related information units. One of the most common goals for developing ontology is for sharing the understanding about the structure of information among people or software agents. Ontology explicates the conceptualization of the target world and provides us with a solid foundation on which we can build sharable knowledge bases for wider usability than that of a conventional knowledge base.

Ontology has been developed in a variety of areas, such as the large-scale investment (Lenat, 1995), natural language understanding (Dahlgren, 1995) and data integration (Kedad, and Metais, 1999). In fact, it is believed that the use of ontology gives us the design rationale of a knowledge base, kernel conceptualization of the world of interest, semantic constraints of concepts and technologies enabling accumulation of knowledge, which are dispensable for knowledge processing in the real world.

3.1 Ontology Building

Basically, a series of approaches have been reported for building ontology. In 1990, Lenat and Guha published the general steps and some interesting points of ontology building in their Cyc development. In 1995, Gruninger and Fox proposed the enterprise ontology and the TOVE project ontology. Bernaras et al., 1996, presented a method to build ontology in the domain of electrical networks as part of the Esprit KACTUS project. Recently, the On-To-Knowledge methodology has also been proposed for ontology building (Corcho et al., 2003).

Among these developers, we adopt Gruninger and Fox's method to build a mobile malware ontology. The goal of the TOVE (TOronto Virtual Enterprise) Enterprise Modeling project is to create the next generation Enterprise Model, a Common Sense Enterprise Model. By common sense we mean that an Enterprise Model has the ability to deduce answers to queries that require relatively shallow knowledge of the domain. A second generation knowledge engineering approach is adapted to construct our Common Sense Enterprise Model. An ontology is a formal description of entities and their properties, relationships, constraints, behaviors.

The approach to engineering ontologies begins with using some problems to define an ontology's requirements in the form of questions that an ontology must be able to answer. These requirements are called the competency of the ontology, including its objects, attributes, and relations. Next, we specify the definitions and constraints on the terminology, where possible. Lastly, we test the competency of the ontology by proving completeness theorems with respect to the competency.

The method consists of six major activities, which are motivating scenario, informal competency, first-order logic: terminology, completeness theorems, first-order logic: axioms and formal competency questions. We use a top-down strategy for identifying the main concepts in the ontology.

3.2 Ontology Tools.

A number of environments and tools for building ontology have grown exponentially. These tools are aimed at providing support for the ontology development process and for the subsequent ontology usage. Among these, Protégé 4.0 is the latest tool in an established line of tools developed at Stanford University for knowledge acquisition. Protégé 4.0 has thousands of users all over the world who use the system for projects ranging from modeling cancer-protocol guidelines to modeling nuclear-power stations. It helps knowledge engineers and domain experts to perform knowledge management tasks.

4 Ontology Knowledge Representation for mobile malware

In this section, we will adopt ontology to represent the behavioral patterns of mobile malware, where TOVE (TOronto Virtual Enterprise) Enterprise Modeling method proposed by Gruninger and Fox (Gruninger and Fox, 1995) is adopted and the process of ontology construction is described.

4.1 Data description

Since the arrival of the first mobile malware Cabir in June 2004, mobile malware have been advancing steadily beyond their proof of concept probes and onwards to new goals. By July 2006 the mobile malware count has exceeded the three hundred mark and continues to rise in 2007. By analyzing the behaviors of 35 kinds of major mobile malware described by various anti-malware firms, we categorize the types of malware on mobile phones in Table 3. There were no duplicate mobile malware in our data set, and commercial malware scanner confirms every mobile malware in the set. A full description of these behavior features can be found in (Shih et al., 2008). The behavioral description of mobile malware' ontology involves many attributes, and analytical characterization was performed in the malware. Finally, we extract a set of features to compose a feature vector from the mobile malware' behaviors, as shown in Table 4. The entire mobile malware was discovered from 2000 to 2007 and investigated in F-secure security website.

