International Journal of Nanotechnology and Applications
ISSN 0973-631X Volume 11, Number 3 (2017), pp. 237-246

http://www.ripublication.com

EVALUTION OF LAYER BY LAYER OSI MODEL FOR A PREDFINED JOB TO ADDRESS IT AND ERADICATE VARIOUS SHORT COMINGS USING NETWORK TO AUTONOMIC NETWORK

Dr .M.P.Vani

Associate Professor, SITE,
Vellore Institute Of Technology, Vellore

Abstract

Several Network security techniques are used to provide security and privacy for user information, while transferring over the network with respect of layers. That shows how each layer is providing security and privacy using various methods such as encryption, decryption error recovery, and flow-control. In previous paper a proactive framework is designed and developed for providing security and privacy for a network, a framework is having five layers to secure the data. In this paper for that framework providing more security and privacy OSI model is used, this framework is providing security and privacy using OSI model for information, in that seven layers are performing their predefined job to address it and eradicate various short comings from a network. With this approach a framework that will help evolution of network towards secure, privacy and trust-based environments.

Keywords: decryption, encryption, privacy, framework, security

INTRODUCTION:

In information technology, network is the development, outline, and utilization of a network, including the physical (cabling, center point, span, switch, etc), the determination and utilization of telecom convention and PC programming for utilizing and dealing with the system, and the foundation of operation approaches and methodology identified with the network. Computer network is the act of interfacing

two or additionally registering gadgets with each other with the end goal of sharing information. Computer network are worked with a blend of equipment and programming segments. Computer networks can be sorted in a few distinctive ways. One methodology characterizes the kind of system as indicated by the geographic region it spans. Local zone systems (LANs), for instance, ordinarily traverse a solitary home, school, or little office building, though wide territory systems (WANs), reach crosswise over urban areas, states, or even over the world. The Internet is the world's biggest open WAN.

NETWORK SECURITY:

Network security comprises of the approaches embraced to forestall and screen unapproved access, abuse, adjustment, or fores wearing of a computer network and network open assets. Network security includes the approval of access to information in a Network, which is controlled by the system administrator.[citation needed] Users pick or are doled out an ID and secret key or other confirming data that permits them access to data and projects inside their power. System security covers an assortment of PC systems, both open and private, that are utilized as a part of regular employments; leading exchanges and correspondences among organizations, government offices and people. Systems can be private, for example, inside an organization, and others which may be interested in community. System security is included in associations, undertakings, and different sorts of establishments. It does as its title clarifies: It secures the system, and ensuring and administering operations being finished. The most well-known and basic method for ensuring a system asset is by doling out it an exceptional name and a relating secret key.

DETAILED DESIGN OF THE SYSTEM:

Network security with regards to today's quickly changing system situations. The security worldview is changing, and security arrangements today are arrangement driven and intended to meet the necessities of business. To help you confront the complexities of dealing with a present day organize, this section talks about the center standards of security—the CIA triad: Confidentiality, uprightness, and Availability.

Security Policy: A security Policy is an arrangement of standards, practices, and strategies directing how touchy data is overseen, ensured, and disseminated. In the system security domain, approaches are typically point particular, which implies they cover a solitary zone. A security strategy is an archive that communicates precisely what the security level ought to be by setting the objectives of what the security components are to fulfill. Security arrangement is composed by higher administration

and is planned to portray the "what's" of data security.. Data security arrangements underline the security and prosperity of data assets; they are the establishment of data security inside an association.

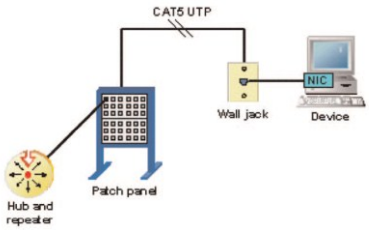


Fig5: The Physical Layer

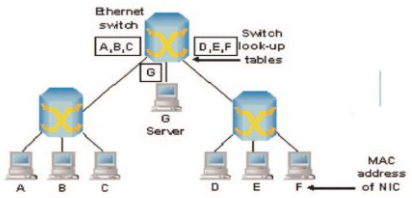


Fig6: The Data Link Layer

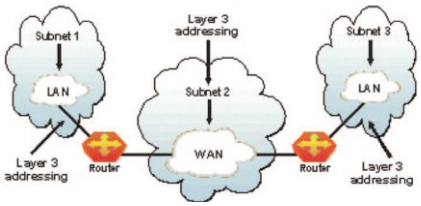


Fig7: The Network Layer

Fig8: The Network Layer

IMPLEMENTATION DETAILS

Working principles:

Every layer is giving sure functionalities; each capacity will work with various standards. These standards are as calculations, here displaying the calculations for every layer how it work.

