IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 01-06
www.iosrjournals.org

Authentication Techniques Help To Improve Security in the Era of Network System: A Study

Mrs. Ruma Rahul Kapre

(ruma_kapre@yahoo.co.in, Department of Computer Science, Dharampeth M. P. Deo Memorial Science College/Nagpur University, INDIA)

Abstract : *In the era of today's world as society is moving towards digital information, network security is becoming a central issue. While transferring the data through internet, security plays a crucial role. Security involves authorization of access of information controlled by the network administrator. The goal of providing security to the network not only makes sure the security of end system but also of the entire network. Authentication is one of the primary ways of establishing and ensuring security in the network. Authentication can be accomplished in many ways. In this paper, an attempt has been made to analyze some of the authentication techniques for providing security to the network system.*

Keywords - *Authorization, Authentication Techniques, Network, Network Security, Network Topology, Network Types*

I. INTRODUCTION

Today's world deals with the wired and wireless network. To protect data transmission over network, security plays an important role. Data Security is the main aspect of secure data transmission over network. Today, Data Security is becoming a challenging issue. It has to cover many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. As development in information technology is on the high peak, the secure transmission of confidential data over network is now a main point of attention. As it is possible that the information on the network could be accessed by an unauthorized user for malicious purpose. It becomes necessary to apply effective encryption/ decryption methods for enhancement of data security. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. User ID and password which are chosen by user or assigned to them are use for accessing the information over network within their authority. Network security covers a variety of computer networks, both public and private. Networks are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. All organizations, enterprises, and institutions are involved in network and want to be secure over network. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password. [1-2]. Following sections deals with the network and network types and network topology.

II. NETWORK

A network consists of a set of nodes and the relations between these nodes. The nodes may be individuals, groups, organizations or societies. [3] Network devices that originate, route and release the data are called network nodes. Nodes consists of personal computers, phones, servers as well as networking hardware. The devices are supposed to be in network, when one device is able to interchange information with the other device, whether or not they have a uninterrupted connection to each other. The network may obtain between individual to individual or individuals to group. In network, computers are linked through a medium and data communication devices. Sharing resources and communicating data is the main principle of network. Computer networks vary in various places like in the transmission media used to communicate the signals, the communications protocols to systematize network traffic, its size, topology and organizational set on.

III. NETWORK TYPES

There are number of different types of computer networks. Computer networks can be distinguished by two things taking into consideration size and their purpose.

The size of a network can be expressed by the geographic area they occupy and the amount of computers that are part of the network. Networks can cover anything from a handful of devices within a only room to millions of devices spread across the entire globe.

Some of the different networks based on size are:

- Personal area network, or PAN
- Local area network, or LAN
- Metropolitan area network, or MAN
- Wide area network, or WAN

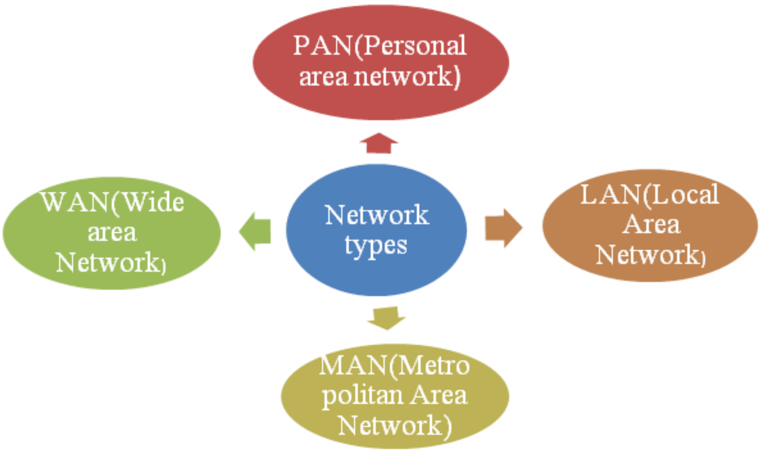


Fig 1: Types of Network

a. Other types of network

Many networks can be considered general purpose, which means they are used for everything from sending files to a printer, accessing the Internet. Such types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

