ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Encounter-Based Distributed System Based on Metropolis Sampler to Detect Malware and to Minimize the Number of Infected Nodes

Md.Basheer
M.Tech Student,
Computer Science Engineering,
Nawab Shah Alam Khan College of Engineering
Technology, Malakpet, Hyderabad,Telangana, India.

Mr.Mohammed Ayaz Uddin, M.Tech
Associate Professor,
Department of CSE,
Nawab Shah Alam Khan College of Engineering
Technology, Malakpet, Hyderabad, Telangana, India.

Abstract:

Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. Mobile malware is software created to infect or gain access to mobile devices such as cell phones, tablets, and PDAs. All smartphones, as computers, are preferred targets of attacks. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps. In this paper we examine and implement a Signature allocation based security system to minimize the infected nodes & detection of malware and restricting its further propagation. Through theoretical analysis and simulations with both synthetic and realistic mobility traces, we show that the distributed algorithm achieves the optimal solution, and performs efficiently in realistic environments.

Keywords:

Malware, Infected Nodes, Distributed algorithm, Smart Phones, Mobile Internet.

Introduction:

Mobile malware was initially considered to be a hoax until it became obvious that malicious software existed and functioned on mobile devices. The earliest recorded mobile malware was called Cabir. It was released in 2004 and was designed to infect Symbian OS platforms via a Bluetooth connection. It was essentially harmless, but nonetheless proved to the public that worms could be found on mobile devices. Since mobile devices usually contain private and valuable information, mobile malware has recently began moving toward having a specific purpose (usually exploiting information) as opposed to viruses created solely for bragging rights.

Attack Types:

Bluetooth:

Attacks via Bluetooth have the ability to infect any phone with Bluetooth capabilities and can even exploit feature phones. These proximity-based attacks use the local Bluetooth network, usually in a crowded area, to send unwarranted requests to phones. Since Bluetooth can be used to transmit files, malicious executables can be sent across the network to everybody that accepts the request and installs the software. Some of these attacks, such as the Cabir, are worms which send out the request from an infected phone without the user knowing, thus quickly spreading it from phone to phone. Protection from these attacks is simple - cell phone users should not leave Bluetooth on, and it if is left on, users should not accept requests from unknown connections.

Application Marketplace:

Malicious software can be installed via application marketplaces. For example, according to webroot.com, applications disguised as Angry Birds level unlockers were available in the Android Market. Once installed, the creator had access to precious information such as browsing history, bookmarks, etc. The application also contacted a remote server that gave the phone instructions for downloading additional malware.To protect against this kind of attack, users can judge the legitimacy of the application with a few simple guidelines. Applications that require a lot of permissions for no apparent reason should be avoided. Also, the credibility of a publisher can easily be researched if the user is unsure.

WiFi:

Information can be stolen from devices when they are connected to public WiFi hotspots. Users should not do banking, shopping, or other tasks that expose personal information while connected to unsecured networks. This is not an issue unique to mobile devices, but because of the nature of mobile devices, they are more likely to be used in public places on these networks.

SMS:

SMS attacks are generally similar to each other. Malicious software is installed on the phone by some means which continually sends unnoticed text messages from the user's phone to premium numbers which creates charges on the user's account. According to Kaspersky Labs, the SMS-Trojan was first discovered for the Android operating system in early 2011. The news report says,"The Trojan-SMS category is currently the most widespread class of malware for mobile phones, but Trojan-SMS.

AndroidOS.Fake Player.a is the first to specifically target the Android platform." To protect against these attacks, users should be cautious of what applications are installed on their devices and who the creators of the applications are.SMS attacks can also simply be spam messages with links to malicious sites. The problem with this type of attack is that it must target specific phones in order to execute scripts that are compatible.

QR Codes:

Because QR Codes are completely obfuscated by nature, they provide the means of taking curious smartphone users to malicious web sites. There are three ways QR codes can be maliciously presented to a user.The first method is placing a QR code by itself with no explanation or context, causing some people to get curious and scan it. The second way of getting people to scan the code is to place a stamp or sticker over an existing one so that it is disguised as a harmless QR code. The third way of presenting malicious codes to the public would be digitally through email.