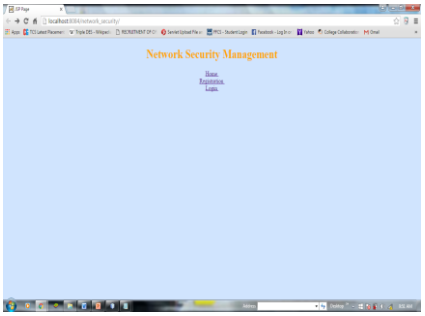


Fig14: Home Page of NetworkSecurity Management

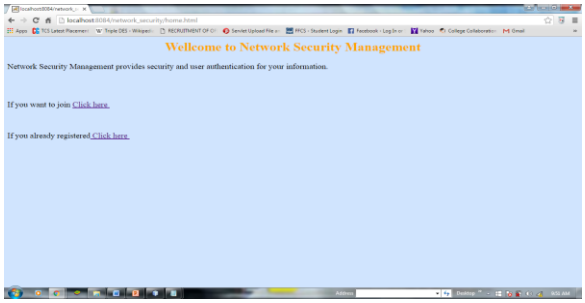


Fig15: Home Page of Network Security Management

In the event that client needs to secure the data client can login into Network Security Management, if the client is as of now enrolled in it on tapping the connection click here. On the other hand client is new then clock on to the snap here connection to register.it will divert to enlistment page

If the user is new then register firstly,

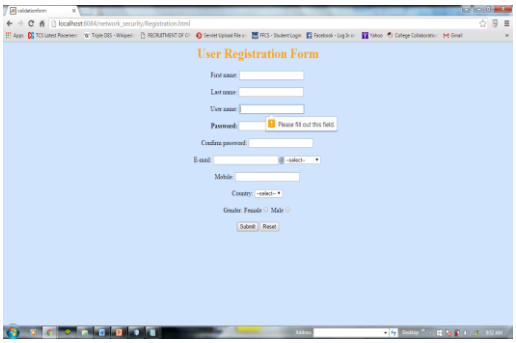


Fig16: User Registration Form

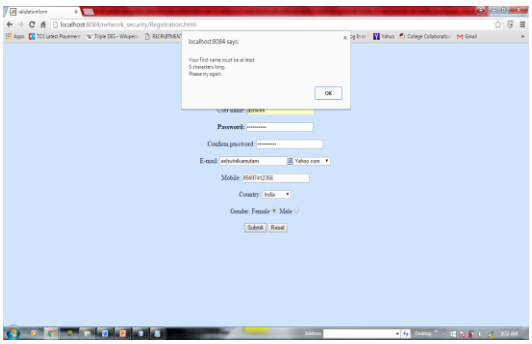


Fig17: Warning Message for Registration

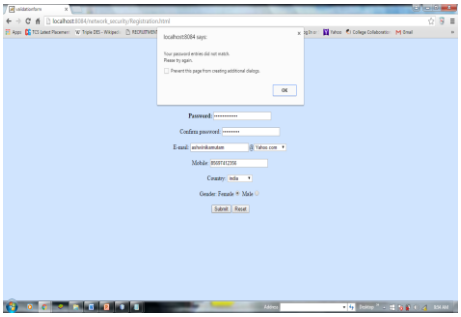


Fig18: Warning Message for Password Field

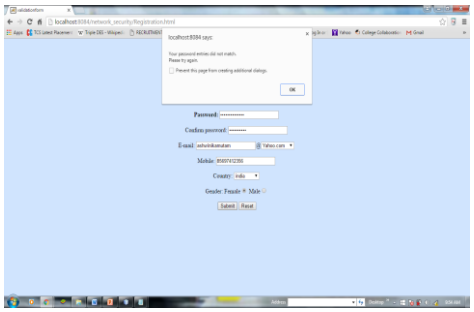


Fig19: Warning Message for CPassword Field in Registration Form

in registration

After finish of enlistment it will divert to login page. here login verification is secures the client data

