SECURE NETWORKS: A COMPLETE REVIEW

Vaibhav Tripathi[1], Gaurav Pathak[2]
NIMS University, Jaipur, Rajasthan

Abstract: Following thirty years of work on PC security, why are every one of the frameworks in administration today to a great degree vulnerable to assault? The primary reason is that security is ex-contemplative to set up and a disturbance to run, so individuals judge for a fact how little of it they can escape with. Since there's been little harm, individuals conclude that they needn't bother with much security. Also, setting it up is complicated to the point that it's scarcely ever done right. While we anticipate a disaster, less difficult setup is the most vital stride toward better security. In an appropriated framework with no focal administration like the Internet, security requires a reasonable anecdote about who is trusted for every progression in building up it, and why. The essential instrument for telling this story is the "represents" connection between principals that portrays how power is dele-gated, that is, who trusts whom. The thought is basic, and it clarifies what's happening in any framework I know. A wide range of methods for encoding this connection regularly make it difficult to see the hidden request.

Keywords: Data Mining , Hadoop, Big Data

I. INTRODUCTION

The world is turning out to be more interconnected with the approach of the Internet and new systems administration innovation. There is a lot of individual, business, military, and government data on systems administration bases around the world. System security [1] is happening to extraordinary significance on the grounds that of licensed innovation that can be effortlessly obtained through the web. There are as of now two on a very basic level diverse systems, information systems and synchronous system involved switches. The web is viewed as an information system. Since the present information system comprises of computer-based switches, data can be gotten by exceptional projects, for example, "Trojan steeds," planted in the switches. The synchronous system that comprises of switches does not support information and hence are not debilitated by assailants. That is the reason security is underscored in information systems, for example, the web, and different systems that connection to the web.

The incomprehensible point of system security is dissected by investigating the accompanying:

- History of security in systems
- Internet design and defenseless security parts of the Internet
- Types of web assaults and security strategies
- Security for systems with web access
- Current advancement in system security equipment and programming

In light of this examination, the eventual fate of system security is guage. New patterns that are developing will likewise be considered to comprehend where system security is heading. [2]. Information security is the part of security that permits a customer's information to be changed into incomprehensible information for transmission. Regardless of the possibility that this incomprehensible information is blocked, a key is expected to decipher the message. This strategy for security is successful to a specific degree. Solid cryptography in the past can be effectively broken today. Cryptographic strategies[3] need to keep on advancing because of the progression of the programmers too. While exchanging ciphertext over a system, it is useful to have a safe system. This will consider the ciphertext to be ensured, with the goal that it is more improbable for some individuals to try and endeavor to break the code. A protected system will likewise keep somebody from embeddings unapproved messages into the system. Along these lines, hard figures are required and also attack-hard systems [2].

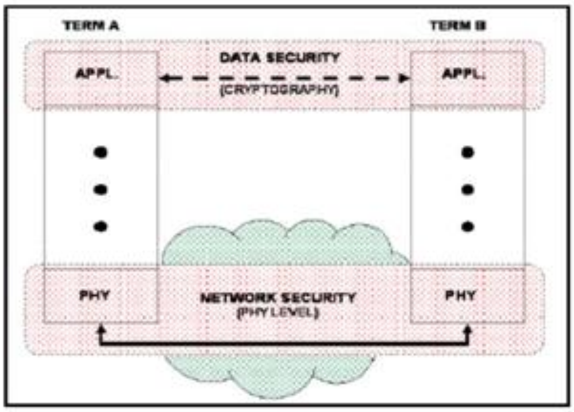

Figure 1: Based on the OSI model, information security and system security have an alternate security capacity [2].

The relationship of system security and information security to the OSI model is appeared in Figure 1. It can be seen that the cryptography happens at the application layer; accordingly the application scholars know about its presence. The client can pick diverse techniques for information security. System security is for the most part contained inside the physical layer. Layers over the physical layer are likewise used to achieve the system security required [2]. Verification is performed on a layer over the physical layer. System security in the physical layer requires disappointment recognition, assault location components, and astute countermeasure techniques [2].

