ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

History, Importance & Wonder of Network Security in Present

Meenu Rani Dey*, Rakesh Patel, Renuka Bareth
Kirodimal Institute of Technology, Raigarh(C.G.),India

Abstracts

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. 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. The businesses create an "intranet" to remain connected to the internet but secured from possible threats.

Keywords: Network Security.

Introduction

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 acquire through the internet.[1]

What is network?

A network has been defined as any set of interlinking lines reassembling a net, a network of roads an interconnection system, a network of alliances. This definition suit our purpose well: a computer network is simply a system of interconnected computers.[2]

When developing a secure network, the following need to be considered

- **Access** – authorized users are provided the means to communicate to and from a particular network.
- **Confidentiality** – Information in the network remains private
- **Authentication** – Ensure the users of the network are who they say they are.
- **Integrity** – Ensure the message has not been modified in transit.
- **Non-repudiation** – Ensure the user does not refute that he used the network.[7]

Types of Attacks

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur. There are following types of attack:

Passive Attack-

A **passive attack** monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. **Passive attacks** include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack:

In an **active attack,** the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Distributed Attack:
A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a "trusted" component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack:
An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

Close-in Attack:
A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Close physical proximity is achieved through surreptitious entry into the network, open access, or both.

One popular form of close in attack is **social engineering** in a social engineering attack, the attacker compromises the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

Phishing Attack:
In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

Hijack attack:
Hijack attack In a hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accident.

Spoof attack:
Spoof attack In a spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

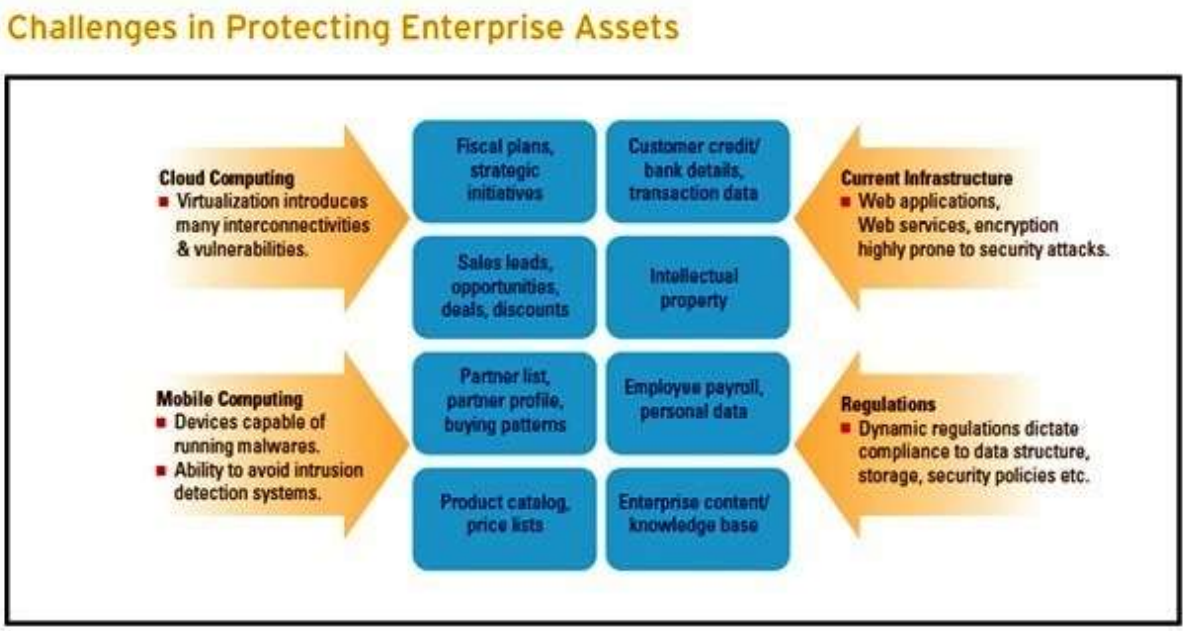
Buffer overflow :
Buffer overflow A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

Exploit attack:
Exploit attack In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

Password attack:
Password attack An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters.[3]

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Challenges for network security



Infrastructure technologies are extremely vulnerable. Most enterprises are connected to the outside world through the Internet, VPNs, B2B networks, etc. and unfortunately all of these channels are susceptible to unauthorized and unauthenticated access. Virtual environments epitomized by cloud and mobile computing add to these security challenges.Securing the Enterprise with a Framework-based Approach:

