International Journal of Future Innovative Science and Engineering Research
Volume-1, Issue-I ISSN (Online): 2454- 1966

Research Manuscript Title

SHIELDING MOBILE NETWORKS FROM MALWARE WITH MISCELLANEOUS DEVICES

Website: www.istpublications.com

M Hepsy[1], A MahabubBasha[2] ,U.NilabarNisha[3]

[1]M.Tech Student, Department of IT,

Jayam college of engineering and technology, Dharmapuri.

[2]Senior Professor, Department of ECE, K.S.R engineering college, Tiruchengode.

[3]Assistant Professor, Department of IT, Jayam college of engineering and technology, Dharmapuri.

E mail: hepsy05@gmail.com1, mahabubbasha1952@yahoo.com2 ,u.nishaofficial@gmailcom

MARCH – 2015

M Hepsy, A MahabubBasha, U.NilabarNisha, "Shielding Mobile Networks From Malware With Miscellaneous Devices", International Journal of Future Innovative Science and Engineering Research, Volume-1, Issue-I , Pages: 36

SHIELDING MOBILE NETWORKS FROM MALWARE WITH MISCELLANEOUS DEVICES

M Hepsy[1], A MahabubBasha[2] ,U.NilabarNisha[3]

[1]M.Tech Student, Department of IT,

Jayam college of engineering and technology, Dharmapuri.

[2]Senior Professor, Department of ECE, K.S.R engineering college, Tiruchengode.

[3]Assistant Professor, Department of IT, Jayam college of engineering and technology, Dharmapuri.

E mail: hepsy05@gmail.com1, mahabubbasha1952@yahoo.com2 ,u.nishaofficial@gmailcom

ABSTRACT

Smart phones are envisaged providing applications and services and it also becoming the quarry of malware. From the ingredient of malware, since some enlightened malware that can diversion the signature discernment would appear with the blooming of the shielding system, new shielding mechanisms will be required. In this project, first I formulate the optimal signature scattering with the consideration of the diversity of mobile devices and malware. I proposed distributed algorithm to spread the malware signatures and to efficiently avoid malware dissemination and to help contaminated nodes to regain and designing a defense system for both MMS and proximity malware. I proposed MD5 algorithm to verify the data integrity.

***Index terms: mobile malware, distributed algorithm, disparate mobile networks*.**

I. INTRODUCTION

The mobile malware discovered so far have exploited vulnerabilities in Bluetooth to infect a proximity device and then exploits SMS to spread itself to other devices in the mobile network. New type of network that provides an application always becomes the main quarry of new malware. Mobile malware because of transpire of powerful devices, such as Android, blackberry devices and mobile applications such as MMS(multimedia messaging service), peer-to-peer file sharing , mobile games, mobile commerce and the emergence of mobile internet. Mobile data communication has become a very important and promptly evolving technology as it allows users to transmit data from remote locations to other remote locations. This is the biggest problem of business people on the mobility. Mobile computing can use cell phone connections to make phone calls as well as connecting to the internet. Malware residing in the wired internet can now utilize mobile devices and network to propagate. Malware has become the major restriction in the development of networks. The possible effects of malware propagation on consumers and mobile phone providers are severe. A Malware attack has moved notably from the internet to the popular mobile networks.

Mobile malware can spread through two different powerful approaches. First, a MMS virus can send a copy of itself to all mobile phones whose numbers are found in the contaminate phone address book. This virus can spread rapidly without geographical restriction. Second an Bluetooth virus can infect the devices in proximity.Bluetooth malware propagates slowly because of the human mobility. Comm warrior, cabir are belonging to the proximity malware. These worms

continue to exist in the network and remain undetected because of the decentralized contamination. The three strategies for detecting and alleviation Bluetooth malware are local detection, uses local evidence to detect the malware and prevent further dissemination by the devices. Disabling the malware protects extent propagation but makes no strive to advice other devices or the network about the presence of malware.

In Bluetooth signature dissemination, each device sustain a table S of signature of malware files. Device X computes a content based signature S. when X contact with another device Y. X spread the signature s to Y. If Y is contaminated instantly disables the malware. Y then adds S to its signature table S. whenever another device shares a file with. Y will check the file against the signature in S.

