Volume 2, No. 04, June 2013 ISSN – 2278-1080

The International Journal of Computer Science & Applications (TIJCSA)

RESEARCH PAPER

Available Online at http://www.journalofcomputerscience.com/

A Survey on Various Security Threats and Classification of Malware Attacks, Vulnerabilities and Detection Techniques

Dr.(Mrs).G.Padmavathi
Professor and Head,
Department of Computer Science,
Avinashilingam Institute for Home Science and
Higher Education for Women, Coimbatore-641043.
Mail id:ganapathi.padmavathi@gmail.com

S.Divya
Research Scholar,
Department of Computer Science,
Avinashilingam Institute for Home Science and
Higher Education for Women, Coimbatore-641043.
Mail id:divya.vidhu1505@gmail.com

Abstract
The rapid growth of Wireless Network has raised a great concern for security threats. Currently, security is regarded as one of the critical parameter for the acceptance of any wireless networking technology. Any node under attack in wireless network presents an anomalous behavior called the malicious behavior. In this circumstance, the entire operation of a network gets troubled and to prevent such malicious behaviors, several security resolutions have been found. Malware is a common term that is used to define the type of malicious software that plays a vital role in security threats to the computer and Internet. In this paper, the categories of malware, malware vulnerabilities and the existing handling mechanisms are discussed.

Keywords - Security Threats, Malware Attacks, Malware Vulnerabilities, Malicious propagation.

1. Introduction

A security threat is a potential cause of unwanted event, which may result in damage to a system or a network. Wireless networks are exposed to various threats and attacks. Out of which malware attacks pose serious threats to the wireless networks exploiting the fundamental limitations of wireless network [1], such as limited energy, dynamism in topology due to mobility and unreliable communication.

In 1988, Morris worm caused $10 to $100 million damage on the Internet with 60,000 computers connected. Within the period of five years, 4,00,000 computers got affected by Blaster worm. Anti-Spyware in 2011, attacked Windows 9x, 2000, XP, Vista, and Windows7. Due to the rapid growth of consumer demands and advancements in wireless technologies, malware attacks in the internet imposing billions of dollars in repair.

Hence, the survey proposes the need to defend against these attacks. Section 2 presents briefly the security threats in the wireless network. Section 3 discusses the purpose, various types of malware attacks and vulnerabilities of malware attacks. Section 4 explains the existing malware detection techniques and section 5 gives the conclusion.

2. Security threats in wireless networks

A threat to a computing system is a set of situations that has the possibility to cause loss or damage. There are various security threats [3] to the wireless network. Figure 1 gives the classification of threats

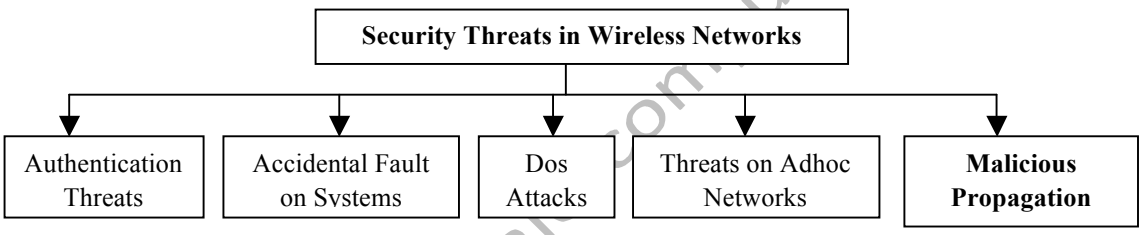

Figure 1. Classification of Security Threats in Wireless Networks

2.1. Authentication threats

A password remains vulnerable in many systems. With full access privileges, a system administrator may leak sensitive company information that may greatly affect the stability and reputation of the organization. In many cases, inadequate or no encryption is used and anyone 'in between' can view and modify the network traffic.

2.2. Accidental fault on Systems

Unauthorized access to company wireless and wired networks can come from a number of different methods. One of these methods is called accidental association. When a user enters into a computer and it bolts on to a wireless access point from a neighboring companies overlapping network, the user may not know that this has occurred. So, proprietary company information is exposed and there may exist a link from one company to the other.

