# Study on prediction of Network Security: Ethics and Privacy

**Parveen Kumar**
*Assistant Professor, SPN College Mukerian*
*parveenspn20@gmail.com*

***Abstract*- Network security refers to protecting the websites domains or servers from various forms of attack. Network security is important in every field of today's world such as military, government and even in our daily lives. Having the knowledge of how the attacks are executed we can better protect ourselves. The architecture of the network can be modified to prevent these attacks, many companies use firewall and various polices to protect themselves. Network security has a very vast field which was developed in stages and as of today, it is still in evolutionary stage. To understand the current research being done, one must understand its background and must have knowledge of the working of the internet, its vulnerabilities and the methods which can be used to initiate attacks on the system.**

***Keywords*: DOS attacks, Firewalls, Encryption, Port Scanning, SSL, SHTTP, VPN.**

## I. INTRODUCTION

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. A specialized field in computer networking that involves securing a computer network infrastructure. Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work.

A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network[1].

A computer security risk is any action that could cause lost of information, software, data, processing incompatibilities, or cause damage to computer hardware, a lot of these are planned to do damage. An intentional breach in computer security is known as a computer crime which is slightly different from a cybercrime.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

## II. Need of security of computer network

Security assessment of computer network security is based on the analysis of users' computer network system. Main functions are monitoring whether there are mutations in computer network system and software. It requires a convenient, flexible and complete model to process the analyzation to avoid the complexity of space system[2].

The need of security of computer network is to fulfill users' requirements of computer network's integrity and confidentiality during the usage of computer network. Through a complete systematical security strategy, computer security is insured. The strategy of security of computer network's usage can help computer system to judge users' process of usage to prevent unknown attack. It can also insure the system's main movements could reach the requirements of computer network security. With different computer usage, the need of computer security nature could be divided into different risk level based on the use, in order to protect the security of computer network and analyze specific security feature based on specific requirements. In practical use, computer confidentiality risk levels are shown in table 1.

 

TABLE I

Confidential risk rating scale

| Classification | Feature description |
|---|---|
| C1 | Show host availability |
| C2 | Gets a OS type and version number |
| C3 | Gets the application and version information |
| C4 | Existence of detecting objects in the target host. |
| C5 | Read some user specific information |
| C6 | Read more ordinary user files |
| C7 | Read a certain privileged documents or kernel system processes spatial content |
| C8 | Read arbitrary files or system privilege configuration file content monitoringnetwork activity |

From the table, we can see that every level are rather separated but also connected to each other. Every level could be regarded as a kind of users' requirements of computer security. This is the separated part. They do not conflict each other. When unknown personnel attack the computer, after the security feature is destroyed, other risks would appear. Different levels of security vulnerability would influence the occurrence of risks. That's where they are connected.

## III. DIFFERENT TYPES OF SECURITY ATTACKS [3]

### *A. Passive Attacks*

This type of attacks includes attempts to break the system using observed data. One of its examples is plain text attack, where both the plain text and cipher text are already known to the attacker. Properties of passive attacks are as follows:

• *Interception*: The data passing through a network can be easily sniffed and thus attacking the confidentiality of the user, such as eavesdropping, "Man in the middle" attacks

• *Traffic analysis*: Also attacks confidentiality. It can include trace back on a network like a CRT radiation.

### *B. Active Attacks*

**1) *Man in the middle attack***

This is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Man-in-the-middle attacks can be thought about through a chess analogy. Mallory, who barely knows how to play chess, claims that she can play two grandmasters simultaneously and either win one game or draw both. She waits for the first grandmaster to make a move and then makes this same move against the second grandmaster. When the second grandmaster responds, Mallory makes the same play against the first. She plays the entire game this way and cannot lose. A man-in-the-middle attack is a similar strategy and can be used against many cryptographic protocols. One example of man-in-the-middle attacks is 2)Active eavesdropping: It is the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle

In this attack the attacker sends data stream to one or both the parties involved or he can also completely cut off the data stream. Its attributes are as follows:

• Interruption: It prevents an authenticated user form accessing the site. It attacks availability. Such as DOS attacks.

• Modification**:** In this the data is modified mostly during transmission. It attacks integrity.

• Fabrication: Creating counterfeit items on a network without proper authorization. It attacks authentication.


