Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 11, November 2013, pg.270 – 276

RESEARCH ARTICLE

Evolution of Security Attacks and Security Technology

Ankalarao Konakalla[1], Bhavani Veeranki[2]

[1]Anurag Engineering College, Kodad & JNTUH, Andhra Pradesh
[2]Anurag Engineering College, Kodad & JNTUH, Andhra Pradesh

[1] ankalarao.cse@anurag.ac.in; [2] bhavaniece115@gmail.com

Abstract— ***This paper presents a Security Attacks and Security Technology. Internet Security is a complex in terms of both topology and emerging technology. In such an environment, security measures applied for small well-defined networks cannot work effectively. The lack of adequate knowledge and understanding software and security engineering leads to security vulnerabilities.For example, a financial firm's New York City data centre may receive real-time updates from a stock exchange in Switzerland, conduct financial transactions with banks in Asia at that time Security Attacks may happen. Moreover, different solutions must be combined to be effective against different types of attacks and the security of the system must be constantly monitored.***

Keywords— topology; data centre; TCP/IP

I. INTRODUCTION

Internet is a worldwide collection of connected computer networks that are accessible by individual variety of ways using a particular set of communication protocols which is known as TCP/IP.

II. INTERNET SECURITY

Today millions of end systems use the Internet regardless of national or geographic boundaries or time. Over the past decade, the Internet has enabled individuals across the world to become increasingly connected. The development and expansion of the Internet has created innumerable new opportunities for personal interaction and entrepreneurial ventures. Not only has the cost of communication fallen considerably, but perhaps even more importantly, the sphere of potential trading partners has expanded dramatically creating immense new gains from exchange. However, along all its advantages the Internet is not free from risks and cyber criminalities as in the real world. The main goods on the Internet are valuable information which can be lost, eavesdropped, manipulated or misused and the computer systems which can be corrupted.

The Internet is in general an adversarial environment where attacks can be easy, inexpensive and may be hard to prevent, detect or trace. The consequences are however, drastic in terms of time and money. In general, it is difficult to ensure the main security goals which are confidentiality, integrity and availability. There are many reasons for today's security risks on the Internet, the Internet was designed to be an open and distributed environment without any central instance controlling the communication among the users and mutual mistrust was not of primary concern. Critical to these advances in ecommerce is the existence and development of Internet security. To illuminate this, consider a case where there was little or no security on the Internet, with the

risk of falling victim to fraud, information theft, viruses, etc. users would have little incentive to utilize the Internet.

III. COMPUTER SECURITY ATTRIBUTES

There are four main computer security attributes, including confidentiality, integrity, privacy, and availability. Understanding the security attributes is crucial in order to conduct risk analysis and find the suitable control for each attribute.

Confidentiality can be considered as secrecy. Unauthorized persons should not gain access to others' data or other computing assets. Different degrees of confidentiality are possible in electronic transmissions, as confidentiality can depend on simple passwords, secure connections, or more advanced technologies. Integrity involves accuracy of data. To achieve integrity, only authorized persons are able to create, edit, and delete data in an approved manner. One should ensure that the prevention of tampering is included when considering this attribute as well Availability means computer assets should be available for and accessible to authorized persons when they need them and should not be interrupted Privacy is the ability and/or right to protect your personal secrets; it extends to the ability and/or right to prevent invasions of your personal space. It simply means that the subject of information should be able to Control the information.

IV. INTERNET SECURITY THREATS AND SOLUTIONS

Table 1 below shows the relationship between the various attack methods and their corresponding Internet solutions

Computer Security attributes	Attack Methods	Technology for Internet Security
Confidentiality	Eavesdropping, Hacking, Phishing, DoS and IP Spoofing	IDS, Firewall, Cryptographic Systems, IPSec and SSL
Integrity	Viruses, Worms, Trojans, Eavesdropping, DoS and IP	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Privacy	Email bombing, Spamming, Hacking, DoS and Cookies	IDS, Firewall, Anti-Malware Software, IPSec and SSL.
Availability	DoS, Email bombing, Spamming and Systems Boot Record Infectors	IDS, Anti-Malware Software and Firewall.