There are three prime targets for attackers:

Data: smartphones are devices for data management, therefore they may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs);

Identity:

smartphones are highly customizable, so the device or its contents are associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile phone contract, and an attacker may want to steal the identity of the owner of a smartphone to commit other offenses;

Availability:

by attacking a smartphone one can limit access to it and deprive the owner of the service.

The source of these attacks are the same actors found in the non-mobile computing space:

Professionals, whether commercial or military, who focus on the three targets mentioned above. They steal sensitive data from the general public, as well as undertake industrial espionage. They will also use the identity of those attacked to achieve other attacks;Thieves who want to gain income through data or identities they have stolen. The thieves will attack many people to increase their potential income; Black hat hackers who specifically attack availability. Their goal is to develop viruses, and cause damage to the device. In some cases, hackers have an interest in stealing data on devices.Grey hat hackers who reveal vulnerabilities. Their goal is to expose vulnerabilities of the device. Grey hat hackers do not intend on damaging the device or stealing data.

Consequences:
When a smartphone is infected by an attacker, the attacker can attempt several things:

The attacker can manipulate the smartphone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) via sms or email;The attacker can easily force the smartphone to make phone calls. For example, one can use the API (library that contains the basic functions not present in the smartphone) PhoneMakeCall by Microsoft, which collects telephone numbers from any source such as yellow pages, and then call them.[8] But the attacker can also use this method to call paid services, resulting in a charge to the owner of the smartphone.

It is also very dangerous because the smartphone could call emergency services and thus disrupt those services;A compromised smartphone can record conversations between the user and others and send them to a third party. This can cause user privacy and industrial security problems;An attacker can also steal a user's identity, usurp their identity (with a copy of the user's sim card or even the telephone itself), and thus impersonate the owner. This raises security concerns in countries where smartphones can be used to place orders, view bank accounts or are used as an identity card; The attacker can reduce the utility of the smartphone, by discharging the battery.

For example, they can launch an application that will run continuously on the smartphone processor, requiring a lot of energy and draining the battery. One factor that distinguishes mobile computing from traditional desktop PCs is their limited performance. Frank Stajano and Ross Anderson first described this form of attack, calling it an attack of "battery exhaustion" or "sleep deprivation torture"; The attacker can prevent the operation and/or starting of the smartphone by making it unusable. This attack can either delete the boot scripts, resulting in a phone without a functioning OS, or modify certain files to make it unusable (e.g. a script that launches at startup that forces the smartphone to restart) or even embed a startup application that would empty the battery;The attacker can remove the personal (photos, music, videos, etc.) or professional data (contacts, calendars, notes) of the user.

Existing System:

The target landscape for malware attacks (i.e., viruses, spam bots, worms, and other malicious software) has moved considerably from the large-scale Internet to the growingly popular mobile networks with a total count of more than 350 known mobile malware instances reported in early 2007.This is mainly because of two reasons. One is the emergence of powerful mobile devices, such as the iPhone, Android, and Blackberry devices, and increasingly diversified mobile applications, such as multimedia messaging service (MMS), mobile games, and peer -to- peer file sharing. The other reason is the emergence of mobile Internet, which indirectly induces the malware. Malware residing in the wired Internet can now use mobile devices and networks to propagate. Currently, mobile malware can propagate through two different dominant approaches.

Via MMS, a malware may send a copy of itself to all devices whose numbers are found in the address book of the infected handset. This kind of malware propagates in the social graph formed by the address books, and can spread very quickly without geographical limitations. The other approach is to use the short-range wireless media such as Bluetooth to infect the devices in proximity as "proximity malware."

De Merits of Existing System:

•Increasingly diversified mobile applications, such as multimedia messaging service (MMS), mobile games, and peer -to- peer file sharing.

•The emergence of mobile Internet, which indirectly induces the malware.

•Malware residing in the wired Internet can now use mobile devices and networks to propagate.