Table 3. Samples of mobile malware

Type	Target OS	Name
Trojan	Symbian	Appdisabler.J，Blankfont.A，Bootton.A，Cardblock.A，Cardtrap.A，Cdropper.A，CommDropper.A，Doomboot.A，Flerprox.A，Fontal.A，Gavno.A，Locknut.A，MGDropper.A，Mosquitos，Pbstealer.A，RommWar.A，Romride.A，Skudoo.A，Sendtool.A，SDropper.A，StealWar.A，Skulls.A，Singlejump.A
	Java	RedBrowser
Trojan-spy	Symbian	FlexiSpy.A
Worm	Symbian	Cabir.A，Commwarrior.A，Lasco.A
	Symbian, VBS	Eliles.A
Virus	Windows	Duts
	Windows (MSIL)	Cxover.A
Spyware	Symbian	Acallno.A，Mopofeli.A

Table 4. Extracted feature from mobile malware behaviors

	Feature	Content
x_1	Attachment file	Include pictures, jokes and execute files etc.
x_2	Embedded URL	ActiveX controls URL
x_3	Embedded Script	JavaScript and VBScript
x_4	Download files	Download danger files
x_5	Install application software	Install danger software, ex. games, screensavers
x_6	Execute file type	exe, vbs, scr, pif, bat, chm, com…
x_7	Varying file extension	The extension of file is varying and questionable

4.2 Ontology Building

The capability of ontology can represent the knowledge and relationship of the specific domain. To find out the dynamic malicious patterns, we build ontology to represent the behaviors of mobile malware. We are based on the steps and strategies of the TOVE Enterprise Modeling method (Gruninger and Fox, 1995) to build the ontology of mobile malware behavior as follows.

Motivating scenario. In recent years, due to the advantage of smart phone that is becoming more popular. However, the number of malware targeting mobile phones soared from one to more than 300, in past three years. Mobile malware may result in loss of confidential information, excess services fees, and battery draining. Since the knowledge presentation capability of ontology, this paper aims to explore the various behavioral characters and construct an ontology of mobile malware. We find out the unalterable characteristics through analyzing.

Informal competency. We described the domain application and competency question of an ontology base on motivation scenario. In the future applications, ontology must be able to answer the questions which follow the principles of the design phase of several questions. Competency questions were shown as following:

CQ1: How to identify the type of mobile malware
CQ2: How to describe behaviors of the mobile malware
CQ3: How to identify the infection routes of mobile malware
CQ4: How to identify the attacks pattern of mobile malware
CQ5: How to identify the spreading ways of mobile malware
CQ6: How to identify the damage type of mobile malware

Terminology. In this step, we defined the terminology of mobile malwares' ontology. This study divided the behavior of mobile malwares into four hierarchies: infection routes, attack patterns, damage types, spreading ways.

Formal competency questions and axioms. These two steps are the application of the phrases for the terminology, and transfer informal competency questions to formal competency questions. However, when the phrases can not to represent the deeper relationships, axioms must be used to establish the norms. This study builds the ontology of mobile malware through behavior analysis. We describe informal competency question, solving strategies and design the axioms to infer, make ontology can be adapted in mobile malware detection.

Completeness theorems. The competency question is adapted to verify the soundness of ontology in final step. Protégé-4.0 is used to create ontology for mobile malware and make a technical judgment. Adopting those steps above, the mobile malware' ontology is shown in Fig. 2, with Protégé 4.0.