Table1. Attack methods and solutions

V. INTERNET ATTACKS

A) VIRUSES

Viruses are self-replicating programs that infect and propagate through files. Usually they will attach themselves to a file, which will cause them to be run when the file is opened. Viruses often have additional properties, beyond being an infector or macro virus. A virus may also be multi-partite, stealth, encrypted or polymorphic. Multipartite viruses are hybrid viruses that infect files and system and/or boot-records. This means multi-partite viruses have the potential to be more damaging, and resistant.

A stealth virus is one that attempts to hide its presence. This may involve attaching itself to files that are not usually seen by the user. Viruses can use encryption to hide their payload. A virus using encryption will know how to decrypt itself to run. As the bulk of the virus is encrypted, it is harder to detect and analyse. Some viruses have the ability to change themselves as time goes by, or when they replicate themselves. Such viruses are called polymorphic viruses. Polymorphic viruses can usually avoid being eradicated longer than other types of viruses as their signature changes. Macro viruses are simply macros for popular programs, such as Microsoft Word, that are malicious. For example, they may delete information from a document or insert phrases into it. Propagation is usually through the infected files.

If a user opens a document that is infected, the virus may install itself so that any subsequent documents are also infected. Some macro viruses propagate via email, such as the Melissa virus covered in the next section. Often the macro virus will be attached as an apparently benign file to fool the user into infecting themselves.

B) SYSTEM AND BOOT RECORD INFECTORS

System and Boot record infectors were the most common type of virus until the mid 1990s. These types of viruses infect system areas of a computer such as the Master Boot Record (MBR) on hard disks and the DOS boot record on floppy disks. By installing itself into boot records, the virus can run itself every time the computer is booted up. Floppy disks are often infected as users tend to leave floppy disks in the floppy drive. If left in the floppy drive, on reboot, the computer may boot from the floppy disk. Thus, the virus has a chance to execute. These types of viruses were very common in the early days of personal computing. However, with the introduction of more modern operating systems, and virus checks being enabled in the Basic Input Output System (BIOS), few of these viruses are being created today. New means of propagation, such as the Internet, are also much more attractive to virus creators.

C) Eavesdropping

Eavesdropping involves interception or gaining access to communications by unauthorized party. Passive eavesdropping happens when an unauthorized person listens secretly to the networked messages. On the other hand, active eavesdropping means that an intruder not only listens to but also injects something into the communication to distort or create bogus messages for example by changing partly or all content of the messages, reusing the old messages, deleting the messages or modifying the source of messages. Thus messages sent back and forth in communication line are exposed to interception or eavesdropping. Once the intruders' breaks into the network, they can silently examine messages during transmission and steal sensitive information that they want. The messages need protection to maintain their secrecy so that unauthorized persons can't scan them. It is vulnerable liability for companies as customers may claim or sue the companies if eavesdroppers succeed and disclose customers' personal data.

D) Hacking

Hackers can be people who are career criminal. They are competent and highly skilled at using computers. Once they analyze and discover a leak point in the target system, they will find ways to access and attack the system. They can use various kinds of attacks or even develop their own ways to attack the computer system. For example, they may access a system, and create bogus information or try to create an information flood. They can also break through Web servers to access or steal information.

E) Worms

A worm is a self-replicating program that propagates over a network in some way. Unlike viruses, worms do not require an infected file to propagate. There are two main types of worms, mass-mailing worms and network-aware worms. Mass-mailing worms are an interesting category as many attacks in this category could quite easily be classified as a worm, virus or both. For the purpose of this research and the taxonomy, a mass-mailing worm is a worm that spreads through email. Once the email has reached its target it may have a payload in the form of a virus or Trojan. Email, although it may become a file on its journey, is more abstract than a file. Therefore, while some attacks may use email attachments to send viruses, the attack vector is still email. An attack such as Melissa should be classified first as a mass-mailing worm. Network-aware worms are a major problem for the Internet. Worms such as SQL Slammer have shown that the Internet can be degraded by a well written worm. Network-aware worms generally follow a four stage propagation model. Although this is a generalization, most network-aware worms will fit into this model. The first step is target selection. The compromised host targets a host. The compromised host then attempts to gain access to the target host by exploitation. For example, the SQL Slammer worm exploited a known vulnerability in Microsoft SQL Server 2000 and Microsoft Desktop Engine. Once the worm has access to the target host, it can infect it. Infection may include loading Trojans onto the target host, creating back doors or modifying files. Once infection is complete, the target host is now compromised and can be used by the worm to continue propagation.

