ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

WINDOWS OPERATING SYSTEM VULNERABILITIES

Gaurav Sharma, Ashish Kumar, Vandana Sharma

Abstract

Computers have brought about a revolution across all industries. Computers have become the most important part for the success of any enterprise. Computers are the best means for proper storage and management of data. They can assist as knowledge bases and can be utilized for financial transactions due to their processing power and storage capacities. PCs handle and keep a track of data which is very confidential and essential for an organization. So, managing the security of these computers is a very important task. This realization has led to the development of techniques that attempt to detect problems or loopholes in software systems. However, there exist some software failures which could be used for an intentional attempt to severely damage the systems. These software failures commonly denoted as computer vulnerabilities, have special properties that separate them from other software failures. The detailed analysis of each vulnerability classifies its characteristics, policies violated by its exploitation, and leads to the understanding of the measures that are needed to eradicate these vulnerabilities in future programs. This paper aims to demonstrate several vulnerabilities in the

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

Windows Operating system. It will demonstrate and analyze how registry, clipboard, autoplay and task manger are vulnerable to attacks in Windows XP, Windows Vista and Windows 7.

Keywords: Patches, Security, Vulnerability, Windows Operating System

Introduction

In 2000, there were more than 50,000 computer viruses. In 2002, the count of known viruses, Trojans, worms, and their variations became 60,000. Today there are more than 1000,000 known computer viruses[1]. A. James Clark from University of Maryland's showed that every 39 sec an attack occurs on an internet enabled computer. [2] In today's world where software has become very important part of our lives, it has become very important for us to have secure software. The computer programs are becoming immersed in our lives. They virtually control everything from online education to business. In [3] it is shown that the United States is target of majority of Server-Side HTTP attacks. There are several sources and fewer destinations of these attacks. China is the second largest source of attacks after the United States. United States is top most target of such attacks.

To confront the security loopholes in software which can be technically referred as "Vulnerabilities", there is huge demand of vulnerability analyzers and other security related software. A vulnerability can be defined as *The existence of a weakness, design, or*

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

implementation error that can lead to an unexpected, undesirable event/s compromising the security of the computer system, network, application, or protocol involved.[4] Publically accessible databases are available for Vulnerabilities. These vulnerabilities provide basis for major system-related security breaches, which are the most harmful. These breaches are very difficult to inspect, because data is infrequent. Detailed discussion of breaches is available in [5].Vulnerabilities are classified according to their asset class they belong to such as hardware, software-operating system, application, network, personnel, site and organizational .Common types of software defects that lead to vulnerabilities are: Memory safety violations, Input validation errors, Metacharacters, Improper shell handling, so they are interpreted :SQL injection, Code injection, E-mail injection, Directory traversal, Cross-site scripting in web applications, HTTP header injection ,HTTP response splitting etc., Race conditions, Privilege-confusion bugs, Privilege escalation , User interface failures .[6] Vulnerabilities are introduced into programs by number of ways some of them are

1. Coders introduce vulnerable code into software unknowingly. This occurs due to lack of understanding and awareness of secure programming techniques.

2. Developers do not have appropriate tools for the vulnerability assessment of code and compiled applications.

Software vendors provide patches and updates for the system to fix these vulnerabilities. However, during hackers take advantage of these vulnerabilities to install malicious code on user machines for stealing secret data for monetary gains. The hacked computers can be

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

further used to launch Denial of Service attacks on servers. These machines can be misused to infringe the computers of government departments [7]. According to [8] the process of vulnerability discovery can be categorized into three different phases. Phase 1 comprises the collection of sufficient knowledge about the system. This phase is carried out by testers which will enable them to compromise the system .Actual vulnerabilities discovery happens in phase 2. Finally, in phase 3, vulnerability detection effort will then start drifting towards the subsequent version of the software. These phases form an "S" shape. It is anticipated to follow the vulnerability principle according to which the discovery rate is in line with momentum gained by the market acceptance of the product. It is also linear with the saturation of vulnerability discovery. The model also suggests that there is limited number of vulnerabilities that could be found. Rescorla, in [9] adopted the probabilistic G-O model (Goel and Okumoto model)[10], but no significant empirical evidence of its relevance was found . In [5] Alhazmi and Malaiya proposed a model which relates the number of vulnerabilities to the entire effort spent on detecting vulnerabilities.