In broadcast signature dissemination, network provider to spread signature using a broadcast mechanism. When the server receives m alerts from distinctive devices for a particular malware occurrence, it broadcasts a induced signature to the entire mobile network. This signature instantly cures all contaminated devices. These three strategies are suitable only for Bluetooth malware. For detecting and alleviation proximity malware, community based proximity malware coping scheme by utilizing the community structure reflecting a stable and controllable granularity of security. These works quarry the Bluetooth malware. In this project, I address the difficult task of designing a protection system for both Bluetooth virus and MMS. I proposed a distributed algorithm to efficiently avoid malware propagate and to help contaminated nodes to recover.

An efficient shielding system is to help contaminated nodes to regain and protect healthy nodes from extent contamination. The signature should disseminate of known malware to many node. The unnecessary sacking is avoided in the network using the signature distributing technique. We cannot distribute the signatures because the service infrastructure is not always available. Therefore a practical way for signature distribution is to use a distributed algorithm.

We propose the optimal signature for the following basics

1) The network contains diverse devices as nodes.
2) Different types of malware can only infect the targeted systems.
3) The storage resource of each device for the defense system is limited.

II. EXISTING SYSTEM

Malware disseminate by MMS/SMS to stop the propagation the counter mechanism is used. This mechanism only quarry the MMS spreading malware Proximity malware propagation intrinsic depend upon the traces of mobile user contacts. Develop a simulation and analytic model for Bluetooth worms, and show that mobility has a significant impact on the propagation dynamics. Detects of mobile user contacts reflect actual behavior but difficult to use a particular set of facts and only capture a subset of all contacts due to lack of geographic coverage. One limitation with user traces is that it is difficult to cover an entire geographic area with sensors. Synthetic models are tensile and provide the necessary geographic coverage, but lack the full authenticity of user mobility traces. MMS spreading malware use a feasible social network model to obtain the social

graph to model the address books in the phone, which exploited by the malware to propagate. Epidemic model applied to malware propagation on the internet. The deterministic epidemic models represent the dynamics of malware spreading. It is based on homogeneous. Homogeneous are not good approximation for encounters of mobile devices.

Disadvantages

Distribute the signatures cannot centralize algorithms because the service infrastructure is not always available. Signature flooding costs too much and the local view of each node constrains the global optimal solution. Design of defense system not to efficiently detect malware and could not optimally distribute the signatures. It has unable to diffuse the encountered malware.

III. PROPOSED SYSTEM

We propose an efficient shielding system to protect contamination nodes to regain. Signature distributions help to detect the equivalent malware and disable extent propagation.

I proposed Message digest algorithm to encounter and diffuse the detected malware and proposed distributed algorithm to reduce the number of contaminated nodes. The synthetic and reality trace is fixed so it cannot prove the scalability. So I exploit MAP trace, where the number of nodes in a system can be flexibly set. The MD5 message digest algorithm is a widely used cryptographic hash function producing a 128 bit hash value. It is used to verify data integrity through the creation of a 128 bit message digest from data input that is claimed to be as unique to that specific data.

Distributed algorithm is successfully coordinating the behavior of the independent parts of the algorithm in the face of processor failures and unreliable communications links. It is efficiently avoid malware propagation. Security and authentication mechanisms should consider.

Advantages

Efficient shielding system is to help the contaminated nodes to regain. The unnecessary sacking data is avoided in the network using the signature technique. It is used to be as unique to that specific data and diffuse the attacks. The efficiency of our shielding system is to reducing the contaminated nodes in the system.

IV. DESIGN OVERVIEW

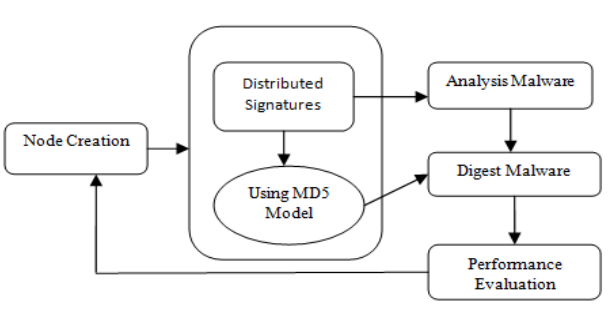

Fig. 1. Mobile Malware Detection

First we create a node after creating a node we create a helpers node. Helper node is used to distribute the signature to network. The distribute signature analysis the malware. MD5 is used to verify the data integrity and provide a security. Performance evaluation and modeling of mobile malware spreading using the Delay Tolerant network model. The distribute algorithm is used to minimize the contamination nodes to regain.