Proposed System:

We introduce an optimal distributed solution to efficiently avoid malware spreading and to help infected nodes to recover. Consider a mobile network where a portion of the nodes are infected by malware. Our research problem is to deploy an efficient defense system to help infected nodes to recover and prevent healthy nodes from further infection. Typically, we should disseminate the contentbased signatures of known malware to as many nodes as possible consequently, distributing these signatures into the whole network while avoiding unnecessary redundancy is our optimization goal. However, to address the above problem in the realistic mobile environment is challenging for several reasons.

First, typically we cannot rely on centralized algorithms to distribute the signatures because the service infrastructure is not always available. Therefore, a sensible way for signature distribution is to use a distributed and cooperative way among users. We propose an optimal signature distribution scheme by considering the following realistic modeling assumptions: 1) the network contains heterogeneous devices as nodes, 2) different types of malware can only infect the targeted systems, and 3) the storage resource of each device for the defense system is limited.

System Architecture:

The overview of our proposed DoS attack detection system architecture is given in the below, the deployment is performed as per the requirement of Hardware and software specified in the requirements phase.

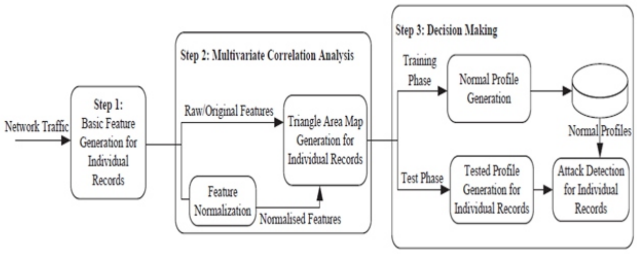
Network Traffic
Step 1: Basic Feature Generation for Individual Records
Step 2: Multivariate Correlation Analysis
Raw/Original Features
Triangle Area Map Generation for Individual Records
Feature Normalization
Normalised Features
Step 3: Decision Making
Training Phase
Normal Profile Generation
Normal Profiles
Test Phase
Tested Profile Generation for Individual Records
Attack Detection for Individual Records

Fig System Architecture

Block Diagram:

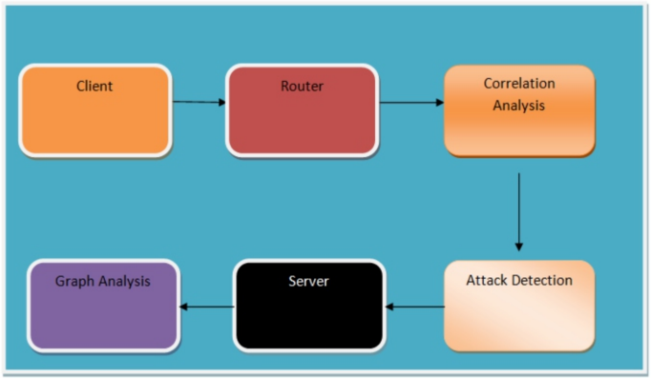

Fig Block Diagram

MODULES:

The project consists of four models they are as follows
1.Malware Signature Finder and Spreading Module
2.Problem Formulation and Centralized Algorithm
3.The Metropolis Sampler
4.Performance Evaluation

Modules Description:

1.Malware Signature Finder and Spreading Module:

In this module, malware signature will be analyzed and distributed over connected node. We consider a system of N heterogeneous wireless nodes belonging to K types (e.g., type of OS), which can be infected by K types of malware, denoted by set IK.

In the defense system, we assume that there are S helpers, denoted by set SS, storing the signatures to help other nodes with detecting the malware.

2.Problem Formulation and Centralized Algorithm:

Based on the malware spreading model, we first formulate the problem, and then give a greedy algorithm to achieve the optimal signature distribution. Now, we validate the proposed malware spreading model expressed, which is based on the epidemic model for malware spreading and the fluid model in DTN. Since our model characterizes the fraction of the malware infected nodes, we simulate the malware spreading, and compare the simulation results of infected ratio with that obtained by the model. As we have claimed that this model characterizes the MMS and proximity malware spreading, we validate the malware spreading in both the proximity and MMS scenarios.