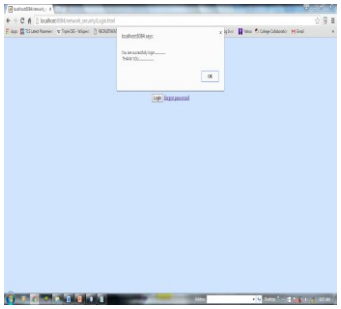


Fig20: Login page

Fig21: Uploading File

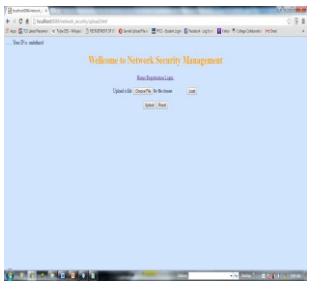


Fig22: File Uploaded

Triple DES Algorithm:

Triple DES uses a "key bundle" that comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

I.e., DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))

I.e., decrypt with K3, encrypt with K2, then decrypt with K1.

Each triple encryption encrypts one block of 64 bits of data.

For every situation the center operation is the opposite of the first and last. This enhances the quality of the calculation when utilizing keying choice 2, and furnishes similarity with DES with keying choice 3.

The standards define three keying options:

Keying option 1

All three keys are independent.

Keying option 2

K1 and K2 are independent, and K3 = K1.

Keying option 3

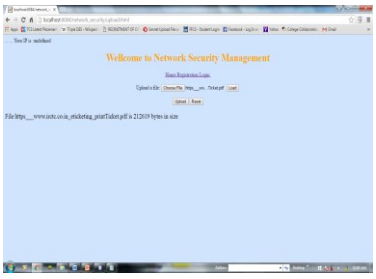
All three keys are identical, i.e. K1 = K2 = K3.

Keying option 1 is the strongest, with 3 × 56 = 168 independent key bits.

Keying option 2 provides less security, with 2 × 56 = 112 key bits. This option is stronger than simply DES encrypting twice, e.g. with K1 and K2, because it protects against meet-in-the-middle attacks.

Keying option 3 is equivalent to DES, with only 56 key bits. It provides backward compatibility with DES, because the first and second DES operations cancel out. It is no longer recommended by the National Institute of Standards and Technology (NIST),[5] and is not supported by ISO/IEC 18033-3.

Each DES key is nominally stored or transmitted as 8 bytes, each of odd parity,[11] so a key bundle requires 24 bytes for option 1, 16 for option 2, or 8 for option 3.



File Uploaded successfully and logedout

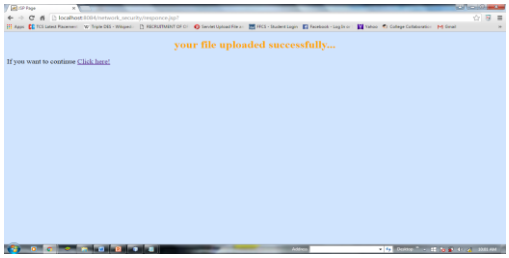


Fig23: File size in Bytes after Uploading

After choosing the uploaded file to check the size of the file to prevent exceptions of size of the file to click on to the load button it will gives size of the file in bytes. If file is more then of required size user can check before uploading and change the file size with compressing technique and can upload a valid file. After uploading a file user log out automatically. If user wants to continue the previous session again, the page will redirect to login page on clicking on click here link.

Sources of Network Threats:

Presently, we've secured enough foundation data on systems administration that we can really get into the security parts of every one of this. As a matter of first importance, we'll get into the sorts of dangers there are against organized PCs, and afterward a few things that should be possible to secure yourself against different dangers.

Denial-of-Service: Do's (Denial-of-Service) assaults are presumably the nastiest, and most hard to address. These are the nastiest, in light of the fact that they're anything but difficult to dispatch, troublesome (infrequently inconceivable) to track, and it is difficult to decline the solicitations of the assailant, without likewise rejecting real demands for administration.