Operating system Vulnerabilities

There are massive varieties of operating systems; only four central families exist in the mainstream – Windows, OS X, Linux and UNIX. According to [11] Microsoft Windows dominates the world's operating systems market with almost 90% of the market share while Apple and Linux share the remaining 10% with a lot of other available operating systems. In [12] the analysis of five operating systems reveals that the mean time between vulnerability disclosures

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

for *Windows* operating is about double than those of the *MAC OSX* and open source operating systems. On the other hand, the software lines of code" of Windows operating systems is lower than that of *MAC OSX* and *Debian 3.1* Each operating system has its own package of vulnerabilities extending from local exploits and to remotely available attack vectors. As far as "straight-out-of-box" conditions go, both Microsoft's Windows and Apple's OS X are full of remotely reachable vulnerabilities. Even before deploying the servers, Windows based machines contain numerous exploitable loopholes which allow hackers access the system as well as execute random code.

When it comes to corporate, most systems rely on trained administrators and IT departments which frequently patch and update the operating systems and its services. The scenario for home computers is different. The more customer oriented operating systems made by Microsoft and Apple are each "hardened" in their own capacity. As soon as user begins to subjectively enable fiddling around with the default settings, the systems immediately become susceptible to intrusion. When appropriate patches or automatic updates are not enabled, owners of Windows and OS X computers are the most susceptible to quick and thorough remote violations by hackers. As per Microsoft Security Bulletin MS08-067 in 2009 more than 90% of the Microsoft targeted attacks were the buffer overflow vulnerability attacks. Most of these attacks on Microsoft Windows operating systems were by Conficker/Downadup worm and its variants. Even worms like Sasser and Blaster, which were infamous in 2003-2004 were also active in this period. [3] The attacks mentioned above are common to both Operating Systems and Applications. As a resolution, Vendors provide patches and updates frequently. Operating

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

System vulnerabilities get quickly addressed by vendors in the first fortnight of their lifetime. The vulnerabilities found in applications, receive less attention and get patched slowly. Widely used applications, such as Microsoft Internet Explorer, Microsoft Office, and Adobe Reader are more vulnerable to threats. Attacks using PDF vulnerabilities have reportedly increased in 2008 and 2009. In the last few years, the number of vulnerabilities exposed in applications is much greater than the number of vulnerabilities in operating systems as in fig. 1. As a consequence, extra exploitation attempts are recorded on application programs.

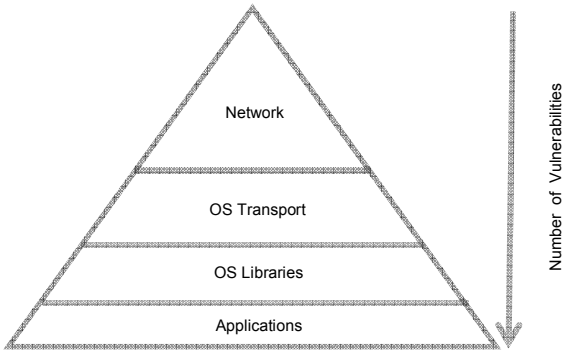

Fig.1 –Number of vulnerabilities category wise trend

Windows operating system Vulnerabilities

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

Many vulnerabilities have been published for windows operating system. Some of the common vulnerabilities found in all versions of windows are: DoS, Remote Code Execution, Memory Corruption, Overflow, Sql Injection, XSS, Http Response Splitting, Directory Traversal, Bypass something Gain Information/Privileges, CSRF File Inclusion etc. According to [13] ninety seven Windows XP vulnerabilities were reported in year 2010. So far eighty one vulnerabilities have been reported in 2011. The maximum number of vulnerabilities detected were of Gaining Privileges by which the confidentiality and integrity was highly impacted.

Experiment

To explore the loopholes in windows operating system a program was developed. This program had identified number of vulnerabilities in various versions of Windows operating system. Some of the vulnerabilities detected are

Autoplay Vulnerability

Autoplay feature came in Windows XP. This feature checks removable media/ devices then identifies and launches appropriate application based on its contents. This feature is useful for authentic users but is a gateway for an attacker. The program developed was able to gain access and execute arbitrary code by inserting USB using this feature.This vulnerability can be exploited locally. The complexity of attack in this case is low. The system confidentiality and integrity is lost completely.

