ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Vulnerable Security Aspects of Windows

Dr. Rajinedr Singh *, Shakti Kumar
* S.D.College,Ambala Cantt,Haryana, India
rsrana42@rediffmail.com

Abstract

With the advancement in technology we are having everything available on a single click. Instead of wasting a lot of time while standing in a queue for a task to be done now we just have to open our device and connect it to the internet and the task completes in few minutes. This all is possible due to the availability of network. On one side where we are saving the time on the other side we are exposing our secret information to a third party which may misuse it. It is because the structure of internet and windows itself allowed many security problems to occur. We can modify the architecture of internet to reduce the possibility of attack on data. If we talk about various business organizations they keep themselves protected from threats by connecting there self to intranet instead of internet. The Network and windows Security can be simple or complex depending upon the requirements. In order to understand the present scenario of research in this field we must first understand its importance, history and various technologies which can be used to provide security measures.

Keywords: *Windows Security, Security Importance, History of security, Attack Methods, Vulnerable aspects*.

Introduction

In the world of Information and Technology no one is isolated. We are connected to each other through internet and new networking technology. Internet itself is now acting as a data store which have information related to personals, commercial, military and government sectors. So security of this kind of data is taken as a serious aspect. Fundamentally there are two different types of networks and they are : *Synchronous Network* and *Data Network.* Synchronous network are less vulnerable because they just have switches to forward the data but they doesn't buffer the data, while data networks are more vulnerable because they make use of routers through which information can be obtained easily through special programs such as Trojan Horses. We can analyse the security by researching the following points:

1. History of security in Networks
2. Internet Architecture
3. Types of Internet Attack
4. Current Hardware and Software development for security[1]

History of Network Security

On one side Vinton Cerf was elected the first chairman of InterNetworking Working Group(INWG) and later known as father of internet.[10] On the other side Polish cryptographer created an enigma machine in 1918 that converted plain message to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. [1] In 1960s, the term "hacker" is coined by a couple of Massachusetts Institute of Technology (MIT) students.[3] During the 1970 The telenet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers[3]. Initially when protocols were introduced they were not secured

Internet Architecture

IP is the internet protocol which is network layer protocol and the key element of Internet technology. The IP protocol is the protocol most used by computer systems to intercommunicate. The majority of higher-level applications or protocols (HTTP, SMTP, P2P, etc.) are based on this protocol for their functioning. Computers and devices using the IP protocol are assigned a unique identifier called IP address to route the message through the different communication network nodes from source to destination. This identifier is a 32-bit integer number which is usually represented as four numbers, from 0 to 255, each separated by a dot, for its greater ease of handling. IP was first announced by IETF (Internet Engineering Task Force) in 1970's. There are old

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

versions, current version which is IPv4 and new version which is IPv6. [20]
IPv4 looks like this:
255.255.255.255
And IPv6 looks like this:
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Old version of IP technology
IPv0, 1, 2, 3
In 1970's, IETF's workgroups were working on Internet protocol and they were firstly invented the old version of IP. IPv1, IPv2 and IPv3 were used to development of IPv4. They never used for public and they were always remained as experimental versions. [22]
IPv5
In 1979, Internet Stream protocol was invented. Its uniqueness was to transmit the video, audio and multimedia messages over the internet. This Internet Stream Protocol was called IPv5. It was never used for public and it never saw the light of day. It is working on the same level with IPv4. However, it is using different header format than IP datagram is used. [24]
Disadvantages of Current IPv4

IPv4 has a lot of weakness and disadvantages. IPv4 inventers did not think that this technology will become this much popular and this much people work with it. The first disadvantage of IPv4 is that the number of IP addresses. There is 2^32 ip addresses which is around 4 billion. Today's world, it is not enough and the world needs more ip addresses. The second problem is mobility problem. IPv4 doesn't support mobility and handover mechanisms. If the mobile goes form one network to another network, the connection need to be establish again. Moreover, IPv4 uses NAT (Network Address Translation) to increase the number of IP addresses. It gives users private ip addresses then a lot of users enter the internet by using only one public IP address. However, NAT has a lot of problem. Firstly, NAT causes problem in RTC (real time communication) protocol. This protocol is used for VoIP and multimedia communication. Secondly, it causes security problems. Because it changes the IPSec headers and it damages the end-to-end security and data integrity. Finally, it has peer-to-peer communication problems. Since everybody doesn't have a real IP address, the connection between users is hard to establish because of the public IP usage. [25]
IPv6 Overview
After seeing the disadvantages of IPv4, Internet Engineering Task Force (IETF) had found IPng (Internet Protocol next generation) workgroup in 1990's. This group's aim was to find a new IP protocol to solve the problems on the current IPv4. It has a lot of people such as Industry professionals, universities and organizations and they worked together for 10 years. For the last 5 years, IPv6 starting time was suspicious. Network experts were making predictions about starting time of IPv6 but mostly they were wrong. Finally, at 6 June 2012, IPv6 was officially started. The major companies started to use IPv6 and a lot of others are expected to join them. [26]

Types of Attack

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and trojans. The other form of attack is when the system's resources are consumes uselessly.[1]

Eavesdropping
Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [8].

