RESEARCH PAPER | Computer Science | Volume : 6 | Issue : 1 | JANUARY 2016 | ISSN - 2249-555X

Defending Against the Malware by Means of Using Epidermic Methodology

KEYWORDS: Malware propagation, exponential distribution, global scale malware, malware datasheets

Ms.K.Prathipa	Mr.S.Prakadeswaran	Dr.T.Senthil Prakash
PG Scholar, Shree Venkateshwara Hi-Tech Engg College, Gobi, Tamilnadu , India	Assistant Professor, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, India.	Professor & Head, Shree Venkateshwara Hi-Tech Engineering College, Gobi, Tamil Nadu, India.

ABSTRACT *Malware is malicious software program deployed by cyber attackers to compromise computer systems by exploiting their security vulnerabilities. This method investigates how malware propagates in networks from a global perspective. These formulate the problem, and establish a rigorous two layer epidemic model for malware propagation from network to network. The analysis indicates that the distribution of a given malware follows exponential distribution, power law distribution with a short exponential tail, and power law distribution at its early, late and final stages, respectively. In the proposed method the distribution of a given malware at their ISP domains, where the conditions for the two layer model are analyzed. Extensive experiments have been performed through two real-world global scale malware data sets, and the results confirm our theoretical findings.*

INTRODUCTION

A rationally developed technology to store data from more than one client. Cloud computing is an environment that enables users to remotely store their data. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. It helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backups remotely to third party cloud storage providers rather than maintain data centers on their own. An individual or an organization may not require purchasing the needed storage devices. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. There are three objectives to be main issue

Confidentiality – preserving authorized restrictions on information access and disclosure. The main threat accomplished when storing the data with the cloud.

Integrity – guarding against improper information modification or destruction.

Availability – ensuring timely and reliable access to and use of information.

If he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem there are lot of techniques introduced to make secure transaction and secure storage. The encryption standards used for transmit the file securely. The assured deletion technique aims to provide cloud clients an option of reliably destroying their data backups upon requests. The encryption technique was implemented with set of key operations to maintain the secrecy.

LITERATURE SURVEY

This work mainly focuses on the Android platform and aim to systematize or characterize existing Android malware. Then characterize them from various aspects, including their installation methods, activation mechanisms as well as the nature of carried malicious payloads. The goals and contributions of this paper are threefold. First, we fulfill the need by presenting the first large collection of 1260 Android malware samples1 in 49 different malware families, which covers the majority of existing Android malware, ranging from their debut in August 2010 to recent ones in October 2011. The dataset is accumulated from more than one year effort in collecting related malware samples, including manual or automated crawling from a variety of Android Markets.

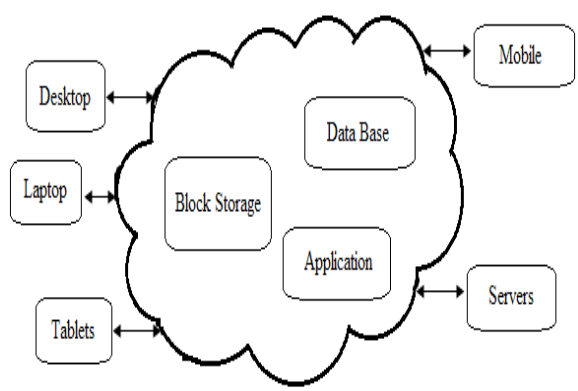


Figure 1: Data sharing with cloud storage

EPIDERMIC MODELS FOR COMPLEX NETWORKS:

Research on complex networks have demonstrated that the number of hosts of networks follows the power law. Peoplefound that the size distribution usually follows the powerlaw, such as population in cities in a country or personal income in a nation [2]. In terms of the Internet, researchershave also discovered many power law phenomenon, suchas the size distribution of web files [5]. Recent progressesreported in [26] further demonstrated that the size of networks follows the power law.The power law has two expression forms: the Pareto distributionand the Zipf distribution. For the same objects of the power law, we

