# Study of Network Security and Possible Security Mechanisms

Sushma Laxman Wakchaure[1], Shailaja Dilip Pawar[2], Bipin Balu Shinde[3], Dipali Navnath Argade[4], Vijay Vitthal Thitme[5]

[1,2,3,4,5]Lecturer, Department of Computer Technology, Amrutvahini Polytechnic, Sangamner, India

***Abstract*****: Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. Security is a fundamental component in the computing and networking technology. The first and foremost thing of every network designing, planning, building, and operating a network is the importance of a strong security policy. Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are different kinds of attack that can be when sent across the network. By knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these required different security mechanisms. In this paper, we are trying to study most different kinds of attacks along with various different kinds of security mechanism that can be applied according to the need and architecture of the network. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed. For the first few decades of their existence, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem. The requirements of information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.with the introduction of computer the need for automated tools for protecting files and other information stored on the computer became an evident .this is especially the case for a shared system, such as time sharing system and the need is even more acute for systems that can be accessed for a public telephone or a data network. The generic name for the collection of tools to protect data from the hackers is "computer security".**

***Keywords*****: Network security, Accountability, Access control, Management policy, Cryptography, Attacks, Hackers, Cloud-environment security.**

## 1. Introduction

Network Security management is different for all kinds of situations and is necessary as the growing use of internet. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming [8]. The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet. The vast topic of network security is analyzed by researching the following:

1. History of security in networks
2. Internet architecture and vulnerable security aspects of the Internet
3. Types of internet attacks and security methods
4. Security for networks with internet access

5. Current development in network security hardware and software

Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand where network security is heading.

### *A. Network Security*

System and network technology is a key technology for a wide variety of applications. Security is crucial2 to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message. When developing a secure network, the following need to be considered:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. "Intranets" are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself. The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource's intended function
- To gain system knowledge that can be exploited in later attacks

The last reason for a network intrusion is most commonly guarded against and considered by most as the only intrusion motive. The other reasons mentioned need to be thwarted as well. Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. Current work is being performed in using a layered approach to secure network design. The layers of the security model correspond to the OSI model layers. This security approach leads to an effective and efficient design which circumvents some of the common security problems. protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key. When internet was created, the quality of service (QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text-based. As the internet expanded and technology evolved, other forms of communication began to be transmitted across the internet. The quality of service for streaming videos and music are much different than the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated.

## 2. Differentiating Data Security and Network Security

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Even if this unintelligible data is intercepted, a key is needed to decode the message. This method of security is effective to a certain degree. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well. When transferring cipher text over a network, it is helpful to have a secure network. This will allow for the cipher text to be protected, so that it is less likely for many people to even attempt to break the code. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack-hard networks. It can be seen that the cryptography occurs at the application layer; therefore, the application writers are aware of its existence. The user can possibly choose different methods of data security. Network security is mostly contained within the physical layer. Layers above the physical layer are also used to accomplish the network security required Authentication is performed on a layer above the physical layer. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent countermeasure strategies.

## 3. History of network security

Recent interest in security was fueled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in U.S. history. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies. Since then information security came into the spotlight. Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies are emphasizing security for the intellectual property. Internet has been a driving force for data security improvement. Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secure.

### 1) *Brief History of Internet*

The birth of the interne takes place in 1969 when Advanced Research Projects Agency Network (ARPANet) is commissioned by the department of defense (DOD) for research in networking. The ARPANET is a success from the very beginning. Although originally designed to allow scientists to share data and access remote computers, e-mail quickly becomes the most popular application. The ARPANET becomes a high-speed digital post office as people use it to collaborate on research projects and discuss topics of various interests. The Inter Networking Working Group becomes the first of several standards-setting entities to govern the growing network. Vinton Cerf is elected the first chairman of the INWG, and later becomes known as a "Father of the Internet." In the 1980s, Bob Kahn and Vinton Cerf are key members of a team that create TCP/IP, the common language of all Internet computers. For the first time the loose collection of networks which made up the ARPANET is seen as an "Internet", and the Internet as we know it today is born. The mid-80s marks a boom in the personal computer and super-minicomputer industries. The combination of inexpensive desktop machines and powerful, network-ready servers allows many companies to join the Internet for the first time. Corporations begin to use the Internet to communicate with each other and with their customers.

### 2) *Security Timeline*

Several key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s. Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II. In the 1960s, the term “hacker” is coined by a couple of Massachusetts Institute of Technology(MIT) students. The Department of Defense began the ARPANet, which gains popularity as a conduit for the electronic exchange of data and information. This paves the way for the creation of the carrier network known today as the Internet. During the 1970s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers. During the 1980s, the hackers and crimes relating to computers were beginning to emerge. The 414gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy's crime of stealing information from military computers. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to over 6,000 vulnerable computers connected to the Internet. Based on concerns that the Morris Worm ordeal could be replicated, the Computer Emergency Response Team (CERT) was created to alert computer users of network security issues.

## 4. Internet architecture and vulnerable security aspects

The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's best-known deficiencies, they seem to be insufficient. 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.