**Fig1: Different types of attack**

### *C. NETWORK ATTACK :*

1) *Packet Sniffing Attack:* It is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

### D. DOS Attack

DOS attacks [7] today have become a major threat to network security all over the world. They can be easily launched by anyone with the basic knowledge of network security. They don't require as much time and planning as some other attacks, in short they are cheap and efficient method of attacking networks. They can shutdown the company network by overflowing it with requests and thus affect availability of the network. With the help of easy to use network tools such as Trinoo, which can be easily downloaded of the internet any normal user can initiate an attack on DOS attacks usually works by exhausting the targeted network

 

of bandwidth, TCP connections buffer, application/service buffer, CPU cycles, etc. DOS attacks use many users connected to a network known as zombies most of the time users are unaware of that their computer is infected.

**(E) WEB ATTACK**

***1) Phishing***

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The word is neologism created as homophone of *fishing* due to the similarity of using a bait in an attempt to catch a victim. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and users should not use the same passwords anywhere on the internet.

***2) SQL Injection:***

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is It is not strongly typed and unexpectedly injection SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation

**(III)Virus/Worm/Trojan**

**A. *Virus***

A computer virus[8] is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, logging their keystrokes, or even rendering the computer useless. However not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without user consent. Virus writers use social engineering and exploit detailed knowledge of security vulnerabilities to gain access to their hosts' computing resources. The vast majority of viruses target systems running Microsoft Windows, employing a variety of mechanisms to infect new hosts, and often using complex anti-detection/stealth strategies to evade antivirus software. Motives for creating viruses can include seeking profit, desire to send a political message, personal amusement, to demonstrate that a vulnerability exists in software, for sabotage and denial of service, or simply because they wish to explore artificial life and evolutionary algorithms.

**B.*WORM***

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.


**Fig2: The basic working of worms**

Worms spread by exploiting vulnerabilities in operating systems. Vendors with security problems supply regular security updates and if these are installed to a machine then the majority of worms are unable to spread to it. If vulnerability is disclosed before the security patch released by the vendor, a zero-day attack is possible. Users need to be wary of opening unexpected email, and should not run attached files or programs, or visit web sites that are linked to such emails.

**C. TROJAN HORSE:**

Trojan House any malicious computer program which misrepresents itself to appear useful, routine, or interesting in order to persuade a victim to install it.


**Fig3: Trojan Horse Virus**

C Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by drive-by download. Although their payload can be anything, many moderns' forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage.

## (IV)Types of Password Hack

### A. *Password Guessing*

Password guessing [9] is a technique used by attackers to crack passwords. Attackers generally used a dictionary-based password guessing attack to take the easy way. Hybrid attacks have been more successful in most cases, as it is both faster and less complicated. In the worst case scenario, a brute force attack is used. It is both time consuming and complicated.


**Fig4: Password guessing method**

Password guessing is very fast in cases where users have chosen to use default passwords. Dictionary-based attacks are much faster when users have chosen English text as passwords. In cases where users have used simple text and numbers such as "devine123", hybrid attacks come into play. In cases where users have more complicated passwords such as "John! Smith120", a brute force attack might be a choice of the attackers. This is not always the case and it varies on a case by case basis. Brute force attacks are faster than the other two types in some cases.

### B. *Dictionary Attacks*

A dictionary attack is a technique or method used to breach the computer security of a password-protected machine or server. A dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password or trying to determine the decryption key of an encrypted message or document. Dictionary attacks are often successful because many users and businesses use ordinary words as passwords. These ordinary words are easily found in a dictionary, such as an English dictionary.


**Fig5: A dictionary Attack**

Two countermeasures against dictionary attacks include:

1. Delayed Response: A slightly delayed response from the server prevents a hacker or spammer from checking multiple passwords within a short period of time.
2. Account Locking: Locking an account after several unsuccessful attempts (for example, automatic locking after three or five unsuccessful attempts) prevents a hacker or spammer from checking multiple passwords to log in.

Dictionary attacks are not effective against systems that make use of multiple-word passwords, and also fail against systems that use random permutations of lowercase and uppercase letters combined with numerals.

C. *Key logger attack* - A key logger is any piece of software or hardware that has the capability to intercept and record input from the keyboard of a compromised machine. The keylogger often has the ability to sit between the keyboard and the operating system and intercept all of the communications without the user's knowledge. The key logger can either store the recorded data locally on the compromised machine or, if it's implemented as part of a larger attack toolkit with external communication capabilities, sent off to a remote PC controlled by the attacker. Although the term key logger typically is used in relation to malicious tools, there are legitimate surveillance tools used by law enforcement agencies that have key logging capabilities, as well.