F) Trojans

Trojans get their name from the Iliad by Homer, which describes the battle for Troy. Homer writes about how the Greeks created a giant horse, filled it with soldiers, and left it outside Troy. The Trojans, thinking it was a gift of surrender, wheeled the horse inside Troy. At night, the Greek soldiers came out of

the horse and opened the gates for the rest of the Greek army. Troy was quickly defeated. Today's Trojans work in a very similar way. They will appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as remote access methods and viruses.

G) IP Spoofing Attacks

Spoofing is when attackers can forge their identity, appearing to be using a trusted Computer, and therefore are able to gain unauthorized access to other computers. It is the act of using one machine to impersonate another. A malicious cracker may gain entry by "spoofing" the source IP address of packets sent to the firewall. The firewall may let them through if the address used is a trusted host identity. To avoid such attacks responsible management of information is essential. Moreover, this type of attack is usually combined with other types of attack to hide the identity of crackers, and makes detection and prevention hard. Unfortunately, with the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, it is possible to reduce the number of IP-spoofed packets entering and exiting private networks. One method to reduce such attacks is to install a filtering router that rejects incoming packets to external interface having an internal source address or uses a reserved private network number or other invalid addresses. In addition, outgoing packets having a source address different from your internal network has to be blocked to prevent a source IP spoofing attack from originating from your site. These filters will not stop all spoofed attacks since outside attackers can spoof packets from any outside network, and internal attackers can still send attacks spoofing internal addresses.

H) Denial of Service

The Denial of Service (DoS) occurs when a system receiving the requests becomes busy trying to establish a return communications path with the initiator (which may or may not be using a valid IP address). The targeted host receives a TCP SYN and returns a SYNACK. It then remains in a wait state, anticipating the completion of the TCP handshake that never happens. Each wait state uses system resources until eventually, the host cannot respond to other legitimate requests.

I) Email Bombing and Spamming

Email bombing is characterised by abusers repeatedly sending an identical email message to a particular address. Email spamming is a variant of bombing; it refers to sending email to hundreds or thousands of users. Email spamming can be made worse if recipients reply to the email, causing all the original addressees to receive the reply. It may also occur innocently, as a result of sending a message to mailing lists and not realizing that the list explodes to thousands of users, or as a result of an incorrectly set-up auto-responder message. Email bombing/spamming may be combined with email spoofing making it more difficult to determine who the email is actually coming from. If your email system looks slow or email doesn't appear to be sent or received, the reason may be that your mailer is trying to process a large number of messages. When large amounts of email are directed to or through a single site, the site may suffer a denial of service through loss of network connectivity, system crashes, or failure of a service because of overloading network connections, using all available system resources and filling the disk as a result of multiple postings and resulting syslog entries.

J) Phishing

Phishing is an attempt by a third party to solicit confidential information from an individual, group, or organization, often for financial gain. Phishers are groups or individuals who attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information. They may then use the information to commit fraudulent acts.

VI. Internet Security Technology

With the rapid growth of interest in the Internet, network security has become a major concern to companies throughout the world. The fact that the information and tools needed to penetrate the security of corporate networks are widely available has increased that concern. Internet security tools typically provide authentication, encryption, identify attacks, and block and filter packets. There are two different access control approached used, the Discretionary Access Control (DAC) and the Mandatory Access Control (MAC). Commercial systems are based on DACs which indicates that the resources' owner specifies who may access and who may not access the resources. MAC on the other hand, works as a security officer that decides who is allowed and who is disallowed access to a particular resource.