Volume : 6 | Issue : 1 | JANUARY 2016 | ISSN - 2249-555X

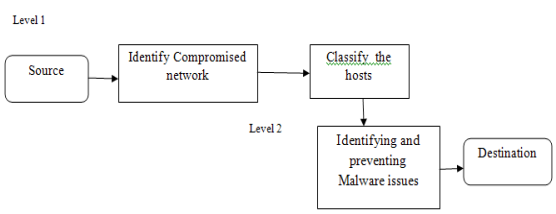
can use any one of them to represent it. However, the Zipf distributions are tidier than the expression of the Pareto distributions. In this paper, we will use Zipf distributions to represent the power law.

PROPOSED WORK:

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system. It differs from the flowchart as it shows the data flow instead of the control flow of the program. A data flow diagram can also be used for the visualization of data processing. The DFD is designed to show how a system is divided into smaller portions and to highlight the flow of data between those parts. The level 1 is descripted the server can check if the login user are valid or invalid user, the data about the user checked by the data base. If user is not valid the server cannot allow the user to process. If the user need to registration after completed the registration the user are valid to process. It will be continued in level 2.

CASE STUDY

This method proposes a two layer malware propagation model to describe the development of a given malware at the Internet level. Compared with the existing single layer epidemic models, the proposed model represents malware. Propagation better in large scale networks. It find the malware distribution in terms of networks varies from exponential to power law with a short exponential tail, and to power law distribution at its early, late, and final stage, respectively.



The defenders may care more about their own network, e.g., the distribution of a given malware at their ISP domains, where the conditions for the two layer model may not hold. These problems can be identified and solved in the network. This believes it is not a simple linear relationship in the multiple malware case compared to the single malware one. These findings are firstly theoretically proved based on the proposed model, and then confirmed by the experiments through the two large-scale real-world data sets.

Advantage

- It helps in protecting personal data of clients existing on network.
- This method facilitates protection of information that is shared between computers on the network.
- Hacking attempts or virus / spyware attacks from the internet will not be able to harm physical computers. External possible attacks are prevented.
- Private networks can be provided protection from external attacks by closing them off from internet. Network Security makes them safe from virus attacks, etc.

CONCLUSIONS

The distribution of multiple malware on large-scale networks is identified using two layer epidemic models using two layer approaches. The dynamics of the late stage is identified. It defines the transition point between the early stage and the late stage. The malware distribution for middle size networks such as ISP networks with many subnetworks is solved using this approach. The distribution of coexist multiple malware in networks. In reality, multiple malware may coexist at the same networks. Due to the fact that different malware focus on different vulnerabilities, the distributions of different malware should not be the same. Hence it can solve using the epidemic approach.

FUTURE ENHANCEMENT

In this paper, we thoroughly explore the problem of at large-scale networks. The solution to this problem is desperately desired by cyber defenders as the network security community does not yet have solid answers. Different from previous modelling methods, we propose a two layer epidemic model: the upper layerfocuses on networks of a large scale networks, for example, domains of the Internet; the lower layer focuses on the hosts of a given network. This two layer model improves the accuracy compared with the available single layer epidemic models in malware modelling. Moreover, the proposed two layer model offers us the distribution of malware in terms of the low layer networks.

REFERENCE [1] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: Analysis of a botnet takeover," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 635–647. [2] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "My botnet is bigger than yours (maybe, better than yours): Why size estimates remain challenging," in Proc. 1st Conf. 1st Workshop Hot Topics Understanding Botnets, 2007, p. 5. [3] D. Dagon, C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in Proc. 13th Netw. Distrib. Syst. Security Symp., 2006. [4] P. V. Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," IEEE/ACM Trans. Netw., vol. 17, no. 1, pp. 1–14, Feb. 2009. [5] Cabir. (2014). [Online]. Available: http://www.f-secure.com/en/ web/labs_global/2004-threat-summary [6] Ikee. (2014). [Online]. Available: http://www.f-secure.com/vdescs/worm_iphoneos_ikee_b.shtml