2.3. Denial of Service (DoS) Attack

Denial of service is an attack that prevents users from making use of a service in a computer or network and target the computer network connectivity or bandwidth. Bandwidth attacks overflow the network with high volume of traffic and all available network resources are consumed and user requests cannot get through. Connectivity attacks overflow a computer with high volume of connection requests that all available OS resources are consumed and the computer can no longer process legitimate users requests.

2.4. Threat on Ad-hoc Networks

Ad-hoc networks are termed as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of risks in networks have little protection, encryption technique can be used to provide security.

2.5. Man-in-the-Middle Attacks

A man-in-the-middle attack tempts computers to log into a computer which is set up as a soft AP (Access Point). This attack relies on handshake protocols to execute a de-authentication attack and forces AP connected computers to break their connections and reconnect with the crackers soft AP.

2.6. Malicious propagation

Email has become the primary means of communication for many organizations. Tampering the computer system includes penetration, Trojan horse virus and the generation of illegal codes to alter the standard codes within the system. This type of operation can be termed as malicious misuse [3]. The various categories of malicious propagation are listed below:

- Social Engineering - Virus writers, Scareware vendors and Phishers are users of Social Engineering.
- Attacks on web Applications - Attacks when users visit a website, clicking in an E-mail or link from Social Engineering site and visiting a legitimate website.
- Drive-by downloads attack - Causes threats such as log keystrokes, rootkit, herd system into botnet and infect web browser with Trojan Horse.

This section briefly explained the different types of security threats in Wireless Network and different Malicious Propagations. These malicious propagation leads to different attacks to the network and among those malware attacks greatly affects the internet, financial services, online services, Network security and media. Out of these security threats Malware has been observed to be the more vulnerable attack in the network.

3. Malware Attack

Software that accomplishes deliberately the harmful purpose of an attacker is commonly known as malicious software or malware [Moser et al. 2007]. Malware [1] is a generic term that used to describe many types of malicious software, such as viruses and worms.
This section discusses the purpose, categories and vulnerabilities of malware attacks in the wireless networks.

3.1. Purpose of malware

The purpose of Malware is to cause damage or penetrate users computer for the purpose of hacking personal data for illegal activity such as financial crimes. Many DoS viruses, and the Windows Explore Zip worm, are designed to demolish files on a hard disk, or to corrupt the file system by writing void data to them. Profit category of malware develop spyware that are

programs designed to monitor display unsolicited advertisements, users' web browsing, or redirect affiliate marketing revenues to the spyware creators.

3.2. Categories of Malware

The various malware attacks in the wireless networks are listed in the table 1 below:

Table 1. Malware classifications

Malwares	Infection	Spread Through	Various Types	Preventive Measures
Virus	-Slows down host computer and destruct program files and system hardware	Internet Download, Attachment in E-mails, File Sharing Network	Boot sector virus, Polymorphic virus, Macro virus, Stealth virus, Retro virus	-Anti-virus software -current updates -Periodic System scan
Worms	-High bandwidth Consumption -Web browser irregularity - OS and System error Fault	Email, Instant Messaging, Relay Chats, File Sharing	Conficer, Black worm, Morris worm, XSS, Ramnit worm, Blaster worm	-Updated firewall and Antivirus software -Update of OS and Software
Trojan Horses	-System crash -Keystroke logging -Passwords and credit card theft	MP3 files, image games, Movies	Netbus, Vundu, Zlob Trojan, Beast, Zeus, Coreflood	-Anti-virus software -Anti-Trojan Programs
Blended Attacks	-Damage network at a same time -Disrupts exe files, HTML file and registry keys	E-Mail, IRC, File sharing Network	Morris worm, Win 32/Nimda.A@mm, Win 32/Bolzano, VBS/Bubbleboy	-Memory scanner solutions -Host - based IDS solutions
Keylogger	-Infects Websites -Exploits USB and storage Media	Secondary storage devices like DVD drive, USB Flash drives	Hardware based Keylogger and Software based Keylogger	-Anti keylogger -Anti-spyware -Security tokens
Rootkit	-Website Infection -Admin access exploited	Smartphones, PDA	Application level, Kernel level, Hardware/firmware, Hypervisor, Boot loader level	-Anti-malware solution -Firewall with security patches installation

Thus, the above table discusses the various Malware infections, their propagation, various types and their preventive measures.