A) Cryptographic systems

Cryptography originally denotes the art of keeping information secret by the use of codes and ciphers. It is a prevalent tool for security engineering today since one can notice that the computer industry has

extensively utilized cryptography as a basic standard in secured software development. The main process of cryptography is to encrypt or scramble an input message called 'plain text' with cryptography algorithm, which results in an output message called 'cipher text or cryptogram'. At the receiver side, in order to change cipher text into a readable format, a cryptographic key must be used for decryption. A cryptographic key is created from a string of digits. If the same key is used for both encryption and decryption, it is called a symmetric key. Another kind of key is an asymmetric key, which simply means the encryption key differs from the decryption key. At the present time, a strong cryptography is considerably powerful security technology. The strong cryptography algorithm is based on reliability of mathematical calculation. The calculation of cryptographic key is so complicated that it could not be cracked within a short time. Anyone, who wants to crack it, is supposed to take several years to achieve his goal. As long as people rely on mathematical complexity, the strong cryptography is still the most efficient tool to safeguard computer security. The immediate or significant arguments against this idea have not yet come forward.

B) Firewall

A firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defense mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. There are basically two different types of firewalls packet filters and proxies. Packet filtering firewalls are those designed to filter IP addresses, MAC addresses, TCP or UDP ports, and subnets, among others. A packet filter is, in principle, a router with the ability to filter or block traffic to and from a network. Packets to a specific service can also be blocked. IP packets to a computer on an internal network with certain options turned on or off could also be screened. Information on the TCP/IP level is used to decide whether to allow or disallow a particular type of traffic. Packet filtering firewalls look at each packet header entering or leaving the network and accept or reject a particular packet based on specific rules defined by the user/network administrator. Packet filtering is fairly effective and transparent to users. They, however, are difficult to configure and are also susceptible to IP spoofing a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. Proxy servers, on the other hand, intercept all the messages entering and leaving the network but it differs in that the proxy hides IP addresses of the clients in the internal network.

C) Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure to firewalls, virus scanners, and encryption that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. Attacks can take many forms, as previously discussed. Attack can occur through applications such as Netscape, Internet Explorer, Eudora, or Microsoft Outlook and also via the operating system, regardless of whether it is UNIX, Windows or Mac-based. You also can be attacked via the network through Denial of Service (DoS) attacks or attacks against protocols (Householder, 2000). IDS products are used to monitor connection in determining whether attacks are been launched. Everything from a simple port scan to a full attack against your Web server can be detected by the IDS system. A flag is raised when an attack is suspected. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. Software and hardware designed to detect attackers can pick up many levels of intrusions. IDSs will not be capable of detecting certain things, such as information about ISP and IP address range. Public information doesn't really affect the system until the attackers begin to ping the system to see if it is alive. These techniques are used for reconnaissance and mapping out potential targets.

D) Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so called anti-Malware tools are used to detect them and cure an infected system. This type of tool acts as an internal defense mechanism. The most common type of anti-Malware software is virus scanners. These tools often consist of two different but related parts: a scanner (or verifier) and a disinfector. Vulnerability scanners are special tools designed to automatically find vulnerabilities in systems.

E) Internet Protocol Security (IPSec)

The technology that brings secure communications to the Internet Protocol (IP) is called Internet Protocol Security (IPSec). The architecture for IPSec compliant systems is defined in RFC 2401 (Security Architecture for the Internet Protocol) by the Network Working Group of the IETF. The RFC 2401 defines

IPSec as a framework that provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithms(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPSec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPSec can be used in two modes, namely transport mode and tunnel modes. IPSec is a collection of open standards that work together to establish data confidentiality, data integrity and authentication between peer devices.

F) Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that actually uses many different standards of key exchange, authentication and encryption to get its job done. The server typically provides regular web service http on port 80, and SSL-encrypted web traffic https over port 443. SSL is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL is a good choice for adding end-to-end protection to applications, it protects against eavesdropping, session hijacking and Trojan servers. SSL can be applied to online security and privacy that provide authentication, integrity, confidentiality and Non-repudiation. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

VII. EMAIL SECURITY

Email infrastructures from outside threats including spam, phishing, unpredictable email volumes, malware and other form of objectionable or dangerous content before they hit the enterprise. Key capabilities within Proof point Enterprise Protection include

A) Threat detection

Powered by a machine learning technology, Proofpoint MLX™, and global reputation, Proofpoint email threat detection examines millions of possible attributes in every email—including message envelope headers and structure, images, sender reputation as well as unstructured content in the message body—to block phishing and spear phishing attacks, spam and other forms of malicious or objectionable content. Sophisticated policy and routing control ensure security and effective management of all classifications of content.