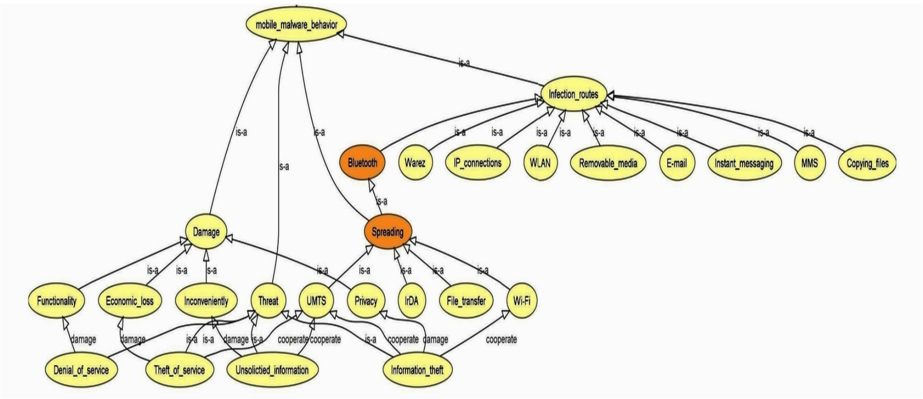


Fig. 2. The ontology of the mobile malware behaviors

Malware is consistently ranked as one of the most frequent security threats in organization, and malware prevention has become a major business. Therefore, understanding some aspects of protection are needed. Even with malware protection software, the best ways to protect our mobile phones from malware are to open executable files carefully, scan SMS and MMS before reading them and avoid opening suspicious attachments. Sometimes transfer data wirelessly seem to come from someone you know, but the person who sent the file may not even know it has been sent. In order to protect your mobile phones, users must know the things to do and the things cannot be done. It still has to emphasize on "prevention is better than cure". Users should practice some security measures in order to prevent themselves from being infected by malicious program.

We have developed a mobile malware behavioral ontology that describes many attributes, analytical characterization and relationships between these behaviors of mobile malware. By the capability of ontology knowledge management and presentation, a checklist of diagnoses, as shown in Table 5, can also be derived for organization and individuals use in the prevention of mobile malware. Note that, a new mobile malware may defeat this checklist by simply generating a rule that would opposite to the checklist rules in Table 5. Organizations should contact with provider and always keep a newly updated checklist in the long run.

Table 5. A end user's security checklist for his/her smart phone

Mobile malware checklist User: ___________ Date: ____________

* Check (∨) in the following checkboxes to ensure the security of smart phone.

□ Do not download any files from questionable web sites.
□ Do not install Warez or shareware, such as games or screensavers.
□ Do not install any suspicious application to your phone.
□ Do not open or copy any files attached to a memory card if the file name is questionable or unexpected.
□ Be absolutely sure of the origin of the application before accepting it.
□ Hide your visibility to all Bluetooth enabled phones.
□ Configure the pairing password of the Bluetooth device
□ If Bluetooth is not required, it should be turned off.
□ When receiving a SMS or MMS that is not include pictures, jokes, downloads, attachments, etc.

* Check (∨) in the following checkboxes for the suspicious SMS/MMS. More checks a SMS/MMS has, more dangerous it is.

□ The SMS/MMS from an unknown, suspicious or untrustworthy source.
□ The extension of attachment is double extension.
□ The extension of attachment is varying and questionable.
□ File extension of attachments are executable files such as .bat, .chm, .cmd, .com, .exe, .ocx, .pif, .scr, .shs, .vbe, .vbs, or .wsf etc.
□ Subject line is questionable or unexpected.
□ The source of sender is unknown, suspicious or untrustworthy.
□ The content of a SMS/MMS has URL.
□ The content of a SMS/MMS asks download of files.

* Check (∨) in the following checkboxes for the suspicious Bluetooth connection. More checks a Bluetooth connection has, more dangerous it is.

□ The Bluetooth connection from an unknown or untrustworthy source.
□ The Bluetooth connection asks files transfer.
□ The extension of files is varying and questionable
□ The extension of files is executable files.

Version X.X mm/dd/yy

5 Conclusion and Future Work

The growing popularity of mobile devices such as smart phones, handsets and PDAs has made mobile devices a more attractive target for mobile malware. In fact, hundreds of mobile malware and new variants have evolved in the past several years, which can quickly spread via non-traditional vectors such as SMS/MMS messaging, Bluetooth and traditional IP-based applications. Mobile security has been a very important issue for smart phone end users and organizations. However, the relevant researches are actually rare, especially in behavioral analysis of mobile malware.