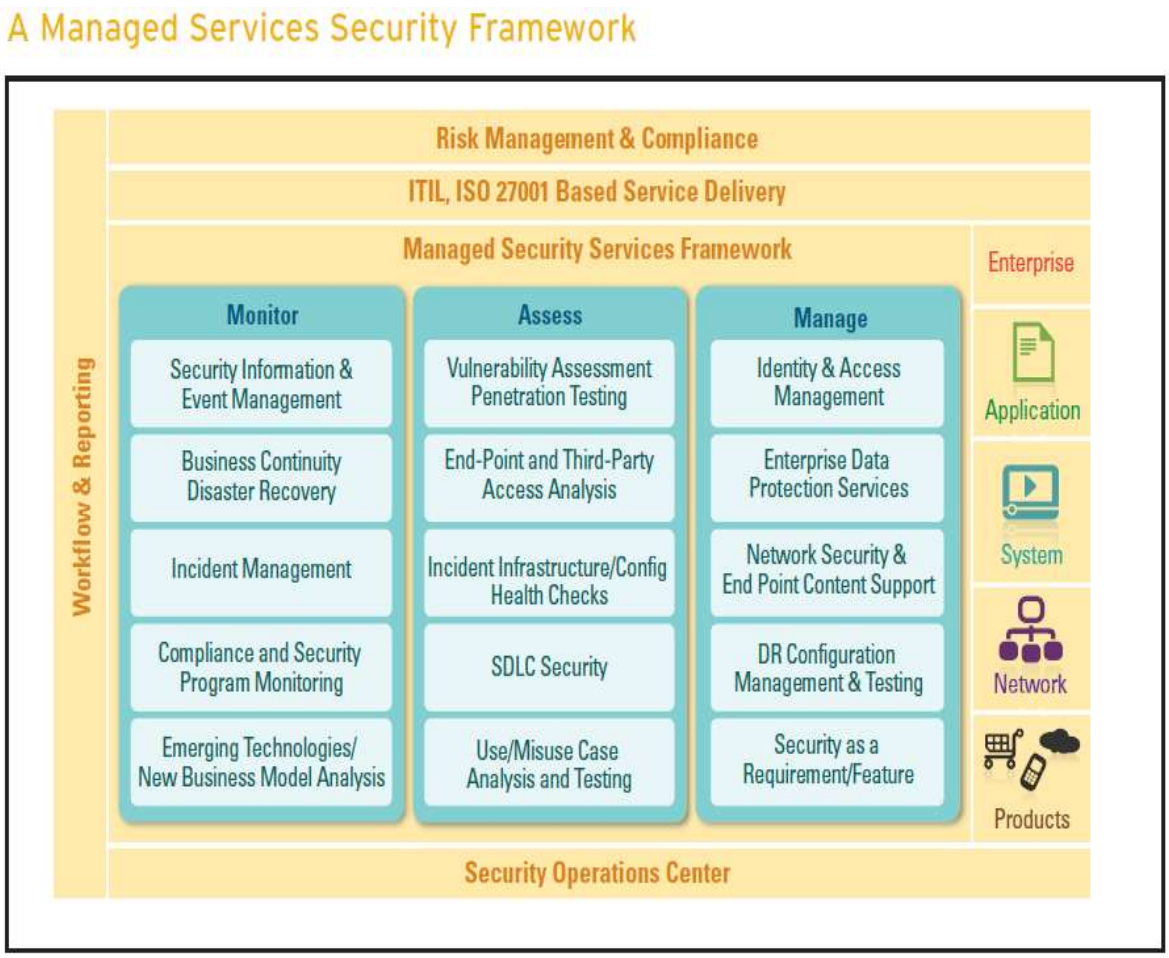
Security must be approached using a holistic perspective — both for the enterprise itself, as well as for the well-being of customers. There are two key aspects to consider when building a solution framework. One is to approach security as an enterprise asset feature; the other is to approach it from a product feature point of view.