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

Clipboard Vulnerability

The software developed was able to get access to clipboard data and modify it. This vulnerability can allow attacker to get access to sensitive clipboard data. In windows clipboard is common for all applications. This may lead to access and modification in the clipboard of all applications in the operating system.

Registry Vulnerability

MS-Windows stores its configuration settings and options in a hierarchical database which is known as windows Registry. Registry is used for low level operating system settings and for settings of applications running on the platform. All vital components of operating system such as kernel, UI, device drivers, SAM etc. make use of registry. The registry editor of windows is not a secured program. It allows the editing of registries without the permission of the owner. As there is no message specially displayed before editing of registry with software of executable files, therefore the attackers are able to change the DWORD value of registry easily which poses a serious threat

PNG Vulnerability

Software was able to cause denial of service (DoS attack). In this vulnerability Windows allows an attacker to use Portable Network Graphic (PNG) image with properly crafted resolution in the IHDR block which leads to 100% CPU consumption. Windows operating system is not equipped

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
http://www.ijccr.com
VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

to handle malicious PNG files. This vulnerability may result into excessive usage of resources and causes system crash. Thus, denying service to users. This vulnerability does not result into confidentiality or integrity loss and has partial availability impact.

Result and Discussion

In the experiment, user was able to gain access through autorun vulnerability which is a serious threat to the confidentiality and integrity of the same. Clip board vulnerability can also result into severe damage to the data. Registry vulnerability can lead to unwanted operating system settings by malicious user. PNG vulnerability causes denial of service and consumes resources. Microsoft has still not released any patch for this vulnerability. Effect of these vulnerabilities was tested on all popular versions of MS Windows like Windows XP, Windows Vista and Windows 7. Summary of effect of these vulnerabilities is given in Table 1.

Vulnerability	Integrity Impact	Confidentiality Impact	Availability	Gained Access
Registry	Y	Y	Y	Y
Clipboard	Y	Y	Y	Y
Autoplay	Y	N	Y	Y
PNG	N	N	Y	N

Table 1: Vulnerability Impact

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

User was able to gain access through Registry, clipboard and autoplay vulnerability and integrity of system was also affected by these three vulnerabilities. Through registry and clipboard vulnerability confidentiality of system was also compromised.

Conclusion

With the advent of technology new vulnerability or weaknesses are discovered every day. This paper explored the foundations of an attack using a system developed. An experiment was conducted which demonstrated that upgraded versions of windows operating system still have number of vulnerability which can be lead to compromise the system. There are certain vulnerabilities which do not have any patch available.PNG is such a vulnerability. Window is highly popular operating system but still it is prone to attacks. System developed was able to use vulnerabilities like Registry, Autoplay and Clipboard to get access to the system. These vulnerabilities in Microsoft Windows make it more prone to attacks. A user must be aware of these vulnerabilities and use more security measures to protect the system. Operating system vendor should test their product well in advance and provide secure environment.

References

[1] http://www.cknow.com

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

[2] http://csdl2.computer.org

[3] http://www.sans.org

[4] http://www.enisa.europa.eu

[5] Alhazmi, O., Malaiya, Y. and Ray, I. (2005) Security Vulnerabilities, in Software Systems: A Quantitative Perspective in

Data and Applications Security 2005, LNCS 3654, 281-294.

[6] Wikipedia.com

[7] R. Srinivasan , Protecting Anti-Virus Software Under Viral Attacks, Master Degree of Science, Arizona State University (2007).

[8] Alhazmi, O., Malaiya, Y. and Ray, I. (2005) Security Vulnerabilities, in Software Systems: A Quantitative Perspective in Data and Applications Security 2005, LNCS 3654, 281-294.

[9] Glass, R.L. (2004) A look at the economics of open source, in Comm. of the ACM, 47,2, 25-27

[10] Goel, A.L. and Okumoto, K. (1979) Time-Dependent Error-Detection Rate Model for Software and Other Performance Measures, in IEEE Transactions on Reliability, 28, 3, 206-211.

[11] http://www.w3schools.com

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

VOLUME 1 ISSUE 3 MANUSCRIPT 13 NOVEMBER 2011

[12] Schryen, Vulnerabilities in open and closed source software, Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th 2009

[13] http://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26