**Fig6. A key logger Attack**

Although the term key logger typically is used in relation to malicious tools, there are legitimate surveillance tools used by law enforcement agencies that have key logging capabilities, as well.

### (V) Architecture of Network Security

The Basic architecture [5] provides IT services in an open networking environment and should be ready to handle Internet threats (i.e., hackers, malicious code, DoS attacks). They deploy a multi-tier network security architecture consisting of Web, application, and database server zones and appropriate security layers. Today the Internet provides standard access for most e-commerce applications, e-banking, and data centers. It is convenient and cost-effective because geographically distributed users do not need to install, configure, and upgrade any client application. Figure 7 shows an network security architecture. The zones construction is relevant to the functional elements

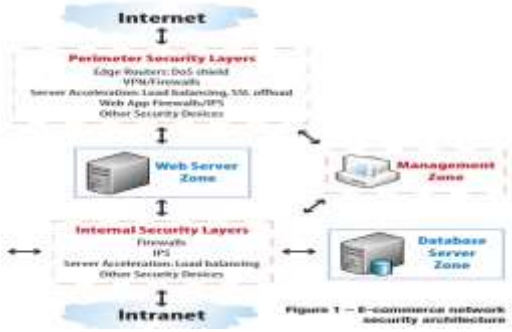


**Fig7. The basic Architecture of Network Security**

the Web servers are responsible for interaction with the users, the application servers perform data processing, and the database servers provide data storage. The servers of the same type (e.g., Web servers) that provide different e-commerce services should be separated and located in different zones. A dedicated security zone is also created for the management systems.

The security layers are divided into at least two groups – perimeter and internal. Perimeter security layers usually consist of edge routers providing first line of DoS protection and dedicated security devices (i.e., network firewall, data encryption-VPN, intrusion prevention system-IPS, web application firewall-WAF) as well as server-acceleration devices (i.e., load balancing, SSL offload). For effective attack prevention, it is important to perform SSL offload before IPS and WAF inspection.

### (VI)Virtual server protection

Virtual servers are commonly used in IT systems and e-commerce. Consolidation of many servers on one hardware platform provides a cost savings. However, it is important to note that servers in virtualized environment like VMware ESX are vulnerable to the same threats as physical servers (i.e., hacking, malicious code, DoS). E-commerce systems that utilize virtual servers also require appropriate network security architecture, i.e., the security zones and layers. Additionally the safeguards should be ready to handle the attacks specific for the virtualized environment (e.g., vmkernel**).** See Figure 8(I,II).

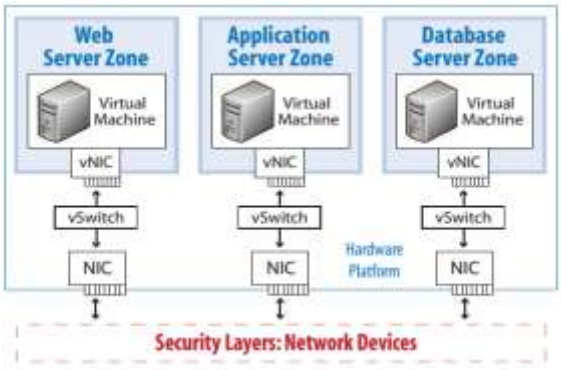


**Fig 8(I). Security layers implemented on network devices**

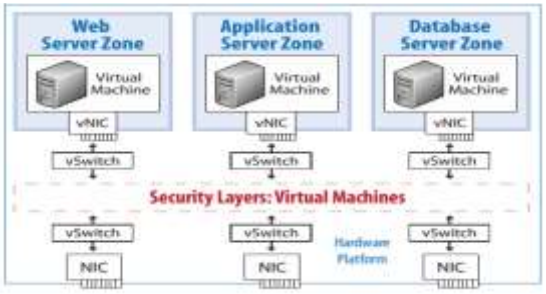


**fig8(II). Concepts of network security architectures in virtualized environment**

Virtual servers of different security zones can be separated on dedicated virtual switches (vSwitch) and network interfaces(NIC), or share the same vSwitches and NICs and be separated using VLANs (802.1q). The security zones are created in similar ways as in physical networks. The security layers can be implemented in two ways, i.e., using the network security devices or the safeguards deployed as virtual machines. Figure 2 presents the concepts of network security architectures implemented in the virtualized environment.