II. IMPORTANCE AND RELEVANCE OF THE STUDY

Delan Alsoufi [1], Khaled Elleithy [1], Tariq Abuzaghleh [1] and Ahmad Nassar [1], proposed that Wireless sensor networks are becoming significantly vital to many applications, and they were initially used by the military for surveillance purposes. One of the biggest concerns of WSNs is that they are very defenceless to security threats. Due to the fact that these networks are susceptible to hackers; it is possible for one to enter and render a network. For example, such networks may be hacked into in the military, using the system to attack friendly forces.

Leap protocol offers many security benefits to WSNs. However, with much research it became apparent that LEAP only employs one base station and always assumes that it is trustworthy. It does not consist of defence against hacked or compromised base stations. In this paper, intensive research was undertaken on LEAP protocols, finding out its security drawbacks and limitations. A solution has been proposed in order to overcome the security issues faced in implementing this protocol whilst employing more than one base station. The performance of the proposed solution has been evaluated and simulated to provide a better network performance.

Ammar Yassir[2] and Smitha Nayak[2] ,research paper discusses the issue of cyber crime in detail, including the types, methods and effects of cyber crimes on a network. In addition to this, the study explores network security in a holistic context, critically reviewing the effect and role of network security in reducing attacks in information systems that are connected to the internet. As, all this adversely affects the efficiency of information security of any kind of security that exists and is used in information systems. Since hackers and other offenders in the virtual world are trying to get the most reliable secret information at minimal cost through viruses and other forms of malicious soft-wares, then the problem of information security - the desire to confuse the attacker: Service information security provides him with incorrect information; the protection of computer information is trying to maximally isolate the database from outside tampering. In other words, the Internet is a large computer network, or a chain of computers that are connected together. This connectivity allows individuals to connect to countless other computers to gather and transmit information, messages, and data. Unfortunately, this connectivity also allows criminals to communicate with other criminals and with their victims.

Salah Alabady[3] , presented a design and implementation of a network security model , using routers and firewall. Also this paper was conducted the network security weakness in router and firewall network devices, type of threats and responses to those threats, and the method to prevent the attacks and hackers to access the network. Also this paper provides a checklist to use in evaluating whether a network is adhering to best practices in network security and data confidentiality. The main aim of this research is to protect the network from vulnerabilities, threats, attacks, configuration weaknesses and security policy weaknesses.

NAGAMALLESWARA RAO. DASARI [4] and VUDA SREENIVASARAO [4] propose novel multi server authentication and key agreement schemes with user protection in network security. We first propose a single-server scheme and then apply this scheme to a multi-server environment. The main merits include:
(1) The privacy of users can be ensured; (2) a user can freely choose his own password; (3) the computation and communication cost is very low; (4) servers and users can authenticate each other; (5) it generates a session key agreed by the server and the user; (6) thier proposed schemes are Nonce-based schemes which does not have a serious time synchronization problem.

Ateeq Ahmad[5] , Security is a branch of computer technology known as information security as applied to computers and networks. The objective of online security includes protection of information and property from theft, corruption, or threats attack, while allowing the information and property to remain accessible and productive to its intended users. The term online system security means the collective processes and mechanisms by which sensitive and valuable information and services are protected from publication, tampering or collapse by unauthorized activities or untrustworthy individuals and unplanned events respectively. The basic aim of this article is to Prevention against unauthorized security Attack and Threats.

Yang Xiao,Chaitanya Bandela,Xiaojiang (James) Du,Yi Pan and Edilbert Kamal Dass [6] , introduces the WEP as well as all kinds of attacks. Then, two approaches to enhance the WEP are proposed to overcome some known vulnerabilities and thus to provide better data confidentiality and authentication. Finally, simulation methodology is presented and simulation results are provided. Thier studies show that the proposed enhancements provide better data confidentiality with some degree of computing cost as the trade-off.