3.3. Malware Vulnerabilities

Vulnerability is a weakness which allows an attacker to compromise the availability, integrity or confidentiality of a computer system [3]. Vulnerabilities may be the outcome of a programming error or a flaw in the design that will affect security.
There exists various vulnerabilities and they are shown in figure 2 below.

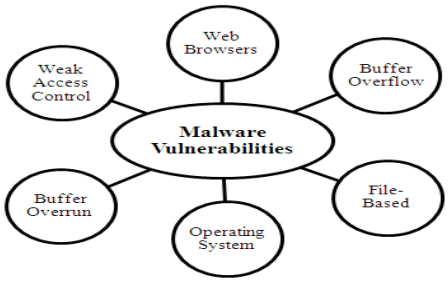

Figure 2. Different Malware Vulnerabilities

3.3.1. Buffer Overflow Vulnerability

Buffer overflow vulnerability allow an attacker, from a remote location, to obtain full system level access to any server that is running under default installation of Windows NT 4.0, Windows XP or Windows 2000, that uses the Microsoft Internet Information Services (IIS) Web server software.

3.3.2. File based vulnerability

PDF files that contain vulnerabilities are often associated with Advanced Persistent Threat (APT) style attacks than self-replicating malware. In this particular case, the vulnerability is most often used in Web toolkit based attacks.

3.3.3. Operating System Vulnerability

Operating systems face escalating security challenges. XP has its own unique vulnerabilities and Windows 98 accessed most of its vulnerabilities from Windows 95. The majority of existing malware is written to attack Windows systems, and then these systems are more vulnerable to yielding to malware attacks.

3.3.4. Buffer-Overrun Vulnerability

Buffer-overrun vulnerability, in which an interface designed to keep data in a small area of memory, allows the caller to supply more data than will fit. This extra data then overwrites the interfaces own executable structure.

3.3.5. Web Browser Vulnerability

Web browser vulnerabilities are a serious security problem due to their major role in online fraud and in the propagation of malicious code, adware, and spyware. Browser functionality is extended by various plug-ins, this plug-in component results in potential attack surface for client-side attacks.

3.3.6. Weak Access Control Vulnerabilities

Access control is a security process that controls usage of specific resources within the predefined criteria and is a portion of the AAA (Authorization, Authentication, Accounting) security model. This weakness describes a case where software fails to restrict access to an object properly.

This section briefly discusses the various vulnerabilities affecting the network by these malware attacks. Among these vulnerabilities, buffer overflow vulnerability greatly affects the network.

4. Malware handling techniques

Malware detection has to perform with the quick detection and validation of any instance of malware to prevent further damage to the system [5]. Some of the basic malware detection techniques are shown in the figure 3 below.

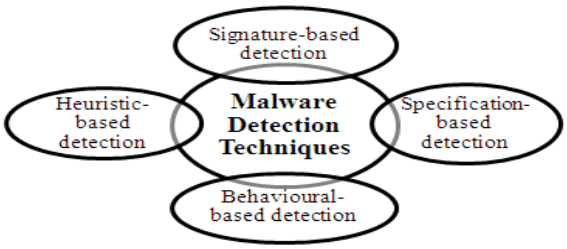

Figure 3. Existing Malware Detection Techniques

4.1. Signature-based malware detection

Commercial antivirus scanners search signatures which are typically a sequence of bytes within the malware code to declare whether the program scanned is malicious or not. A pattern-matching approach for commercial antivirus is one of the where the scanner scans for a sequence of byte within code to identify and signal a malicious code.

4.2. Specification-based malware detection

Specification-based malware detection is a technique where a detection algorithm directs the deficiency of pattern-matching. Specification-based detection come from anomaly based detection. The implementation of a specification-based detection approximates the specification of application or system.