B) Virus protection

Effectively and efficiently combats viruses, worms, Trojans and other forms of malware with an industry□leading email threat management solution that combines efficient message handling, comprehensive reporting, and robust policy management with the world's leading anti□virus engines.

E) Zero-hour phish and anti-virus

Protects enterprises against new phishing attacks, viruses and other forms of malicious code during the critical first minutes after new attacks are released and before full information is available to characterize the threat.

D) Smsrt Search

Offers easy, real□time visibility into message flows across an organization's entire messaging infrastructure, using built-in logging and reporting capabilities coupled with advanced message tracing, forensics and log analysis capabilities.

VIII. CONCLUSIONS

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Security is critical and must be ensured so that Internet users can have confidence engaging in activities on the Internet. This paper presents a security solution for Internet security. In the nearest future new security technology will be developed to further improve the efficiency of business and communications.

IX. ACKNOWLEDGMENT

We thank all the faculty members of Department of CSE and ECE for valuable suggestions on the Evolution Security Attacks and Security Technology. We also thank the reviewers for valuable feedback

X. REFERENCES

[1]Mahesh Balakrishnan, Tudor Marian, Kenneth P. Birman, Fellow, ACM, Hakim Weatherspoon, and Lakshmi Ganesh " Maelstrom Transparent Error Correction for Communication Between Data Centers.pdf" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 19, NO. 3, JUNE 2011
[2] Isern, G. Internet Security Attacks at the Basic Levels ACM SIGOPS Operating Systems Review, 32(2):4–15,2002.
[3] Bishop, M. Taxonomy of (UNIX) System and Network Vulnerabilities. Technical Report CSE9510, Department of Computer Science, University of California at Davis, May 1995.
[4] Wenliang, D. Categorization of software errors that led to security breaches Proceedings of the 21st National Information Systems Security Conference (NISSC'98), 1998,
[5] Frantzen, M. A framework for understanding vulnerabilities in firewalls using a dataflow model of firewall internals, Computers and Security, vol. 20, no. 3, pp., May 2001.
[6] Summers, S. 2002. "Secure Computing Threats and Safeguards." McGraw-Hill
[7] Kemmerer, R and Vigna, G. January 2002. Security & Privacy: "Intrusion Detection: A Brief History and Overview." IEEE Computer Society
[8] Householder, A, January 2002. Security & Privacy: "Computer Attack Trends Challenge Internet Security." IEEE Computer Society
[9] Zwicky, E, 2000, Internet and Web Security: Building Internet Firewalls, O'Reilly, Beijing, 869pp
[10] S. Kent and R. Atkinson, "Security architecture for the internet protocol," RFC 2401, Internet Engineering Task Force, Nov. 1998
[11] Howard, J and Longstaff, T. A Common Language for Computer Security Incidents Technical report, Sandia National Laboratories, 1998.

AUTHOR'S PROFILE:

Konakalla Ankalarao Received his B.Tech and M.Tech degree's in Computer Science Engineering from Juwaharlal Nehru Technological University, Hyderabad, India. Preasently Working as an Assistant Professor in the dept. of Computer Science Engineering at Anurag Engineering College(AEC),Kodad. He is having 2+ years of experience; his research interests include Information Security, Network Security, Data Mining and Cloud Computing.
E-Mail: konakalla.ankalarao@anurag.ac.in
Ph. No: +91-8498993331

Bhavani Veeranki Received her Diploma in Electronics and Communication Engineering at State Board of Technical Education And Training India. Preasently Pursuing her B.Tech degree in Electronics and Communication Engineering at Anurag Engineering College(AEC),Kodad; her research interests include VLSI, Embedded Systems, Information Security and Network Security.
E-Mail: Bhavaniece115@gmail.com
Ph. No: +91-8790469955.