This paper provides a new type method of behavior analysis for mobile malware. The method begins with extraction of key behavior signatures of mobile malware by applying ontology theory. As a result, end users and organizations must take even more precautions to guard against the introduction of mobile malware into their smart phones.

Currently, anti-malware software continues to play a central role in defending against mobile malware. The majority of detection software relies on up-to-date a malware signature database to detect malware. However, it is a challenge to distribute malware signatures files to mobile devices in a timely manner, and therefore limits the effectiveness of complex anti-malware solutions in battery-powered handsets. We have illustrated a construction of ontology architecture to manage the knowledge in relation to mobile malware. It is likely to be a useful approach to assist organizations in better understanding the interests of mobile malware. The result of our proposed method is very meaningful, and can be easily incorporated with a handset to assist the detection of mobile malware. In the future, we will develop a behavioral detection framework based on the ontology of mobile malware behavior to overcome the limitations of signature-based detection while addressing unique features and constraints of mobile handsets.

References

[1] A. Bernaras, I. Laresgoiti and J. Corera, “Building and reusing ontologies for electrical network applications”, *In Proceedings of the European Conference on Artificial Intelligence* (ECAI'96), pp.298-302, Budapest, Hungary, 1996.

[2] A. Bose and K. G. Shin, “On Mobile Viruses Exploiting Messaging and Bluetooth Services”, *In Proceedings of the 2th IEEE International Conference on Security and Privacy in Communication Networks*, pp.1-10, 2006.

[3] A. Bose, Xin Hu, K. G. Shin, and Tajoon Park, “Behavioral Detection of Malware on Mobile Handsets”, *In Proceeding of the 6th ACM international conference on Mobile systems, applications, and services*, Breckenridge, CO, USA, pp.225-238, 2008.

[4] J. Cheng, S. Wong, H. Yang, and S. Lu. “Smartsiren: virus detection and alert for smartphones”, *In Proceeding of the 5th ACM International conference on Mobile systems, applications, and services*, San Juan, Puerto Rico, pp.258-271, 2007.

[5] E. Chien, “Security reponses: Backdoor.Brador.A, SymbOS.Skulls and WinCE.Duts.A”, Symantec Corporation, 2004. Available online at http://www.symantec.com, 2009.

[6] M. Christodorescu, S. Jha, S.A. Seshia, D. Song and R.E. Bryant. “Semantics-aware malware detection”. *In Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, California, pp.32-46, May 2005.

[7] Cisco, “Cisco network admission control”, 2003. Available: http://www.cisco.com, 2009.

[8] O. Corcho, M. Fernández-López, and A. Gómez-Pérez, "Methodologies, tools and languages for building ontologies: Where is their meeting point?", *Data Knowledge Engineering*, Vol.46 No.1, pp.41-64, 2003.

[9] Shane Coursen. “The future of mobile malware”, *Network Security*, Vol.2007, Issue 8, pp.7-11, August 2007.

[10] K. A. Dahlgren, “Linguistic ontology”, *International Journal of Human-Computer Studies* Vol.43, pp. 809-818, 1995.

[11] D. R. Ellis, J. G. Aiken, K. S. Attwood, and S. D. Tenaglia, “A behavioral approach to worm detection”. *In Proceedings of the 2004 ACM Workshop on Rapid Malcode (WORM),* pp.43-53, 2004.

[12] P. Ferrie, P. Szor, R. Stanev, and R. Mouritzen, “Security responses: Symbos.cabir”, Symantec Corporation, 2004. Available online at http://www.symantec.com/security_response/writeup.jsp?docid=2004-061419-4412-99, 2009.

[13] J. Flinn and M. Satyanarayanan, “Powerscope: A tool for profiling the energy usage of mobile applications”, *In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications*, pp.1-9, New Orleans, Louisiana, Feb. 1999.