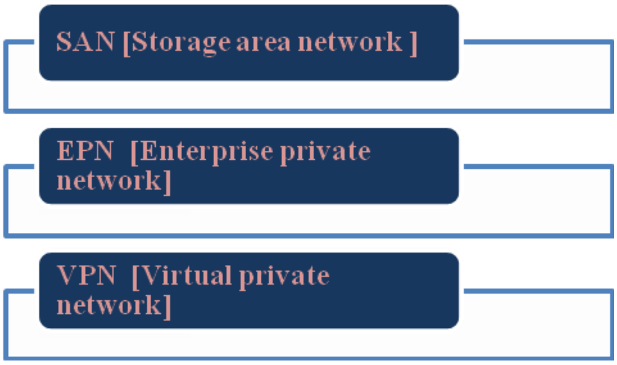

SAN [Storage area network]
EPN [Enterprise private network]
VPN [Virtual private network]

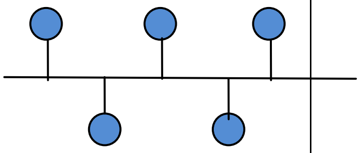
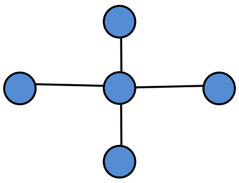
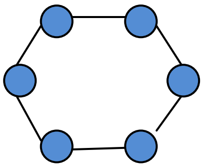
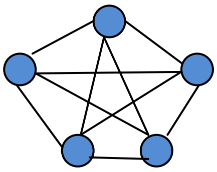
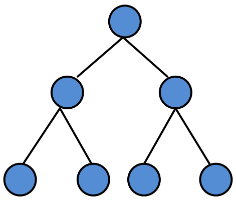
Fig 2: Types of Network

IV. NETWORK TOPOLOGY

For the accomplishment of communicating data and sharing resources, two or more computers are linked together through a medium and data communication devices. The term topology in communication network refers to the way the computers or workstations are linked together in the network.

Following Table 1 discuss basic types of network topologies like Bus Topology, Star Topology, Ring Topology, Mesh Topology and Tree Topology.[4,5]

Table 1: Types of Topology

Sr.no	Name of Topology	Purpose	Diagram
1	Bus Topology	In this topology a set of computers are connected via a single network cable known as bus which acts as a backbone.	
2	Star Topology	In this topology a central switch or hub is used to connect all the components. The devices or users are not linked to each other and it does allow direct traffic between devices.	
3	Ring Topology	In this topology each node connects to exactly two other nodes that is a direct point- to- point link between two neighboring nodes forming a circular pathway for signal like a ring.	
4	Mesh Topology	In this topology, all nodes are connected to each other directly and indirectly forming a mesh of cables used for connection.	
5	Tree Topology	In this topology only one route node exists between any two nodes on the network. Also it is a group of different types of networks connected with each other for extending a network.	

V. IDENTIFICATION, AUTHORIZATION AND AUTHENTICATION OVER ANY TYPE OF NETWORK

From last few decades the way of communication and business transaction has rapidly changed its prototype because of the powerful platform provided by internet. The number of user navigate through the internet is very huge. This huge amount demands authorization of data over network when dealing with social networks, sharing of knowledge, online commerce etc. in a very secure way increasing the enhancement of privacy.[6] Authorization is a mechanism for determining who can access the information resources over any type of network in a secure way. Network Administrator plays an important role in providing authorization of data over network. ‘Identification’, ‘authentication’ and ‘authorization’ are three interrelated concepts, which form the core of a security system.[6].

- Identification communicates an identity to an Information System (IS). The applicant provides an identity in the form of login or an email address, and the password to the IS.
- An authentication is a proof given by applicant to declare that he/she really corresponds to the identity which has been provided.
- Authorization to access information over network is given to the applicant after authentication.[6].