3.The Metropolis Sampler:

In this module we develop the distributed algorithm for the signature distribution problem. The designed algorithm is based on a simulated annealing technique called Metropolis sampler. In the following sections, we first describe the basic notions and the framework of Metropolis sampler, then design the distributed algorithm based on simulated annealing with the Metropolis sampler, and finally prove that the proposed algorithm converges to the optimal performance.

4.Performance Evaluation:

We present numerical results with the goal of demonstrating that our greedy algorithm for the signature distribution, denoted OPT, achieves the optimal solution and yields significant enhancement on the system welfare compared with prior heuristic algorithms. Related to the heuristic algorithms, we consider 1) Important First (IF), which uses as many helpers as possible to store the signature of the most popular malware, 2) Uniform Random (UR), where each helper randomly selects the target signatures to store, and 3) Proportional Allocation (PA), which is a heuristic policy that assigns signatures with the uniform distribution proportional to the market sharing and the weights of different malware.

Merits of Proposed System:

•Our formulated model is suitable for both the MMS and proximity malware propagation.

•A distributed algorithm that closely approaches the optimal system performance of a centralized solution.

•The efficiency of our defense scheme in reducing the amount of infected nodes in the system.

Conclusion: As smartphones are a permanent point of access to the internet (mostly on), they can be compromised as easily as computers with malware. A malware is a computer program that aims to harm the system in which it resides.

A virus is malicious software designed to spread to other computers by inserting itself into legitimate programs and running programs in parallel. The technical challenges are that mobile devices are heterogeneous in terms of operating systems, the malware infects the targeted system in any opportunistic fashion via local and global connectivity, while the to-be-deployed defense system on the other hand would be usually resource limited.

In this paper we examine and implement a Signature allocation based security system to minimize the infected nodes & detection of malware and restricting its further propagation. The system provides optimal signature distribution to defend mobile networks against the propagation of both proximity and MMS-based malware. The proposed system offers protection against both MMS based attack and Bluetooth based attack at the same time.

References:

[1] Ong Li, Member, IEEE, Pan Hui, Member, IEEE, Depeng Jin, Member, IEEE, Li Su, and Lieguang Zeng, Member, IEEE. ”Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices”. IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 2, FEBRUARY 2014.

[2] Bishop, Matt (2004). Introduction to Computer Security. Addison Wesley Professional. ISBN 978-0-321-24744-5.

[3] Dunham, Ken; Abu Nimeh, Saeed; Becher, Michael (2008). Mobile Malware Attack and Defense. Syngress Media. ISBN 978-1-59749-298-0.

[4] Rogers, David (2013). Mobile Security: A Guide for Users. Copper Horse Solutions Limited. ISBN 978-1-291-53309-5.

[5] J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara, and A. Goel, “A Preliminary Investigation of Worm Infections in a Bluetooth Environment,” Proc. Fourth ACM Workshop Recurring Malcode (WORM), 2006.

[6] S. Cheng, W. Ao, P. Chen, and K. Chen, “On Modeling Malware Propagation in Generalized Social Networks,” IEEE Comm. Letters, vol. 15, no. 1, pp. 25-27, Jan. 2011.

[7] C. Kolbitsch, P. Comparetti, C. Kruegel, E. Kirda, X. Zhou, and X.Wang, “Effective and Efficient Malware Detection at the End Host,” Proc. 18th Conf. USENIX Security Symp., 2009.

[8] F. Li, Y. Yang, and J. Wu, “CPMC: (2010).An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks,” Proc. IEEE INFOCOM.

[9] R. Villamarı´n-Salomo´n and J. Brustoloni,(2013) “Bayesian Bot Detection Based on DNS Traffic Similarity,” Proc. ACMymp. Applied Computing (SAC).

[10] Y. Li, P. Hui, L. Su, D. Jin, and L. Zeng,(2011) “An Optimal Distributed Malware Defense System for Mobile Networks with Heterogeneous Devices,” Proc. IEEE Eighth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON).