Cybercrime Cases Analysis: Threat and Vulnerability

Dr.P.B.Pathak

Assistant Professor & Head, Department of Computer Science & Information Technology

Yeshwant Mahavidyalaya Nanded

Abstract— **Computers play a very important role in our life and this importance is ever increasing. There is an urgent need to safeguard the Integrity, Confidentiality, Availability, Reliability and Security of Computer Systems and Networks. Threats to Cybersecurity include Misconfigurations of Computer Systems, Poor User and Administrator Education, Poor Software Design, Network and System Design Issues, Substandard Operational Procedures, Use of Insecure Protocols, Weak Passwords, and finally, Lack of Awareness & Indifference. Vulnerability in a system is a potential weak point in the system that can be accidentally or intentionally exploited to harm the system.**

Index Terms— **Cybercrime, Threat, Vulnerability, Analysis, Cybersecurity**

I. Introduction

An effective Cybersecurity strategy must recognize that the security of the network of information systems that comprise the Internet requires a partnership between government and industry. Both the telecommunications and information technology industries and the governments seeking cost effective comprehensive Cybersecurity solutions. Security capabilities in computer products are crucial to the overall Network Security. However, as more technologies arrive and are integrated into existing networks, their compatibility and interoperability or the lack thereof will determine their effectiveness. Security must be developed in a manner that promotes the interweaving of acceptable security capabilities with the overall network architecture. To achieve such integrated, technology based cybersecurity solutions, network security should be designed around international standards developed in an open process.[1,10]

II. Threat

Threat may be from some categories like Networking threat that are related to the introduction and deployment of new Network technologies, but it also covers emerging threats against infrastructure services like routing, DNS on the current Internet. Hardware and virtualization threats are due to new hardware and software developments that allow computation to be moved to virtual computers and due to malicious hardware. Weak devices threat due to weak devices that are introduced with new computing devices. Complexity threat is due to complex systems. The increased complexity leads to unexpected and unintended dependencies, interactions, and security consequences. Data Manipulation threat stem from the online stored data. This data is becoming increasingly valuable and sensitive. Attack infrastructure threat due to adversaries which actively develop and deploy offensive platforms. Adversaries establish operational bases on the Internet used to carry out malicious campaigns. Human factors threat like insider attacks, social engineering attacks. Insufficient security requirements threat related to legacy and commercial systems without sufficient protection.[2,9]

Threat Defined: Threat can be defined as:

- ➢ A threat is the potential for one or more unwanted consequences caused by a circumstance, capability, action, or event that could be harmful to a system or person. Threats can be caused naturally, accidentally or intentionally. In essence, a threat is a ubiquitous phenomenon.
- ➢ A threat to a computer system can be defined as any potential occurrence, malicious or otherwise, that can have an undesirable effect on the assets and resources associated with a computer system.
- ➢ A threat is the presence of dangerous or adverse circumstances or events with the potential to impact operations, assets, or individuals via disclosure, modification, destruction, or disruption of service.
- ➢ *Motivation of Threat:* The motivations for an attack gives some insight about which areas of the network are vulnerable and what actions an intruder will most likely take. In many cases, the attacks occur from the external Internet. Therefore, a firewall between the Internet and the trusted corporate network is a key element in limiting where the attacks can originate. Firewalls are important elements in network security, but securing a

Manuscript received Feb, 2016.
***Dr.P.B.Pathak**, Assistant Professor & Head,*
Department of Computer Science & Information Technology
,Yeshwant Mahavidyalaya Nanded Maharashtra, India

network requires looking at the entire system as a whole. Some of the common motivations for attacks are Greed, Prank, Notoriety, Revenge, and Ignorance.

- Greed: The intruder is hired by someone to break into a corporate network to steal or alter information for the exchange of large sums of money.
- Prank: The intruder is bored and computer savvy and tries to gain access to any interesting sites.
- Notoriety: The intruder is very computer savvy and tries to break into known hard to penetrate areas to prove his competence. Success in an attack can then gain the intruder the respect and acceptance of his peers.
- Revenge: The intruder has been laid off, fired, demoted, or in some way treated unfairly. The more common of these kinds of attacks result in damaging valuable information or causing disruption of services.
- Ignorance: The intruder is learning about computers and networking and stumbles on some weakness, possibly causing harm by destroying data or performing an illegal act.

Types of Threats: Threat classification may be based on some factors like Impact describes how many users are affected and what damage level is to be expected, Likelihood captures the expected probability that a threat in question is actually carried out, Obliviousness captures the lack of awareness of the public and the research community for a threat, Research and Development (R&D) Needs captures the extent to which new R&D efforts are needed to mitigate a threat. [3,8]

One way of threat classification may be as attacks against the infrastructure of the Internet, Denial of service attacks, attacks against the confidentiality or integrity, both on wired and wireless links. Thus many different types of threats exist they fall into four basic categories: Unauthorized Access, Impersonation, Denial of Service and Human Error Threats.[149]

Unauthorized Access: Unauthorized access is, when an unauthorized entity gains access to an asset and has the possibility to tamper with that asset. Gaining access is usually the result of intercepting some information in transit over an insecure channel or exploiting an inherent weakness in a technology or a product. Getting access to Computer Network resources is usually accomplished by doing some reconnaissance work. Most likely, the corporate network will be accessed through the Internet, tapping into the physical wire, remote modem dial in access, or wireless network access. Also, a very common component to reconnaissance work is social engineering of information.

If an intruder is trying to gain unauthorized access via the Internet, he must do some information gathering work to first figure out which networks or resources are susceptible to vulnerabilities. Some common methods used to identify potential targets are: A reachability check, Port scanning, Tapping into the Physical Wire, Remote Dial-In Access, Wireless Access, and Social Engineering.[4,7]

- A Reachability Check: A reachability check uses tools that verify that a given network or device exists and is reachable.
- Port Scanning: When live systems are discovered, an attacker will usually attempt to discover which services are available for exploitation. This is accomplished by a technique commonly known as Port Scanning.
- Tapping into the Physical Wire: The ease or difficulty of packet snooping also known as Eavesdropping on networks depends largely on the technology implemented. Shared media networks are particularly susceptible to eavesdropping because this type of network transmits packets everywhere along the network as they travel from the origin to the final destination.
- Remote Dial in Access: There are still people out there, who use well known exploits, such as war dialing, to gain unauthorized access. War dialing is using an automated machine for dialing a set of phone lines to find accessible modems. All the attacker has to do is find a user within the organization with an open connection through a modem unknown to the IT staff or a modem that has minimal or, at worst, no security services enabled.
- Wireless Access: Wireless Networks are especially susceptible to unauthorized access. Wireless access points are being widely deployed in corporate LANs because they easily extend connectivity to corporate users without the time and expense of installing wiring.
- Social Engineering: Social Engineering refers to methods to trick or manipulate people into providing sensitive information or performing a task. These non network based techniques are the practice of obtaining confidential information by manipulating users. A social engineer fools a person into revealing sensitive information or getting them to do something that is against typical policies, using their innocence. Social Engineering is made possible because the weakest link of the security chain is the human factor.

Impersonation: Impersonation is the ability to present credentials as if you are something or someone you are not. In large corporate networks, impersonation can be devastating because it bypasses the trust relationships created for structured authorized access. Impersonation attacks are commonly referred to as man in the middle attacks, where an intruder is able to intercept traffic and can as a result hijack an existing session, alter the transmitted data, or inject bogus traffic into the network.

Impersonation can take several forms: Impersonation of Individuals, Impersonation of Devices and Stealing a Private key or recording an authorization sequence to replay at a later time.

- Impersonation of Individuals: Impersonation of individuals is common. Most of these scenarios pertain to gaining access to authentication sequences and then using this information to obtain unauthorized access. Once the access is obtained, the damage created depends on the intruder's motives. With the aid of cryptographic authentication mechanisms, impersonation attacks can be prevented. An added benefit of these authentication mechanisms is that, in some cases, nonrepudiation is also achieved. A user participating in an electronic communication exchange cannot later falsely deny having sent a message. This verification is critical for situations involving electronic financial transactions or electronic contractual agreements because these are the areas in which people most often try to deny involvement in illegal practices.

- Impersonation of Devices: Impersonation of devices is largely an issue of sending data packets that are believed to be valid but that may have been spoofed. Typically, this attack causes unwanted behavior in the network. Impersonation can be deterred to some degree by using authentication and integrity security services such as digital signatures. A digital signature confirms the identity of the sender and the integrity of the contents of the data being sent.
- Stealing a Private key / Packet Spoofing and Replay: Impersonation can come about from packet spoofing and replay attacks. Spoofing attacks involve providing false information about a principal's identity to obtain unauthorized access to systems and their services. A replay attack can be a kind of spoofing attack because messages are recorded and later sent again, usually to exploit flaws in authentication schemes. Both spoofing and replay attacks are usually a result of information gained from eavesdropping. Many packet snooping programs also have packet generating capabilities that can capture data packets and then later replay them.

Denial of Service: Denial of Service is an interruption of service either because the system is destroyed or because it is temporarily unavailable. Examples include destroying a computer's hard disk, severing the physical infrastructure, and using up all available memory on a resource. Many common DoS attacks are instigated from network protocols such as IP.[11]

Common Denial of Service Attacks are:

- TCP SYN attack- Memory is allocated for TCP connections such that not enough memory is left for other functions.
- Ping of Death- Fragmentation implementation of IP whereby large packets are reassembled and can cause machines to crash.
- Land.c Attack -TCP connection establishment.
- Teardrop.c Attack- Fragmentation implementation of IP whereby reassembly problems can cause machines to crash.
- Smurf Attack- Flooding networks with broadcast traffic (ICMP echo requests) such that the network is congested.
- Fraggle Attack- Flooding networks with broadcast traffic (UDP echo requests) such that the network is congested.
- Distributed Denial of Service (DDoS): A variant of a DoS attack has caused even more problems. This is the DDoS attack, where multiple machines are used to launch a DoS attack. The DDoS client is used by the person who orchestrates an attack as the initial starting point. The handler is a compromised host with a special program running on it. Each handler is capable of controlling multiple agents. An agent is a compromised host that is also running a special program. Each agent is responsible for generating a stream of packets that is directed toward the intended victim.