4.3. Behavioral-based detection

Behavior based detection deviates from the surface scanning method in that it identifies the action performed malware. These types of detection mechanism are useful in detecting the malwares which keeps on generating new mutants because they will always use the system resources and services in the similar manner.

4.4. Heuristic-based detection

Heuristic-based detection can be used to identify unknown viruses. It uses 'advanced' and 'passive' heuristics for detecting viruses. Passive heuristics is based purely on scanning a file. Advanced or 'active' heuristics involve a controlled execution of the threat while monitoring it for threatening behavior.

There are also some of the hybrid approaches [2][4][5][6][7][8] existing for the malware attacks. They are listed in the table 2 below:

Table 2. Comparison of Malware handling Techniques

Approaches	False positive rate	True positive rate	False Negative rate	False Alarm rate	True detection rate	Infection ratio
Learnig Approach with SVM	✓					
Unsupervised Network IDS	✓	✓				
Content-Classification Scheme	✓		✓			
Stochastic Mean field games						✓
Traffic Entropy Spectrum	✓	✓				
WSRMAS method						✓
Discrete-time simulation method				✓	✓	
Spectrum based detection					✓	✓
Pulse Quarantine Strategy	✓					
VEISV method						✓

Thus, the above table discusses the various hybrid approaches and their metrics used for the malware detection. Among these parameters false positive rate highly identifies the malware and next to that is the Infection ratio which maximizes the damage caused by the threat in the network.

5. Conclusion

Internet has several security threats affecting the network and the communication security. This survey investigated security threats to wireless network, various categories of malware, their vulnerabilities and detection techniques are discussed. Out of which, the false positive rate and infection ratio are the important parameters in detecting the malwares. The detection techniques which reduce the value of these parameters are found to be the ideal detection technique.

References

[1] Adebayo, Olawale Surajudeen, Mabayoje, Amit Mishra, Osho Oluwafemi, "Malware Detection, Supportive Software Agents and Its Classification Schemes," International Journal of Network Security & Its Applications (IJNSA), Vol. 4, No. 6, November 2012, pp.33-49, ISSN: 0974-9330.

[2] M.H.R.Khouzani, Saswati Sarkar and Eitan Altman, "Maximum Damage Malware Attack in Mobile Wireless Network," IEEE/ACM Transactions on Networking, Vol. 20, No. 20, October 2012, pp. 1347-1360, ISSN: 1063-6692.

[3] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "Wireless Network Security: Vulnerabilities, Threats and Countermeasures," International Journal of Multimedia and Ubiquitous Engineering, Vol. 3, No. 3, July 2008, pp.77-86, ISSN: 1975-0080.

[4] Nir Nissim, Robert Moskovitch, Lior Rokach and Yuval Elovici, "Detecting unknown computer worm activity via support vector machines and active learning," Pattern Analysis and Applications, Vol. 15, No. 2,Springer-Verlag London Limited, May 2012, pp.459-475, ISSN:1433-7541.

[5] Radhika Saini, Manju Khari, "Defining Malicious behavior of a Node and its Defensive Methods in Ad Hoc Network," International Journal of Computer Applications, Vol. 20, No. 4, April 2011, pp.18-21, ISSN: 0975-8887.

[6] Wei Yu, Xun Wang Prasad Calyam, Dong Xuan and Wei Zhao, "Modeling and Detection of Camouflaging Worm," IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 3, May/June 2011, ISSN: 1545-5971.

[7] Yu Yao, Hao Guo, Ge Yu and Fu-xiang Gao, "Discrete-time simulation method for worm propagation model with pulse quarantine strategy," Advanced in Control Engineering and Information Science, ELSEVIER, SciVerse ScienceDirect, Vol. 15, 2011, pp.4162-4167.

[8] Yu Yao, Lei Guo, Hao Guo, Ge Yu, Fu-xiang Gao, Xiao-jun Tong, "Pulse quarantine strategy of internet worm propagation:Modeling and analysis", Computers and Electrical Engineering, ELSEVIER, Vol. 38, 2012, pp.1047-1061.