Viruses
Viruses are self replication programs that use files to infect and propagate [8]. Once a file is opened, the virus will activate within the system

Worms
A worm is similar to a virus because they both are self replicating, but the worm does not require a file to allow it to propagate [8]. There are two main types of worms, mass mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

Trojans
Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus [8].

Phishing
Phishing is an attempt to obtain confidential information from an individual, group, or organization [9]. Phishers trick users into disclosing

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

personal data, such as credit card numbers, online banking credentials, and other sensitive information.

IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP spoofed packets cannot be eliminated [8].

Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [9]. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service

Hardware & Software Development

Hardware development

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security The most obvious use of biometrics for network security is for secure workstation logons for a workstation connected to a network. Each workstation requires some software support for biometric identification of the user as well as, depending on the biometric being used, some hardware device. The cost of hardware devices is one thing that may lead to the widespread use of voice biometric security identification, especially among companies and organizations on a low budget. Hardware device such as computer mice with built in thumbprint readers would be the next step up. These devices would be more expensive to implement on several computers, as each machine would require its own hardware device. A biometric mouse, with the software to support it, is available from around $120 in the U.S. The advantage of voice recognition software is that it can be centralized, thus reducing the cost of implementation per machine. At top of the range a centralized voice biometric package can cost up to $50,000 but may be able to manage the secure log in of up to 5000 machines. The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by incorrectly entering their password repeatedly. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs. Smart cards are usually a credit card sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. The main idea behind smart cards is to provide undeniable proof of a user's identity. Smart cards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions. It may seem that smart cards are nothing more than a repository for storing passwords. Obviously, someone can easily steal a smart card from someone else. Fortunately, there are safety features built into smart cards to prevent someone from using a stolen card. Smart cards require anyone who is using them to enter a personal identification number (PIN) before they'll be granted any level of access into the system. The PIN is similar to the PIN used by ATM machines. When a user inserts the smart card into the card reader, the smart card prompts the user for a PIN. This PIN was assigned to the user by the administrator at the time the administrator issued the card to the user. Because the PIN is short and purely numeric, the user should have no trouble remembering it and therefore would be unlikely to write the PIN down. But the interesting thing is what happens when the user inputs the PIN. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there's absolutely no danger of it being intercepted. The main benefit, though, is that the PIN is useless without the smart card, and the smart card is useless without the PIN. There are other security issues of the smart card. The smart card is cost effective but not as secure as the biometric identification devices.[1]

Software developments

The software aspect of network security is very vast. It includes firewalls, antivirus, vpn, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now. The improvement of the standard security software still remains the same. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analyzing attack patterns in

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

order to create smarter security software
As the security hardware transitions to biometrics, the software also needs to be able to use the information appropriately. Current research is being performed on security software using neural networks. The objective of the research is to use neural networks for the facial recognition software Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. This power, however, is not available in small devices like sensors. Therefore, there is a need for designing light weight security algorithms. Research in this area is currently being performed[1]

Problems Associated With Windows

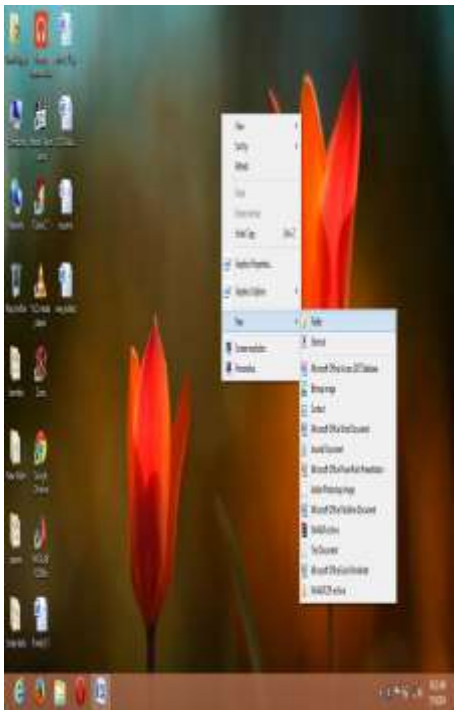

Fig.1 Creation of Folder

We use windows operating system in our day to day life to store data using folders to provide their logical grouping. All windows operating system support ASCII values which can be used to break the rules and to hide the folder without actually using hide file and folder options. Steps to perform this task are represented in the figure given below:
1.First create a Normal Folder (say on Desktop)
2.Go to the properties of folder and click on customize tab. Then click the change Icon button.