While designing a comprehensive secure system selection of authentication method plays a vital role. The same can be done in many ways and on numerous level so as to be customized and also user friendly as well. Authentication protocols are not only capable of simply authenticating the connecting party but also authenticating itself to connecting party.[8]
As a matter of study following are some of the authentication methods

- Password
- One Time Password
- Radio Frequency Identification

a. Passwords

Most extensively used form of authentication technique is Password. Users provide an login id, a typed in word or phrase or perhaps a token card, along with a password. Systems generally stored password in encrypted form in place of plain text. As authentication of this type is simple as compared to others authentication technique. The required hardware is not complicated or robust as this technique does not require much processing power [8].

Password authentication has many risk factors some of more obvious are:-

- Password may be easy to guess
- Writing the password down and placing it in a highly visible area
- Discovering passwords by eavesdropping or even social engineering.

However the risk of eavesdropping can be managed by using digest for authentication. The connecting party sends a value, typically a hash of the client IP address or an additional secret information. Because this hash is unique for each accessed URI, no other documents can be accessed nor can it not be used from other IP address without detection. The password is also not vulnerable to eavesdropping because of the hashing. The system is, however, vulnerable to active attacks such as the-man-in-the middle attack.[8]

b. One-Time Password-Mobile Transaction Authorization Number

In today's day to day transaction over network OTP is becoming very popular. The main advantage of OTP is that it avoid password list. One Time Passwords.(OTP) are utilized as an additional factor in multi-factor authorization/authentication applications. They are only valid for exactly one authorization or authentication request. OTP are send to the user via SMS.[9] The phone number of the user must be registered for the service that provides SMS OTPs for authentication or authorization. OTPs are quite popular as an additional authorization or authentication factor in web-based services.[10]

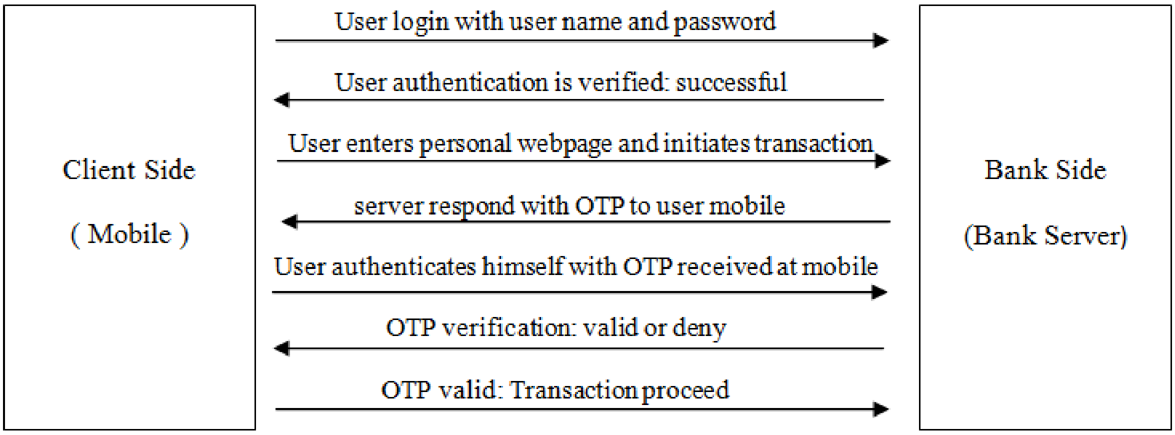

Client Side
(Mobile)
User login with user name and password
User authentication is verified: successful
User enters personal webpage and initiates transaction
server respond with OTP to user mobile
User authenticates himself with OTP received at mobile
OTP verification: valid or deny
OTP valid: Transaction proceed
Bank Side
(Bank Server)

Fig 3: OTP generation and User authentication

The conventional method of producing OTP whenever the user initiates a banking transaction is as follows:

1) The users go into the home page of the bank in which he has his account. He then enters his user name and password.
2) He is allowed to login into his webpage of his individual account, if the user authentication is valid.
3) The user then initiates a transaction.

4) Bank server responds back with OTP also called as [10] mobile Transaction Authorization Number (mobile TAN or mTAN) to his mobile or PDAs. This is the second level of authentication done to avoid password thefts.
5) The user then authenticates with OTP himself with OTP.
6) The OTP is checked at the server whether it is valid or not.
7) The transaction proceeds if valid.