### (VII)How can you achieve security?

Network security [6]consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network

 

security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security is manifested in an implementation of security policy hardware, and software. For the purposes of this discussion, the following approach is adopted in an effort to view network security in its entirety:

*A. Policy*

The IT Security Policy is the principle document for network security. Its goal is to outline the rules for ensuring the security of organizational assets. Employees today utilize several tools and applications to conduct business productively. Policy that is driven from the organization's culture supports these routines and focuses on the safe enablement of these tools to its employees. The enforcement and auditing procedures for any regulatory compliance an organization is required to meet must be mapped out in the policy as well.

*B. Enforcement*

Most definitions of network security are narrowed to the enforcement mechanism. Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and information on the network. These three principles compose the CIA triad:

- Confidentiality - involves the protection of assets from unauthorized entities
- Integrity - ensuring the modification of assets is handled in a specified and authorized manner
- Availability - a state of the system in which authorized users have continuous access to said assets.

Strong enforcement strives to provide CIA to network traffic flows. This begins with a classification of traffic flows by application, user, and content. As the vehicle for content, all applications must first be identified by the firewall regardless of port, protocol, evasive tactic, or SSL. Proper application identification allows for full visibility of the content it carries. Policy management can be simplified by identifying applications and mapping their use to a user identity while inspecting the content at all times for the preservation of CIA.

The concept of defense in depth is observed as a best practice in network security, prescribing for the network to be secured in layers. These layers apply an assortment of security controls to sift out threats trying to enter the network:

- Access control
- Identification
- Authentication
- Malware detection
- Encryption
- File type filtering
- URL filtering
- Content filtering

These layers are built through the deployment of firewalls, intrusion prevention systems (IPS), and antivirus components. Among the components for enforcement, the firewall (an access control mechanism) is the foundation of network security.

Providing CIA of network traffic flows was difficult to accomplish with previous technologies. Traditional firewalls were plagued by controls that relied on port/protocol to identify applications—which have since developed evasive characteristics to bypass the controls—and the assumption that IP address equates to a users identity.

The next generation firewall retains an access control mission, but reengineers the technology; it observes all traffic across all ports, can classify applications and their content, and identifies employees as users. This enables access controls nuanced enough to enforce the IT security policy as it applies to each employee of the organization, with no compromise to security.

Additional services for layering network security to implement a defense in depth strategy 8have been incorporated to the traditional model as add-on components. Intrusion prevention systems (IPS) and antivirus, for example, are effective tools for scanning content and preventing malware attacks. However, organizations must be cautious of the complexity and cost that additional components may add to its network security, and more importantly, not depend on these additional components to do the core job of the firewall.

*C. Auditing*

The auditing process of network security requires checking back on enforcement measures to determine how well they have aligned with the security policy. Auditing encourages continuous improvement by requiring organizations to reflect on the implementation of their policy on a consistent basis. This gives organizations the opportunity to adjust their policy and enforcement strategy in areas of evolving need.

## (VIII) CONCLUSION

Secure networks are important for proper operation of IT systems as most applications work in the networking environment. An essential part of the network design is the security architecture that describes security zones and layers. An appropriate design of the network security architecture provides many advantages (e.g., isolation of low-trust systems, limitation of the security breach's scope, cost savings). When

 

designing the architecture to avoid the errors and achieve project cost-effectiveness, recognized principles should be taken into account (i.e., compartmentalization, defense in depth, adequate protection, etc.). There is not one standard architecture. Different IT systems have specific requirements that the network security architecture should fulfill. With the development of computer network technology, computer network security problems happen all the time. Therefore, people hold worries towards the development of computer network technology. Since computer network security influences people's life, researches to build a computer network security model must be continued.

## REFERENCES

[1] Huang Zhilong. Research on computer network security analysis model [J]. *Research on computer network security analysis model* , **2014**(05).

[2] Zhang Tao; Hu Mingzeng; Yun Xiaochun, Zhang Yongzheng. Research on computer network security analysis model [J]. *Journal of communications*, **2005**(12 ).

[3] Zhang Baoshi. Research on computer network security analysis model [J]. *Electronic technology and software engineering*, **2014**(04 ).

[4] Hong Yaling. On modeling of computer network security [J]. *Computer CD Software and Applications*, **2013**(02 ).

[5] Xv Liuwei. Modeling of computer network security [J]. *Computer CD Software and Applications*, **2013**(06 ).

[6] https://www.paloaltonetworks.com/documentation/glossary/what-is-network-securitv

**[7]** https://en.wikipedia.org/wiki/**Network securitv**

**[8]** https://www.paloalto**networks**.com/.../**what-is-network-security**.html

**[9]** www.cyberoam.com/**networksecurity**.html

 