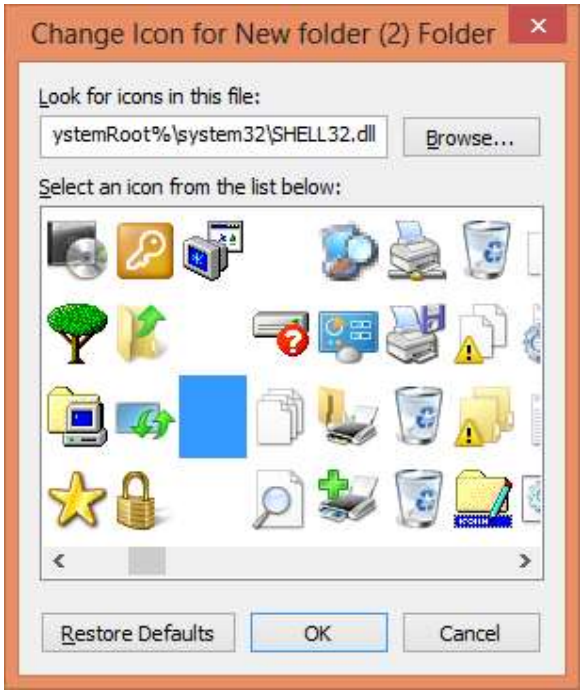

Fig.2Making folder Icon Transparent

3.From change icon window choose transparent icon for folder and half job is done.
4.Now we can see that folder is transparent and only its name is available on desktop not its picture.

Fig. 3 Invisible Folder as Output

5.Now to remove the name of this transparent folder we we have to rename it with a special ASCII key combination that is Alt+0160(From Numeric key Pad). It is a value of space which will be accepted as

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

a empty name in folder and folder will be totally invisible without making it hidden from folder options

Fig.4 Renaming using ASCII code

Conclusion

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive. The network security field may have to evolve more rapidly to deal with the threats further in the future. Also there are many problems associated with window, one of the case we have studied is regarding folders vulnerability. By breaking the rules of windows operating system for folder creation we can customize it in our own way to create a hidden folder. So more security constrains should be applicable to such problems in windows

References

[1] *Network Security: History, Importance, and Future.*

[2] *Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998*

[3] *Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008*

[4] *"Security Overview," www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.*

[5] *Molva, R., Institut Eurecom,"Internet Security Architecture," in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999*

[6] *Sotillo, S., East Carolina University, "IPv6 security issues," August 2006, www.infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf.*

[7] *Andress J., "IPv6: the next internet protocol," April 2005, www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.*

[8] *Warfield M., "Security Implications of IPv6," Internet Security Systems White Paper, documents.iss.net/whitepapers/IPv6.pdf*

[9] *Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008*

[10] *Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005*

[11] *"Internet History Timeline," www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm.*

[12] *Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, vol.85, no.12, pp.2034-2051, Dec 1997*

[13] *"Intranet." Wikipedia, The Free Encyclopedia. 23 Jun 2008, 10:43 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Intranet&ol did=221174244>.*

[14] *"Virtual private network." Wikipedia, The Free Encyclopedia. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Virtual_priv ate_network&oldid=222715612>.*

[15] *Tyson, J., "How Virtual private networks work," http://www.howstuffworks.com/vpn.htm .*

[16] *Al-Salqan, Y.Y., "Future trends in Internet security,"*

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

[17] *Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of , vol., no., pp.216-217, 29-31 Oct 1997*
[18] *Curtin, M. "Introduction to Network Security," http://www.interhack.net/pubs/network-security.*
[19] *"Improving Security," http://www.cert.org/tech_tips, 2006.*
[20] *Serpanos, D.N.; Voyiatzis, A.G., "Secure network design: A layered approach," Autonomous Decentralized System, 2002. The 2nd International Workshop on, vol., no., pp. 95-100, 6-7 Nov. 2002*
[21] *Ohta, T.; Chikaraishi, T., "Network security model,"*
[22] *Networks, 1993. International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Proceedings of IEEE Singapore International Conference on , vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993*
[23] *Report On The Security Implications Of Implementing Ipv6, The National Institute of*
[24] *Communication Technologies, 2010.*
[25] *www.whatismyip.com*
[26] *Internet Protocol, Wikipedia*
[27] *IP Protokolü Nedir, Tübitak-Ulakbim, www.ipv6.net.tr*
[28] *IPv6 Tutorial, SANOG V Dhaka, Bangladesh , 2005*
[29] *www.worldipv6launch.org/*
[30] *Why IPv6 Matters to Your Station, Glenn Davies, 2011*
[31] *IPv6 - The Next Generation Internet, Kaushik Das, 2008*
[32] *Differences IPv4 Vs IPv6, Techsutram, 2009*