Unauthorized Access: ``Unauthorized access'' is an abnormal state term that can allude to various diverse sorts of assaults. The objective of these assaults is to get to some asset that your machine ought not to give the assailant. For instance, a host may be a web server, and ought to give anybody asked for website pages. Notwithstanding, that host ought not give charge shell access without being certain that the individual making such a solicitation is somebody who ought to get it, for example, a nearby chairman.

Executing Commands Illicitly: It's clearly undesirable for an obscure and untrusted individual to have the capacity to execute orders on your server machines. There are two primary characterizations of the seriousness of this issue: ordinary client access, and director access.

Privacy Breaches We have to analyze the danger model: would could it be that you're attempting to secure yourself against? There is sure data that could be entirely harming on the off chance that it fell under the control of a contender, an adversary, or people in general. In these cases, it's conceivable that bargain of a typical client's record on the machine can be sufficient to bring about harm (maybe as PR, or getting data that can be utilized against the organization, and so forth.)

Dangerous Behavior: Among the dangerous sorts of break-ins and assaults, there are two noteworthy classifications.

Information Diddling: The information diddler is likely the most exceedingly bad sort, following the certainty of a break-in won't not be instantly self-evident. Maybe he's toying with the numbers in your spreadsheets, or changing the dates in your projections and arrangements.

Information Destruction: Some of those execute assaults are essentially turned bastards who like to erase things. In these cases, the effect on your processing capacity - and therefore your business - can be nothing not exactly if a flame or other calamity brought on your figuring gear to be totally demolished.

Secure Network Devices: It's vital to recollect that the firewall is one and only passage point to your system. Modems, in the event that you permit them to answer approaching calls, can give a simple intends to an aggressor to sneak around (instead of through) your front entryway (or, firewall). Pretty much as mansions weren't worked with channels just in the front, your system should be ensured at all of its entrance focuses.

Secure Modems; Dial-Back Systems: On the off chance that modem access is to be given, this ought to be monitored painstakingly. The terminal server, or system gadget that gives dial-up access to your system should be effectively managed, and its logs should be analyzed for odd conduct. Its passwords should be solid - not ones that can

be speculated. Accounts that aren't effectively utilized ought to be handicapped. To put it plainly, it's the most effortless approach to get into your system from remote: monitor it deliberately.

Crypto-Capable Routers: A component that is being incorporated with a few switches is the capacity to utilize session encryption between indicated switches. Since activity traversing the Internet can be seen by individuals in the center who have the assets (and time) to snoop around, these are profitable for giving availability between two locales, such that there can be secure courses.

Virtual Private Networks: Given the pervasiveness of the Internet, and the extensive cost in private rented lines, numerous associations have been building VPNs (Virtual Private Networks).

CONCLUSION AND FUTURE WORK:

This project is providing different types of network security techniques to increase the level of security for the layers of OSI model in networking. In each layer security and privacy is providing to the user information using various kinds of methods those are authentication, data privacy using encryption, and decryption, security for user information, like no interruptions while transferring the data, no loss of data, error free information congestion control of data etc. for this paper further improvement chances also available, and research purpose of scope also is there in the form of increase security and privacy using cryptography techniques, and also can use digital signature with the help of cryptography to transfer the information from one system to anther system over the network.

REFERENCES:

[1] Alfredo Matos, Susana Sargento, Rui L. Aguiar Instituto de Telecomunicac¸ ˜oes, Universidade de Aveiro “Waypoint Routing: A Network Layer Privacy Framework” IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

[2] Venkatasubramanian S. and Jothi V. “. Integrated Authentication and Security Check With CDMA Modulation Technique in Physical Layer of Wireless Body Area Network” Department of Information Technology, Nizwa College of Technology, Oman venkatasubramanianphd@gmail.com and Department of Computer Science, Presidency College, Chennai, Tamil Nadu, India,2007

[3] Prof. Mukund R. Joshi, Renuka Avinash Karkade, "Network Security with Cryptography", Information Technology, Sant Gadgebaba Amravati University, Amravati, India, Computer Science and Information Technology, Sant Gadgebaba Amravati University, Amravati, India, mukundjoshi98@yahoo.co.in, IJCSMC, Vol. 4, Issue. 1, January 2015, pg.201 – 204. renuka.karkade@gmail.com.