V. SYSTEM MODULES

A. Node Creation

Create mobile networks including a number of nodes. First we defined the number of nodes and also defined source node, destination node and intermediate nodes. The network contains divergent devices as nodes. Mobile nodes are more efficient to disseminate content and information in the network

B. Helper Node Creation

Helper nodes are referred to as special nodes. This node is used to focusing the all nodes. Helper node is intermediate node for every node in the network. File can be transmitting from source node to destination node through the help of helpers of node. At the same time special node of a helper node generate the signature.

C. Distribute Signature

Distributed signature is used to analyzing the malware nodes through passing the signature. All intermediate nodes received a signatures .This signature distributed for every intermediate node from source node to destination node with the help of the special node.

D. Malware Detection and Encounter Malwares

Detect the malware with the help of a signature. Exponential parameter obtained from the contact records between helpers and general nodes. Apply delay tolerant network technique to identify the malware nodes in the mobile networks. This is to detecting the malware spreading nodes and recovering the contaminated nodes.

E. Performance Trace

Imitate the malware spreading and compare the simulation results of infected ratio. The number of contaminated nodes increases with the growth of spreading rate can observe that the number of contaminated nodes decreases with the increase of regaining rate. MAP trace technique is used to detect the spreading of Bluetooth malware for showing simulations. So determining of the malware spreading time and malware regaining time is reduced.

VI. CONCLUSION

The efficiency of our shielding system is to reducing the amount of contaminated node. Our model quarry MMS and proximity malware at the same time. Our distributed algorithm minimizes the infected nodes and provides a complete solution. The malware nodes inject imitation signatures preying no malware in to the network and persuade denial of service attacks to the defense attacks. Therefore message digest algorithm used for security and data integrity. The proposed signature propagation attains good performance of averting malware propagation under the real world environment.

Our prey is to minimize the malware infected nodes in the network. Distributed algorithm to solve a given problem depends on both the characteristics of the problem. Cross OS malware will transpire and spread.

REFERENCES

[1] Altman.E, Neglia .G,DePellegrini.F, and Miorandi.D, "Decentralized Stochastic Control of Delay Tolerant Networks,"Proc. IEEE INFOCOM, 2009.

[2] Bremaud.P Markov Chains: Gibbs Fields, Monte Carlo Simulation, and Queues. Springer Verlag, 1999.

[3] Hypponen.M, "Mobile Malware," Proc. 16th USENIX Security Symp. 2007.

[4] Hui.p, Crowcroft.J, and Yoneki.E, "Bubble Rap: Social-Based Forwarding in Delay Tolerant Networks," Proc. ACM MobiHoc, 2008.

[5] Grossglauser.M and Tse.D, "Mobility Increases The Capacity of Ad-Hoc Wireless Networks," Proc. IEEE INFOCOM, pp. 1360- 1369, 2001

[6] Khouzani.M,, Sarkar.S, and Altman.E, "Maximum Damage Malware Attack in Mobile Wireless Networks," Proc. IEEE INFOCOM, 2010.390 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 2, FEBRUARY 2014.

[7] Keranen.A, Ott.J, and Karkkainen.T, "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques, pp. 1-10, 2009.

[8] Lawton.G, "On the Trail of the Conficker Worm," Computer, vol. 42, no. 6, pp. 19-22, June 2009.

[9] Li.F, Yang.Y, and Wu.J, "CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-Based Mobile Networks," Proc. IEEE INFOCOM, 2009.

[10] May.R and Lloyd.A, "Infection Dynamics on Scale-Free Networks," Physical Rev. E, vol. 64, no. 6, p. 066112, 2001.