Thus this is a DoS attack, but performed using multiple computers, which then focus the malicious traffic on a victim server, consuming its bandwidth. In most cases, these computers are controlled remotely by hackers and are connected in so called Botnets. Such computers are also called Zombies.[5]

Human Error Threat: There exit numerous human error threats:

Equipment Loss, Miscommunication, Implementation Error, Malfunction Threats, Software Malfunction, Hardware Malfunction, Process Malfunction, Power Disruption, Malicious Threats, Physical break in, Eavesdropping, Malicious Authorized User, Equipment Theft, Social Engineering, Malware that requires user interaction, Malicious Scan, Malicious Unauthorized User, Self Replicating Malware, Process Violation, Environmental Threats, Lightning, Damaging Wind, Temperature or Humidity Extremes, Electronic Emanation/Electromagnetic Pulse, Hazardous Materials, Fire, Flood and Power Surge.[12]

III. VULNERABILITY

In identifying the likelihood of a potential risk, one must consider sources from which threats can arise, potential weakness of the system, and existing controls in the system. The global presence, explosive growth and open access of the Internet and modern communications technology have dramatically increased the vulnerability.

A successful cyber attack requires finding only one vulnerability, whereas a successful cyber defense requires finding all possible vulnerabilities. [13]

Criminal behavior on the Internet is fuelled by the ability to purchase web vulnerability kits and customize them for your exploits. Our reliance on computers and information based technologies has greatly increased potential for vulnerability if information systems are attacked. The vulnerability of the critical infrastructure has led to increasing concern that it will be the target of terrorist attacks.[6]

Vulnerability Defined: Vulnerability can be defined variously as:

- Vulnerability is a flaw or weakness in a system's design, its implementation, or operation and management that could be exploited to violate the system and, consequently, cause a threat. Vulnerabilities may have different dimensions: technical, functional or behavioral.
- A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth that could be exploited by a threat to gain unauthorized access information or disrupt critical processing i.e. a weakness in a system allowing unauthorized action.
- Any information system weakness or flaw attributed to individuals, assets, or operations that make them susceptible to exploitation.
- Vulnerability is a weakness in a system, such as a coding bug or a design flaw.
- Any product flaw, administrative process or act that makes a computer susceptible to attack.
- Any flaw or weakness in the network defense that could be exploited to gain unauthorized access to, damage or otherwise affect the network.
- A flaw or weakness in the design or implementation of hardware, software, networks, or computer based systems including security procedures and controls associated with the systems.
- A weakness that allows specific threats to compromise computer systems.
- A weakness in the hardware, software, or security that leaves a system or network open to threat of unauthorized access or damage or destruction of data.

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited by a threat to violate the system's security policy.

IV. Conclusion

To protect a network's resources from theft, damage, or unwanted exposure, administrators must understand who initiates these things, why, and how they do it. Knowledge will make you, and better able to track down and prosecute unauthorized intruders and attackers. Security is freedom from risk or danger. Organizations should impose controls aimed at mitigating functional areas of vulnerability at each interface point. The functional areas of vulnerability are Identification and Authentication, Access Control, Accountability, Object Reuse, Accuracy, Reliability of Service.

REFERENCES

[1] "Network Security." Wayne State University Medical School Information Systems, http://www.med.wayne.edu

[2] Bluefire Security Technologies. (2003) "Mobile insecurity: A practical guide to threats and vulnerabilities." http://www.bluefiresecurity.com

[3] E.Schultz , R.Shumway "Incident Response: A Strategic Guide To Handling Systems And Network Security Breaches"

[4] Australian Computer Emergency Response Team, (2004), "Computer Crime and Security Survey", Queensland University, Brisbane, Australia.

[5] Berger M.A. (2003), "Password Security is a Must for Any Organization", Computers in Libraries

[6] Clark R (2004) "Message Transmission Security" http://www.anu.edu.au

[7] Kunene G. (2004) "XML Standards Provide Web Services Security." http://www.devx.com

[8] Lange L. (2003) "Web Services Security Gets Serious." http://www.techweb.com

[9] Baker W. H. & Wallace L. (2007) "Is information security under control?" IEEE Security & Privacy.

[10] Cisco (2008) "Small and medium business security." http://www.cisco.com

[11] Microsoft. (2007) "Security Guidance Center." http://www.microsoft.com

[12] W. Jansen and K. Scarfone (2008.) "Computer security, guidelines on cell phone and PDA security." Technical report, NIST- National Institue of standards and Technology, US Department of Comerce. Special Publication

[13] Yan Zhang, Jun Zheng, and Miao Ma.(2008)" Handbook of Research on Wireless Security." Idea Group Inc (IGI)