Security Usage and Its Important for Network Using Case Study: \textit{US-Visit}

Meshal Al-Nasheet,\textsuperscript{1,a} Adel Al-Foudery,\textsuperscript{2,b}

\textsuperscript{1} The Higher Institute of Telecommunication and Navigation, PAAET, Kuwait
\textsuperscript{2} Computer Department, Basic Education College, PAAET, Kuwait

\textsuperscript{a} send4meshal@hotmail.com, \textsuperscript{b} adel_2004@yahoo.com

Abstract— with the evolution of Internet, security takes central role and its history provides a greater understanding of the emergence of security paradigms. In light of this, Internet itself enables several security threats to occur, but the web architecture, if modified, can mitigate the possibility of the attacks sent across networks. The knowledge of imminent hits allows for the emergence of security protocols. Notably, various businesses protect themselves from Internet threats through firewalls and encryption technologies. Firms can deploy intranets to connect seamlessly to the Internet, and at the same time, tenable from possible attacks. As Dowd and McHenry (1998) assert, the whole domain of network security is infinite and is in an evolutionary phase. The range of study comprises a succinct history rolling back to the development of the Internet and the current advancements of its security. To give a clear understanding of the research being performed today, background information of the Internet, its susceptibilities, attack mechanisms, and security protocols are reviewed in the research.

1. Introduction

The world connects seamlessly with the advent of the Internet and novel networking technologies. Because of the intellectual property available on-line, security becomes the issue of a great significance. Currently, two levels of networks exist: data and synchronous networks comprising switches. As the data network, the Internet is prone to attacks. Since present systems encompass computer-oriented routers, information is available through special programs, such as Trojan horses deployed in the routers. In that regard, data networks such as the Internet and other connections interfacing with it emphasize on security (Landwehr & Goldschlag, 1997). Synchronous network comprises switches, which do not buffer data and for that reason are not prone to attacks. People need the platforms of information sharing, but such information requires ultimate security assurance. Networks are the communication links that exist between the managers of an organization and the staff, the government and the public as well as military and other special units. Security is important because it manages an overall use, trust, reliability and the defense of information within the network. The paper discusses the two types of network security levels, together with many other related features like vulnerability of network to the attacks, the history of network security, provision of security for different networks and transitions in hardware and software security since its inception.
2. Background of Network Security

Many organizations, individuals, and governments still strive to establish credible network systems. Perfect network security is however not possible for organizations because new threats emerge each day making it impractical to develop foolproof systems to counter such risks. Many factors led to the introduction of network security in the late 1930s in Poland; this was twelve years before the first encoding of encrypted information. The fact that an organization could not access encrypted information raised fears concerning the inscrutability. Marin (2005) asserts that the process of encoding information made many people realize the importance of safety when handling sensitive materials. Security is important owing to the increasing cases of terrorism attacks across the globe. Terrorists also ensure their networks security to be successful in the operations. In the 1960s, information hacking became a major concern for the USA, Soviet Union and Japan, as each country sought the techniques of protecting information from adversaries during the Second World War. ARPANet was the first renowned network that enabled the exchange of information and security for transferred data in the US. The Department of Defense (DOD) realized that the greatest weapon for many attackers, terrorists, fraudsters, and ill-minded individuals was information. System hackers use information to exploit organizations and to find out minute details prior to launching attacks.

Ten years after the development of ARPANet, Telnet emerged, which offered sufficient data security in comparison to ARPANet. It was a big platform for communication between the residents of the US, the military, researchers and the government. In the same way that network developers tried to establish safe platforms of information sharing, network crimes threatened the survival of the attempts. Landwehr and Goldschlag (1997) indicated that in the 90s, Internet services became affordable and accessible to many people globally; this heightened network security in many companies, governments, and military operations. In the 20th and 21st centuries, organizations introduced the policies for managing networks and enhancing security. The introduction of firewalls, codes, and limited access to various sites was an indication that network security reached a high level of management.