There are two main advantages to OTP [11].

- In the first approach, called time-based OTP, the one-time password changes at numerous intervals (say, every two minutes).
- In the second approach, called event-based OTP, the one-time password is produced for every transaction or login from a different IP address.

5.3 Radio Frequency Identification (RFID)

To transmit a serial number wirelessly over radio waves first generation of RFID was used in the 1950's [6].Mostly it was used for military purpose. The use was limited to only identification purpose. In the early period, industry admits the use of tags and now it has become a successful authentication technique. Application range of RFID tags is very huge

- Item identification for inventory data
- Supply chain management
- Phones with RFID capabilities
- Authentication plastic cards

In our day to day transaction over network, internet plays a very important role .there is a very high need of security between communication capabilities to common items. To accomplish this, the presence of RFID tags will be very helpful as use of these tags has just begun in everyday's life. For example, a credit card with a built-in RFID system could be deducted by a wireless POS (Point of Sale), even if the card is still in the bag of its owner. The conventional protection against those attacks is a PIN code printed on the card, which is needed to unlock the chip. So the attacker will need to have the card in hand to read the code. Such a protection is used for RFID passports. It is considered as a trustable security systems that can be an alternative to password-based security system.[6]

VI. CONCLUSION

Every network system has facing the challenge of network security. More and more authorization of data is becoming secure by applying number of authentication technique in day to day transaction. Provided data can be authenticated by authentication technique. Some of them are simple and some are complex in the terms of implementation, hardware, costing etc. technique like plain password can easily be implemented .they do not required complicated or robust hardware as this technique does not want much processing power. Other methods are more complex and can take more time to implement and maintain but provide strong and reliable authentication. OTP technique has become very popular in the today's world as it provides large amount of security especially in the day to day banking transaction via mobile. RFID technique is also becoming useful in today's network system. Decision of selecting authentication technique plays an important role. Selection of proper authentication technique will definitely increase security to data on network. This paper discusses different types of network and network topology and makes a glance on very few authentication techniques but study on the same can be extended in a large scale.

REFERENCES

[1]. Sumedha Kaushik,Ankur Singhal,"Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, December 2012,pg no-105-107

[2]. Simmonds, A; Sandilands, P; van Ekert, L (2004)" Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285, pp.317–323.

[3]. Nancy katz,david lazer,holly arrow,noshir contractor, network theory and small groups, small group research, vol. 35 no. 3, june 2004 307-332 Doi: 10.1177/1046496404264941

[4]. Nivedita Bisht, Sapna Singh," analytical study of different network topologies", International Research Journal of Engineering and Technology (IRJET) Volume: 02 Issue: 01 | Mar-2015,pgno88-90

[5]. Santanu Santra,Pinaki Pratim Acharjya, "A Study And Analysis on Computer Network Topology For Data Communication", International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013),pg no 522-525

[6]. Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartz-Mann," A Review on Authentication Methods." Australian Journal of Basic and Applied Sci-ences, 2013, 7 (5), pp.95-107. <hal-00912435>

[7]. D. Bhattacharyya, R. Ranjan, Farkhod Alisherov A., and M. Choi. Biometric authentication: A review. International Journal of u- and e- Service, Science and Technology, 2(3):13–27, September 2009.

[8]. [8]. Richard Duncan, "An Overview of Different Authentication Methods and Protocols",October 23, 2001

[9]. Dr.Ananthi Shesashaayee, D. Sumathy, "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security"International Journal of Innovative Research in Computer and Communication Engineering,Vol. 2, Issue 10, October 2014,pgno-6192-6201

[10]. K. Rieck, P. Stewin, and J.-P. Seifert ,"SMS-Based One-Time Passwords: Attacks and Defense" dimva 2013, lncs 7967, Springer-Verlag Berlin Heidelberg 2013,pp. 150–159, 2013

[11]. Andrew Y. Lindell," Time versus Event Based One-Time Passwords", Aladdin Knowledge Systems, 2007