III. COMMON SECURITY ATTACKS

Regular web assaults techniques are separated into classifications. Some assaults pick up framework learning or individual data, for example, listening stealthily and phishing. Assaults can likewise meddle with the framework's expected capacity, for example, infections, worms and trojans. The other type of assault is the point at which the framework's assets are expends pointlessly, these can be brought about by foreswearing of administration (DoS) assault. Different types of system interruptions additionally exist, for example, land assaults, smurf assaults, and teardrop assaults. These assaults are not too known as DoS assaults, but rather they are utilized as a part of some structure or another regardless of the possibility that they aren't specified by name.

Spying

Block attempt of correspondences by an unapproved gathering is called listening in. Latent spying is the point at which the individual just subtly listens to the arranged messages. Then again, dynamic spying is the point at which the interloper listens and embeds something into the correspondence stream. This can prompt the messages being bended. Touchy data can be stolen thusly [5].

Infections

Infections are self-replication programs that utilization documents to contaminate and spread [3]. Once a document is opened, the infection will initiate inside the framework.

Worms

A worm is like an infection since they both are self-replicating, however the worm does not require a document to permit it to spread [8]. There are two principle sorts of worms, mass-mailing worms and network- mindful worms. Mass mailing worms use email as a way to taint different PCs. Network-aware worms are a noteworthy issue for the Internet. A network-aware worm chooses an objective and once the worm gets to the objective host, it can contaminate it by method for a Trojan or something else.

Trojans

Trojans have all the earmarks of being generous projects to the client, yet will really have some noxious reason. Trojans normally convey some payload, for example, an infection [1].

Phishing

Phishing is an endeavor to acquire secret data from an individual, gathering, or association [4]. Phishers trap clients into uncovering individual information, for example, Visa numbers, web managing an account accreditations, and other delicate data.

IP Spoofing Attacks

Satirizing intends to have the location of the PC reflect the location of a trusted PC keeping in mind the end goal to access different PCs. The character of the gatecrasher is covered up by various means making discovery and counteractive action troublesome. With the present IP convention innovation, IP- mock parcels can't be disposed of [2].

Denial of Service

Denial of Service is an assault when the framework getting excessively numerous solicitations can't return correspondence with the requestors [2]. The framework then expends assets sitting tight for the handshake to finish. In the long run, the framework can't react to any more demands rendering it without administration.

IV. CONCLUSION & FUTURE SCOPE

In this paper we quickly evaluated the different data mining patterns from its beginning to what's to come. This survey would be useful to analysts to concentrate on the different issues of information mining. In future course, we will try to focus our research on the field of accident analysis and will perform analysis using the apriori and the modified apriori algorithm which we will propose in our future research work.

REFERENCES

[1] Delan Alsoufi, Khaled Elleithy, Tariq Abuzaghleh and Ahmad Nassar, SECURITY IN WIRELESS SENSOR NETWORKS–IMPROVING THE LEAP PROTOCOL, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.3, June 2012

[2] Ammar Yassir and Smitha Nayak,Cybercrime: A threat to Network Security,IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012

[3] Salah Alabady,Design and Implementation of a Network Security Model for Cooperative Network,International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009

[4] NAGAMALLESWARA RAO. DASARI and VUDA SREENIVASARAO ,PERFORMANCE OF MULTI SERVER AUTHENTICATION AND KEY AGREEMENT WITH USER PROTECTION IN NETWORK SECURITY, International Journal on Computer Science and Engineering , 2010

[5] Ateeq Ahmad, Type of Security Threats and It's Prevention, Int.J. Computer Technology & Applications,ISSN:2229-6093

[6] Yang Xiao, Chaitanya Bandela, Xiaojiang (James) Du,Yi Pan and Edilbert Kamal Dass, Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs

[7] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, International Journal of Advanced Research in Computer Science and Software Engineering,2013