3. Network Security

System and network security technologies are major implications deployed for an assortment of applications, making security a crucial aspect. Even though the security of networks is a critical prerequisite in emerging connections, there is a critical deficiency in deployable security protocols (Kartalopoulos, 2007). There is indeed, a communication fissure between the network developers and the developers of security technologies. As a well-articulated process, network design bases on the Open Systems Interface model, as it provides numerous benefits when developing networks. It offers flexibility, ease-of-use, modularity, as well as the standardization of protocols. Protocols at various layers can merge easily to form stacks, which allow modular deployment. In addition, the deployment of each layer is adaptable without effecting other adjustments and so introducing agility in development. In disparity to network design, building secure networks is not a well-extended process. Secure network design, though, does not encompass the same benefits as network design. While considering the issue, there must be the emphasis made that the entire network is secure. As Molva and Institut Eurecom (1999) observe, network security not only involves the security in the points at every end of the communication channel, but when transmitting data too. A potential hacker could seize the communication link, acquire the data, and decrypt it and re-insert distorted messages. Securing the network then, becomes as significant as
safeguarding the workstations and encrypting the messages. The following parameters are important when designing networks:

- **Access** – Authorized users acquire the means to communicate to and from a specific network.
- **Confidentiality** – Information within the networks remains undisclosed.
- **Authentication** – Ensures that the network users are who they claim to be.
- **Integrity** – Ensures that the messages on transit have not been modified.
- **Non-repudiation** – Ensures that users do not refute having used the network.

An efficient network security map incorporates the understanding of security parameters, potential threats, required security levels, and the factors of network vulnerabilities. This research endeavor accommodates threads involved in comprehending the symphony of a secure network, Internet or otherwise. To mitigate the susceptibility of a computer to the network, there are several tools available, for instance, data encryption, authentication, security-management, firewalls, and intrusion-detection mechanisms. Network invasions include the introduction of packets to inflict harms for the following reasons:

- To gain system information exploitable in subsequent attacks;
- To interfere with functioning system resources;
- To devour resources ineffectually.

Whereas the first reason mostly serves as the only motive for intrusion, network design should aim at thwarting for other reasons too. Typical security is presently placed in the computers forming a network connection, with the security protocols appearing as the elements of a single layer of the OSI reference model (SecurityOverview, n.d.).

![OSI Model](image)

**Fig. 1 show the OSL Model**

### 4. Internet Structural Design and Risk Areas of Networking

Fear of security violations on the Internet compels organizations to adopt the use of intranets or protected private networks. The Internet Engineering Task Force (IETF) has established security instruments at different layers of the Internet Protocol Suite. The analysis of the current and novel versions of the web protocol is inherent to establish various security implications (Serpanos & Voyiatzis, 2002). With such paradigms in place, these security procedures permit for the logical shielding of transmitted data units through the network. Though security could subsist within the protocol, certain threats are not preventable. IP Security and the Internet architecture security are the homogeneity of Internet security.
Upgraded and current versions of IP Security are IPv4 and IPv6 (Andress, 2005) respectively. Despite developing novel procedures, such as IPSec, to overcome security deficiencies on the Internet these security paradigms seem to be inadequate. The figure below shows the deployment of IPSec in providing protected communications. It is a point-to-point mechanism; one end encrypts, the other decrypts, with both ends sharing keys. IPSec is deployable in two modes: tunnel mode and transport mode.

Fig2. Showing IPSec deployment

5. Common Internet Attack Methods

Internet attacks fall in various groups. Some acquire personal information or system knowledge such as phishing and eavesdropping. Adeyinka (2008) denotes that attacks can also tamper with the system’s functionalities, such as worms, viruses, and Trojans. The other type involves consuming the system’s resources uselessly, caused by the denial of service attacks. Land, teardrop, and smurf attacks also exist; although, they are not known by the name as the denial of service attacks, they comprise intrusions of such nature

5.1 Viruses

These self-replication applications infect and propagate using computer files. On opening a file, the virus appears activated within the system. A virus developer manipulates normal information to increase user curiosity for a certain site.