### 1) *IPv4 Architecture*

The protocol contains a couple aspects which caused problems with its use. These problems do not all relate to security. They are mentioned to gain a comprehensive understanding of the internet protocol and its shortcomings. The causes of problems with the protocol are:

1. Address Space
2. Routing
3. Configuration
4. Security
5. Quality of Service

The IPv4 architecture has an address that is 32 bits wide. This limits the maximum number of computers that can be connected to the internet. The 32-bit address provides for a maximum of two billions computers to be connected to the internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution. Routing is a problem for this protocol because the routing tables are constantly increasing in size. The maximum theoretical size of the global routing tables was 2.1 million entries. Methods have been adopted to reduce the number of entries in the routing table. This is helpful for a short period of time, but drastic change needs to be made to address this problem. The TCP/IP-based networking of IPv4 requires that the user supplies some data in order to configure a network. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can request appropriate network configuration from a central server. This eases configuration hassles for the user but not the network's administrators. The lack of embedded security within the IPv4 protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use. IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication. This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key. When internet was created, the quality of service (QoS) was standardized according to the information that was transferred across the network. The difficulties of staying up to date with security issues within the realm of IT education are due to the lack of current information. The recent research is focused on bringing quality security training combined with rapidly changing technology [4]. Online networking security is to provide a solid understanding of the main issues related to security in modern networked computer systems [5].

*2) IPv6 Architecture*

When IPv6 was being developed, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

1. Routing and addressing
2. Multi-protocol architecture
3. Security architecture
4. Traffic control

The IPv6 protocol's address space was extended by supporting 128 bit addresses. With 128 bit addresses, the protocol can support up to 3.4*(10)^38 machines. The address bits are used less efficiently in this protocol because it simplifies addressing configuration.7 The IPv6 routing system is more efficient and enables smaller global routing tables. The host configuration is also simplified. Hosts can automatically configure themselves. This new design allows ease of configuration for the user as well as network administrator. The security architecture of the IPv6 protocol is of great interest. IPsec is embedded within the IPv6 protocol. IPsec functionality is the same for IPv4 and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route. The quality of service problem is handled with IPv6.The internet protocol allows for special handling of certain packets with a higher quality of service. From a high-level view, the major benefits of IPv6 are its scalability and increased security. IPv6 also offers other interesting features that are beyond the scope of this paper. It must be emphasized that after researching IPv6 and its security features, it is not necessarily more secure than IPv4. The approach to security is only slightly better, not a radical improvement.

## 5. Common internet attack methods

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 consuming uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name.

*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.

*2) Viruses*

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

*3) 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. 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.

*4) 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.

*5) Phishing*

Phishing is an attempt to obtain confidential information from an individual, group, or organization. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

*6) 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.

*7) Denial of Service*

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

*8) Advanced Threat Protection with Big Data*

Big Data makes big sense for security as it involves using specialized technologies and techniques to collect, coordinate, store, and analyze truly massive amounts of related and perhaps even disparate data to uncover insights and patterns that would otherwise remain obscured. Leveraging Big Data for information security purposes not only makes sense but is necessary [9]. Big Data analytics can be leveraged to improve information security and situational awareness. For example, Big Data analytics can be employed to analyze financial transactions, log files, and network traffic to identify anomalies and suspicious activities, and to correlate multiple sources of information into a coherent view.

## 6. Technology for Internet Security

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defense and detection mechanisms were developed to deal with these attacks.

*1) Cryptographic systems*

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

*2) 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.

*3) Intrusion Detection Systems*

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

*4) 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.

*5) Secure Socket Layer (SSL)*

The Secure Socket Layer (SSL) is a suite of protocols that 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 provides authentication of clients to server through the use of certificates.

## 7. Current developments in network

### *A. Security*

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented. The research being performed assists in understanding current development and projecting the future developments of the field.

### *B. Hardware Developments*

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 undermining 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.

### *C. 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 order to create smarter security software.

## 8. Future trends in security

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Similarly, the network security will be able to function as an immune system. The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

## 9. Conclusion

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying Sumedha et al., International Journal of Advanced Research in Computer Science and Software Engineering computer network infrastructure, policies adopted by the network administrator to protect the network and the network accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network.

## References

[1] Simmonds, A; Sandilands, P; Van Ekert, L (2004) Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp. 317–323.

[2] A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

[3] Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

[4] Bhavya Daya, Network Security: History, Importance, and Future.

[5] Ateeq Ahmad, ―Type of Security Threats and its Prevention", Int. J. Computer Technology & Applications, Vol 3 (2), 750-752.

[6] Aameer Nadeem, M. Younus Javed, A performance comparison of data Encryption Algorithm, Global Telecommunication Workshops, 2004 Globe Com Workshops 2004, IEEE.

[7] Elkamchouchi, H. M; Emarah, A. A. M; Hagras, E. A. A, A New Secure Hash Dynamic Structure Algorithm (SHDSA) for Public Key Digital Signature Schemes‖, the 23rd National Radio Science Conference (NRSC 2006).

[8] Predictions and Trends for Information, Computer and Network Security http://www.sans.edu/research/security-laboratory/article/2140

[9] Cloud Security Alliance Big Data Analytics for Security Intelligence, https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Big_Data_Analytics_for_Security_Intelligence.pdf