Indian J.Sci.Res. 20(2): 171-173, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

CHALLENGES OF NETWORK SECURITY

P. VASANTHAKUMAR[a1] AND J. GOWTHAMA RAJA KUMARAN[b]

[ab]Department of Computer Science and Engineering, Mahendra Engineering College (Autonomous), Namakkal, Tamil Nadu, India

ABSTRACT

The Internet was expanding with a great speed so as its Security. Security is an essential field that consists of the provisions completed in underlying computer network communications, policies adopted by the internet administrator to protect the network, the internet accessible resources from unknown access and the efficiency of these measures combined together. Government, and business applications carry on to multiply on the Internet and these work-based government and services can pose safety risks to individuals and to information resources of company and governments. Information is an asset that must be protected.

KEYWORDS: Internet, Network Security, Firewall, Attacks, Threats, DOS, Cookies

Network security was a challenge for network operators and Network service providers in order to precaution it from the attack of an intruder. It deals with the requirements needed for a company or the network administrator to help in protecting the network. Computers, networks, and the Internet affect our lives every day or we can say that we are so much dependent relative for them to make our life comfortable. All are connected to the network without any boundary, thus Network Security is essential in these surroundings because any governmental network inaccessible from any system in the world and, therefore, potentially vulnerable to threats from individuals who do not require corporal access to it.

THE OBJECTIVE OF NETWORK SECURITY IS

To Protect the Confidentiality

The data must be access and read only by the authoritative individuals or parties. It is the safeguard of the personal information. We can measure up to confidentiality with privacy. Data encryption, User Ids and passwords, biometric verifications are some of the methods through which Confidentiality can be protected.

To Maintain Integrity

It is the declaration of not only the information can be accessed or modifies by the authoritative persons only, but also the data must be clear, consistent over its entire life cycle. Measures taken to ensure reliability , includes controlling the physical environment of networked terminals and servers, restricting access to data, and maintaining Rigorous Cryptography plays a very major role in ensuring the data.

To Ensure Availability

Data must be available to the authorized persons at the right time. It can be ensured by rigorously maintaining all hardware, preparing hardware repairs immediately and maintaining a correctly functioning operating system environment. Regular backup must be taken, for information services that are highly critical, redundancy is the appropriate method to ensure availability.

TYPES OF NETWORK SECURITY THREATS

Network security threats are becoming more and more complicated and risky since internet are gradually more attractive hunting ground for hackers, criminals, activists and terrorists forced to get noticed, make money, or even bring down corporations and governments through different threats of attacks. Network security threats can be divided into four types.

Unstructured Threats

Unstructured threats frequently initiate from new persons by means of easily accessible hacking tools. These types of hackers are not most brilliant or qualified programmers. Their skills can do a lot of damage to a corporation.

Structured Threats

Structured threats are forced by an individual or a group who are highly trained and technically tougher than the script attackers. They have regular awareness about the network structure design.

[1]Corresponding Author

Exterior Threats

These threats initiated from individuals or group of people functioning outside of the organizations. They do not have official access to every computer system or network.

Interior Threats

A computer network or a server must be secure enough not only from the exterior threats but from the interior also. These threats can be initiated inside the organizations by a frustrated present or a previous employee.

NETWORK SECURITY TYPES

Security by Anonymity

Security of anonymity relies on the fact that a given susceptibility is unseen or undisclosed as a security measure, i.e. no one knows about the system that exists. If anybody or something unintentionally discovers the susceptibility, no valid protection exists to avoid mistreatment.

Firewalls

To start preparing for perimeter-related network-defense policy organizations should implement the firewall. The firewall will prevent the unwanted threats to the network architecture.

Validation

It is another method to implement the network security. By providing a valid username and passwords every user gets exclusive access to the network and one cannot interrupt with other so that it will prevent the unwanted threats.

NETWORK SECURITY DEVELOPMENT

There are many changes in the technology of network security this is due to new mobile operating systems, increasing use of personal devices and so on. Day to day enhancements in technology and communications make all the improvements feasible. There are many remote users, faster network connections, and widespread upgrades to mobile networks which are some of the reasons for network security.

CHALLENGES IN NETWORK SECURITY

Distributed denial of service (DDoS) attacks

We can expect to see a higher risk of business impacting threats with the shift from computer-based attacks, generating a large number of lower bandwidth events, to a virtual server or cloud-based attacks, generating ultra-high bandwidth events. With these new attack vectors, it becomes even more beneficial to identify and mitigate large DDoS events while traffic is in the network cloud.

Password Management

Our challenge is put in place and enforcing stronger user-controlled passwords that are less likely to be broken. This educational and administrative challenge requires creative solutions and enforced policies.

Interrupt

Interrupt of computer networks can affect critical infrastructure and ultimately impact corporate and backbone networks. This challenge is so potentially bad because it combines social engineering with software based tools to provide a complex multi-vectored attack profile.

Mobility

Management and security of networks and smart mobile devices becomes even more challenging when employees want to use their own devices for business purposes. The bring-your-own-device trend exasperates this challenge when we look at protecting the critical information needed to manage the organization and the network without sacrificing the privacy of employee's personal information and activities.

Internet

One of the greatest challenges to security experts is the insight that the internet, a best effort network, is a secure critical infrastructure. The internet is an open connection of diverse networks. We need to put into effect policies that distinguish platforms and security levels based on business criticality. Control networks need different security than general business communications. This includes using network embedded security controls to help reduce risks and to simplify security infrastructure.

Privacy laws

This final challenge is currently being legislated worldwide. We need to balance privacy with the need to gather information that can help address security breaches or fraud, while complying with associated legislation.

CONCLUSION

Network security is not that something you also have or don't- it is a repeated arms race against nasty hackers. Fortunately, as attacks become more complicated, so too does the technology and practices used to protect the network. One of the biggest security concerns today is the insider threat. Another major security concern is lack of consistency in enforcing "acceptable use" policy. Most of the policies are badly written, out of date and poorly communicated. Securing the network is just as important as securing the computers and encrypting the message. In the current scenario, there are a number of ways, which guarantee for the safety and security of the network but it cannot be said they will everlasting. We have to perform regular network security testing.

REFERENCES

Carle E. Landwehr, "Security Issues in Networks with Internet Access", Member, IEEE.

Ghansela S., 2013. "Network Security: Attacks, Tools and Techniques", **3**(6).

Agarwal K., 2014. "Network Security: Attacks and Defence", **1**(3).

http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html

5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), Mouna Jouini

Eric Cole, 2009. Network Security, Bible, 2nd Edition.

Golchha P., 2014. "A Review on Network Security Threats and Solutions", 2347:3878.

Mohammad I., 2014. "A Review of types of Security Attacks and Malicious Software in Network security", **4**(5).

Daya B., "Network Security: History, Importance, and Future", University of Florida Department of Electrical and Computer Engineering.

Vaclav Matyas, "Biometric Authentication-Security and Usability"

https://powermore.dell.com/technology/network-security-three-biggest-challenges/