5.2 IP Spoofing Attacks

Spoofing involves replicating the address of a trusted computer using another PC to permit the access to other computers. The identity of the attacker remains hidden through different methods making exposure and deterrence intricate. With present IP protocol technologies, the elimination of IP-spoofed packets is impossible.

5.3 Trojans
A Trojan often interferes with a user while opening a computer. Most users get them through Internet access. A Trojan sometimes creates an intention for a user to click on links, which are misleading. Accessing them leads to a virus replication in a computer.

5.4 Eavesdropping
It is the interception of communication by unauthorized parties. Active eavesdropping involves an intruder listening and inserting something into the communication medium. Passive eavesdropping, on the other hand, occurs when an attacker only listens secretly to the transmitted messages.

5.5 Worms
Worms affect computers and Internet services that make them worse in comparison to viruses. Normally, when downloading a document, a user notices the document has the sign of a worm and opening the information could infect the computer. On the Internet, many users have worms stored in the spam. This virus takes different forms when a user does not find a way to delete it from the computer and completely from the recycle bin. Mass mailing worms and network-aware ones operate differently, but affect computers and web consecutively.

5.6 Denial of Service
This attack occurs when a system obtains too many submissions to return communication with the requesting users, forcing the system to exhaust resources as it awaits the completion of the handshake (Simmonds, Sandilands & Van, 2004). Ultimately, the system rebuffs to respond to any more submissions, and so rendering it with no service. Many users experience the denial of service at some point of trying to access an account. For instance, in a single account an administrator can notice that more than one person try to get the right of entry. The administrator then denies the access to the second person who uses similar details to access the account. The real owner of the account cannot complain until the other user leaves the account.

6. Phishing
Phishing is a computer attack involving unauthorized access to confidential information from individuals, groups, or organizations. Phishers deceive users of a network into disclosing personal information, such as on-line banking credentials, personal data, and other critical information. Frauds and computer crimes that involve deception of an account owner amount to phishing. Similarly, terrorists, bank fraudsters, and on-line criminals use phishing to access user accounts.

7. Technology for Internet Security
As long as communication takes place across the Internet, intrusion threats will continue to pose serious concerns. Different detection and defense mechanisms are deployable to deal with these threats.

7.1 Firewall
A firewall is a perimeter defense or typical border management mechanism. With the sole purpose of blocking an external traffic, a firewall can also block internal traffic. Operating as a front line defense mechanism against attackers, a firewall system prevents unauthorized
entrance to or from a private network. They are deployable on both software and hardware, or the combination of the two.

7.2 Cryptographic Systems for Handling Encryption

Cryptographic systems entail the use of ciphers and codes to convert information into unintelligible data. The technological function creates readable codes for encrypted information over the Internet.

7.3 Anti-Malware, Anti-spyware and Anti-virus Software and Scanners

Users install anti-malware and ant-viruses for various computers to prevent the activities of viruses, Trojans, and worms that affect the speed of computers and even result in computer being shut down.

7.4 Intrusion Detection Systems

Intrusion Detection Systems provide users with a superfluous protection mechanism to help avert computer attacks. These can be hardware or software apparatus used in detecting attacks (Sotillo & East Carolina University, 2005). IDS tools often want an assurance of safeguarding networks by setting up the systems that detect the activities of an intruder. Computer passwords are intrusion systems that operate on hardware, while servers are hardware that help safeguarding hardware and software from intrusion. New applications like QuickBooks Pro have network intrusion systems that block an intruder from accessing files, email addresses, and even hardware.