Security Attacks' Impact

Financial Impact	Brand and Customer Impact	Operational Model Impact
• Lost time in product development due to insufficient security assessments(s). • Direct revenue impact due to lost product opportunities. • Impact due to delays in product development.	• Customer service issues crop up, leading to issues in customer satisfaction. • Branding suffers due to low customer satisfaction and customer retention issues.	• Impact to customer facing portals, newer business models around SaaS deployment, etc. • Security issues directly impact scalability of Web sites and could possibly lead to blacklisting, etc.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

How we secure from attacks



Denial-of-service attacks come in a variety of forms and aim at a variety of services. Computer users may not stop DoS or DDoS (distributed denial of service) attacks, but they can certainly take steps to reduce the risks associated with them. Here are "5 Tips for Preventing Denial of Service Attacks" to ensure network availability to users:

- ***Avoid single points of failure (which is an issue on network availability).*** **Solution**: Within the network architecture, having a mesh network can be ideal to make either the firewall or router the single point of failure for the communication network between computers. Using a mesh network topology can create a more robust network, as explained by Information and can sustain a node if one should fail, making it possible to re-route its traffic. An alternative solution to avoid single points of failure is to add LAN switches (as shown in the diagram to the right). They could help resolve network failures caused by a DoS attack.
- ***Implement a redundant firewall or router*****. Solution:** To ensure availability, a network could incorporate a redundant hardware system at the switch to eliminate failure points.
- ***Use a firewall.*** A well-configured firewall is able to prevent most attacks. Firewalls are one of the most important screening devices on a network. Even though they are targets themselves for DoS attacks, they are useful as a defense countermeasure in protecting an environment connected to a network.
- ***Deploy a screened subnet, a demilitarized zone (DMZ).*** By placing a DMZ on the network between the router and an external firewall, it can be used as a buffer area to protect the LAN.
- ***Buy an intrusion detection system (IDS).*** A network-based IDS attached to the perimeter of the network can help monitor network activity (such as an attack) with its ability to raise an alarm in time for a network administrator to take protective action.[6]

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Technology for network security

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.

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

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.

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.

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. Clients present a certificate to the server to prove their identity. Security from IPv6: From a security point of view, IPv6 is a considerable advancement over the IPv4 internet protocol.[8]

Future Trends in Security

1. Economic Information Warfare (EIW), consisting of sophisticated attacks against entire economies, commerce and enterprises will accelerate as a global threat

2. Smart Watchers, a new generation of super-sensitive satellite and video networked electronic surveillance, will be everywhere. Real-time personal face scanning and suspicion profiling tied to massive supercomputers, sensory-aware networks and data warehouses w ill determine risks, provide prevention strategies and intelligence on neutralizing threats .

3. National Identity Cards with embedded smart chips, containing an individual's entire Genomic Profile will act as a secure personal identifier.They will wirelessly authenticate an individual's location, security clearance level and identity to a sea of intelligent networks tied to Government, transportation, banking, telecom and enterprises.

4. Pandoras, the next generation of computer virus attacks, will be self-mutating viruses created to destabilize, confuse and destroy critical electronic infrastructures essential to industry and government. These will be used as offensive and defensive weapons by all sides.

5. Sniffers designed to automatically sense, watch, search and identify individual s with critical information, weapons or bombs will have the capability to navigate physical, wireless and electronic realities.

6. Secure-Wearables that are embedded, pinprick size hyper-sensing bio-reactive nano-chips, personal pin codes and GPS location monitoring will assist in security tracking and recovery after kidnapping or theft.

7. DEPS, Digitally Engineered Personalities, personal sensors that live in the global telecom Internet network and provide 24/7 follow-you anywhere security protection for individuals, enterprises and governments, will be necessary and in demand.

8. Biometric Authentication: facial, eye, fingerprint and genomic scanning will be necessary to validate an individual's physical or virtual entry into electronic networks o r physical areas. Security Tattoos with bar-scans will be popular and fashionable.

9. Biowar and Agri-Terrorism targeting the destruction of targeted ecosystems will emerge as common threats putting at risk public health, soil, food and water resources.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

10. Numerous personal privacy violations will occur, requiring new laws to protect and preserve individual. [5]

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 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 originally it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future.

References

1. Bhaya Daya “Network Security:History,i
2. mportance and future”.
3. Matt cartin”Introduction to Network Security”march1997.
4. www.computernetworkingnots.com.
5. Abhijeet Khadilkar, Tom Pai, Shabbir Ghadiali” Overcoming Security Shortcoming: Why Tech companies Embrace A 360-Degree Perspective”2011.
6. http://globalfuturist.com/about-igf/top-tan-trends/trends-in security-.html.
7. www.BrightHub.com
8. Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," *Computer*, vol.31, no.9, pp.24- 28, Sep 1998.
9. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on*, vol., no., pp.77-82, 13-15 May 2008.