[14] A. Gostev, “Mobile Malware Evolution: An Overview”, Kaspersky Lab’s Report on Mobile Viruses, 2006. Available: http://www.viruslist.com/en/analysis?pubid=200119916, 2009.

[15] M. Gruninger and M.S. Fox, "Methodology for the design and evaluation of ontologies", In *Proceedings of the Workshop on Basic Ontological Issues in Knowledge Sharing*, pp.1-10, Montreal, April 1995.

[16] Z. Kedad and E. Metais, “Dealing with Semantic Heterogeneity during Data Integration,” *In Proceedings of 18th International Conference Conceptual Modeling*, pp.325-339, Nov. 1999.

[17] S. A. Khayam and H. Radha, “A topologically-aware worm propagation model for wireless senor networks”, *In Proceedings of 25th IEEE International Conference Distributed Computing Systems Workshops*, pp.210-216, June 2005.

[18] H. Kim, J. Smith, and K. G. Shin, “Detecting Energy-Greedy Anomalies and Mobile Malware Variants”, *In Proceedings of the 6th ACM International Conference on Mobile Systems, Applications, and Services*, pp.239-252, 2008.

[19] G. Lawton, “Is it finally time to worry about mobile malware?”, *Computer*, Vol.41, No.5, pp.12-14, 2008.

[20] D. B. Lenat, “CYC: a large-scale investment in knowledge infrastructure", *Communications of the ACM*, Vol.38, No.11, pp.33-38, 1995.

[21] D. B. Lenat and R.V. Guha, *Building Large Knowledge-Based Systems: Representation and Inference in the Cyc Project*, Addison-Wesley Pub, Boston, Jan. 1990.

[22] J. W. Mickens and B. D. Noble, “Modeling epidemic spreading in mobile environments”, *In Proceedings of the 4th ACM Workshop on Wireless Security*, pp.77-86, Sep. 2005.

[23] J. A. Morales, P. J. Clarke, Y. Deng, and B. M. Golam Kibria, “Testing and evaluating virus detectors for handheld devices”, *Journal in Computer Virology*, Vol.2, No.2, pp.135-147, 2006

[24] Prot´eg´e 4.0, Available online at http://protege.stanford.edu/, 2009

[25] E. V. Ruitenbeek, T. Courtney, W. H. Sanders, and F. Stevens, “Quantifying the effectiveness of mobile phone virus response mechanisms”. *In Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pp.790-800. June 2007.

[26] D. H. Shih, B. Lin, H. S. Chiang and M. H. Shih, “Security aspects of mobile phone virus: A critical survey”, *Industrial Management and Data Systems*, Vol.108, No.4, pp.478-494, 2008.

[27] A. Schmidt, F. Peters, F. Lamour, C. Scheel, S. A. Camtepe and S. Albayrak, “Monitoring Smartphones for Anomaly Detection”, *In International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, Insbruck, Austria, page 40, 2008.

[28] P. Taejoon and K. G. Shin, “Soft tamper-proofing via program integrity verification in wireless sensor netwoeks”, *IEEE Transactions on Mobile Computing*, Vol.4 No.3 pp.297-309, 2005.

[29] Trend Micro, “Network viruswall outbreak prevention appliance”, 2004. Available online at http://www.trendmicro.com, 2009.

[30] K. Wang, G. Cretu, and S. J. Stolfo. “Anomalous payload-based worm detection and signature generation”, *In Proceedings of the 8th International Symposium of Recent Advances in Intrusion Detection (RAID 2005)*, pp.227-246, Sep. 2005

[31] Yury, “Mobile threats – myth or reality?”, Kaspersky Lab’s Report on Mobile Viruses. Nov. 2006. Available online at http://www.viruslist.com/en/weblog?weblogid=204924390 , 2009.

[32] H. Zheng, D. Li, and Z. Gao, “An epidemic model of mobile phone virus”, *In Proceedings of the 2006 1st International Symposium on Pervasive Computing and Applications*, pp.1-5, 2006.