7.5 Secure Socket Layer (SSL)

As a protocol suite, SSL safeguards a network to attain a high security level between a website and a browser. The design of this tool aims at establishing a secure link or tunnel between a web server and a browser, so that any transmitted information is safe within the tenable tunnel. In this regard, SSL offers the certification of clients to serves. Clients can then present certificates to the server to exhibit their identity.

8. Case Study: Us-Visit

Immigration, insecurity, and rising cases of computer crimes intercept normal operations in the US. The Mexican border and the southern borders of the US needed security, which the country was not able to achieve through immigration units and Homeland security. In 2001, the Homeland security believed that technology was necessary for the visa issuing process and the identification of criminals and terrorists. In 2002, the Department of Homeland Security (DHS) got the leeway to develop a “virtual fence” in the US to protect the country from terrorist activities. The DHS realized that a virtual fence would accommodate detectors, scanners, cameras, computers, and other protective gears requisite for handling crime and
terrorist acts (Sotillo & East Carolina University, 2005). At that time, the military and the government had unclear channels of communication and information leaking was a great concern. The Department of Homeland Security needed an assurance that attackers could not acquire information during immigration. The control officers at the immigration department allowed other people to overstay in the country. The 1993 attack on the World Trade Centre scared the entire population. The attackers’ ability to overstay in the US earned them the courage to learn information flow between the immigration department and the DHS. The lack of biometric measures in the 20th century deterred the relevant bodies from getting sufficient information concerning the attackers.

After the 9/11 attack on the US, the department of homeland security in collaboration with the government established the US-VISIT. The system uses biometric strategies of assessing the entry and exit points of foreigners. Foreigners have their fingerprints on immigration databases to identify each person. The US-VISIT security network supports the communication between the government, the DHS, and immigration department to secure the borders (US-VISIT Traveler Information). The system of hardware and software enhances communication between the three units to create foolproof authentication. US-VISIT helps local and federal governments assess movements of illegal immigrants and even cars. The two wings of government have deployed over 40,000 agents to oversee the process while 30,000 others have access to the passwords of various network systems of the US-VISIT

9. Current Developments in Network Security

Network security changes over the time because the complexities of crimes equally evolve through the years. The countries like the US employ the US-VISIT network security system because attacks in the 21st century take the form of biometric or laser technology (US-VISIT Traveler Information). People who engage in fraudulent activities believe that society is reluctant to involve innovative techniques of managing crimes. IT experts develop biometric and laser network systems to handle complex crimes while partaking in further research to manage any new trends of security attacks.

9.1 Developments in Network Security for Hardware

Various organizations consider a firewall as a failed system of handling crimes in hardware systems. Hardware attacks are detrimental because even software operates under it. Recent technological developments encourage biometric data protection since the system involves limited movements of hardware. Biometrics and laser technologies enable a user to operate hardware from a distant position. The attackers seem to be a step ahead of security providers who look for the solutions to the same problems. In most organizations, staff members enter the office after a finger print check at every entrance and exit zone. The biometric system searches for any foreign elements and ensures that the right of entry or exit is unique to each person. For instance, workers cannot make a scanner identify a fingerprint of another person in their absence. Warfield (2004) cites that biometric systems use concurrency control mechanisms to avoid failure of one system. The systems operate in a manner in which in case the hardware fails other picks operations immediately. Biometric systems are expensive and develop at a slow rate. The greatest problem about the innovation is that people can only be creative in terms of security when society identifies the need. Passwords identify a unique IP address for each user, even though EIFT cannot guarantee that another person may not be able to spoof or eaves drop. Biometric technologies cannot accommodate more than one user at a time because the identification of a user needs the presence of the one.
Biometric systems are mostly set in airports, seaports, immigration departments, and military owing to the high-profile security in those sections. Entry or exit zones use biometric hardware to enable security personnel identify people linked to criminal activities. Network security that uses biometric technique discourages eavesdropping (2004) or other types of attacks, as it would be impossible to get the access to the secure environments. Laser technology reduces physical interaction with hardware like computer desktops or laptops. The introduction of applications in iPads, tablets, and iPhones is an indication that the touch capability reduces individual interaction with computers. Users can set commands through voice technology, enabling a computer to identify the voice of a user. In essence, the machine cannot accept commands from a different person. Today, security providers seek the measures of reducing any possibilities of attracting new attacks in an exercise to handle the present problems. Smart and credit cards have a personal identification number, but crimes linked to the electronic cards are numerous. Criminals sometimes acquire PIN numbers through forceful measures or deception to access user accounts. However, the use of passwords is not a safe strategy and the PIN numbers equally deserve an advanced technology of issuance. A new technological development prefers the use of laser and biometric technologies since they reduce password theft and cyber crime.

Network security for hardware is imperative because the latter is prone to external and internal attacks. Computer viruses slow computer speeds and in other cases cause a complete damage of the machines. Today, society strives to find quality network security measures besides laser and biometric technologies because ATM crimes still occur in most parts of the world.

9.2 Developments in Network Security for Software

Network security for software is important because of vulnerability of the software to spam and hacking. The size of hardware that the software will serve is the greatest factor of consideration. Some intends to serve small offices, schools, armed units and government or private organizations. Software development is difficult in comparison to that of hardware and stringent measures are necessary when protecting it. Firewalls, wireless technology, and filters help many organizations handle attacks related to software. The current development in securing software entails the assignment of static IP addresses to users for easy of identification (Tyson, 2009). Software management consumes about 25 percent more resources as opposed to managing hardware. Researchers tend to encourage the use of biometrics in safeguarding software for many users especially in medium-sized units. Through biometric technology, which most companies do not have access to, people can log in to various accounts by scanning fingerprints. Administrators play a role in ensuring that viruses do not interfere with a user account (2009). Barring various sites from access is a role of the administrator together with the authentication of users, allowing access, and providing directives to use virtual private networks to disallow protocol interference. A virtual private network is essential for avoiding the access to a different layer of protocols and using another person’s IP address. Proxy is another secure way of accessing software, as attackers find it difficult to replicate such information.

10. Results of Discussion

The Internet layout in itself causes susceptibilities in the network. Acknowledging the security concerns greatly aids in establishing novel security mechanisms and paradigms for
network security and Internet access itself. Network security is crucial since attackers continually generate criminal tactics of interfering with secure systems through phishing, spamming, or eavesdropping. The history of network security displays the ardent need of technologists to advance safety for information. Intrusion detection techniques are dependent on the nature of threats are usually used. As Al-Salqan (1997) observes, the future of network security will possibly resemble that of an immune system; it should fight off attacks and create itself to face tougher enemies. To another end, the tendency towards biometric technologies could have manifested previously. However, it looks like there is no vigorous pursuit in that line. The good news lies in the fact that several security advancements occur within the same range of security technologies used today, though with some slight modifications.

Each type of security concern raises the need for quality network security that coincides with the problem (AICMS 08, 2008). The USVISIT is an example of secured hardware system, which assists the US in identifying terrorists, criminals, and fraudsters in the entry and exit zones of the country. In summary, network insecurity is often a step ahead of network security, prompting the personnel to develop the best system to deal with futuristic concerns.

11. Conclusion

Network security assures people that intellectual property is secure, and that intruders cannot access sensitive information from another user account. Anti-viruses and security software packages cannot provide requisite protection for information for both passive and active attacks. Former occur during the denial of service, spoofing, cyber attacks and ARP poisoning. On the other hand, active attacks are common in scanners and hardware. The attacks on hardware and software will always exist; security providers must develop a unique promise when developing the systems to counter network threats. Biometric security is expensive for many organizations and this is probably the reason for why cyber crime and ATM thefts are common in the 21st century. Ultimately, the introduction of laser technology in curbing network crime will help in securing many systems.

References


