An Analysis of Advanced Authentication Techniques Emerging in Information Security

Sumrana Siddiqui
Assistant professor
Deccan College of Engineering &Technology

Abstract— Network and Information Security is now becoming important issue in the society as the society is transiting into the era of digital information. Data security is the utmost critical aspect that needs to be considered in ensuring safe transmission of information through the internet. It consists of authorization of access to information in an administrator controlled network. The task of Network security not only requires ensuring the security of the end systems but of the entire network. In this paper, an attempt has been made to analyse the various authentication techniques. The traditional authentication methods are considered along with the emerging authentication techniques. Furthermore, multi-factor authentication has been taken into account along with its advancements.

Key words: secure network, password

I. Introduction

With the advent of technology, internet is being considered the utmost necessity in our day to day life. With the ground breaking approaches of internet; information exchange has become feasible and convenient. The increased number of computer users has in turn resulted in the data being vulnerable to attacks and not being secure. Any kind of small negligence made towards the security factor of any one computer on a network can significantly affect the other computers connected on to the network. The first step towards security is the verification of the user identity popularly known as authentication. Traditional methods such as passwords were often used for authenticating the users. But this did not live up to the mark in preventing unauthorized access to computer resources when used solely for authentication. In this paper, I have brought into account the several authentication technologies that increase the security of the computers and the various pros and cons associated with these authentication technologies along with the next level of security which on being implemented can assure a higher secure environment.

II. The Objectives of Secure Network: The CIA Triad

Security aspects come into play when it is necessary to protect the transmission of information from an opponent possessing threat to the security. The consideration of the following factors leads to a secure environment:

1) Confidentiality: It refers to imposing restriction on the information and providing its access to the authorised users only.
2) Integrity: It refers to ensuring that the information gets modified only by the authorised user.
3) Availability: It refers to assuring that the systems and information is readily available to the authorized users for access.

For securing information, Authentication (i.e. authorised access) is considered as the major phase in the network security. Authentication refers to the assurance that the communicating entity is the one that it claims to be. In a connection-oriented transfer the Entity authentication provides confidence about the identity of the sender and receiver. In a connection-less transfer the message authentication provides confidence about the data and the source of data.

1) Message authentication: It is a technique consisting of a modification detection code which is a message (commonly known as a message digest) that after being passed through an algorithm known as cryptographic hash function creates a compressed image of the message. This provides the integrity of the message and assures that the message has not being changed or altered. To ensure the integrity of the message as well as to authenticate the origin of the message, the message detection code needs to be changed to message authentication code by prefixing it with a secret key. This take cares of the message authentication.
2) Entity authentication: It is a technique involving one entity proving the identity of another entity where the entity can be a person, a process, a client or the server. Claimant is the one whose identity needs to be proven and verifier tries to prove the identity of the claimant. The Table-1 below shows how Entity authentication supersedes Message authentication:

Message Authentication	Entity Authentication
Authenticates a single message at a time during data transfer	Authenticates the entire session of data transfer
Not a real time process	A real time process
Eg: Required when emails are sent	Eg: required when using cash vending machines

Table 1:

III. Conventional Methodologies of Entity Authentication

The traditional techniques of authentication are as follows:

A. Passwords:

The traditional method for authenticating users is to provide them with a secret password, which they must use when requesting access to a particular system. Password based authentication can be divided into the following:

1) Fixed password:

A fixed password is a password that is to be entered again and again for every access. To access the resources, the user sends the identification and password. If the password matches, the access is granted; otherwise, it is denied. There are several schemes that have been built one upon the other

2) One-time password:

A one-time password is a password that is used only once. Unlike the fixed passwords which are changed by the users every 60-90 days or longer, a one time password works in a completely different manner. One time passwords are generated by a mathematical algorithm that is only known to the security server. The user is provided with numbers that change every 60 seconds. The user logs on to the network and is requested to enter id and then the number (i.e. one time password). This information is sent via encryption to the server. If the One time password matches the mathematical algorithm and the id, then the user is authenticated. By combining the id with the Onetime password, the authentication is much stronger than that from the conventional fixed password scheme.

Password systems can be effective if managed properly, but they seldom are. Authentication which relies solely on passwords has often failed to provide adequate protection for computer systems for a number of reasons. Users tend to choose passwords that are easy to remember and henceforth such passwords are easy to decrypt. If passwords are generated automatically randomly, users often write them down because they are difficult to remember. The password authentication technique is vulnerable to attacks also. The Table-2 below lists down the attacks on this technique:

S.No	Attacks	Description
1	Eavesdropping	Trying to acquire the password when somebody is writing
2	Password Cracking	Guessing the password by trying different combinations
3	Password Hacking	Trying to Steal the password in person
4	Vulnerability analysis of password file	Tampering with the source computer and trying to access or change the password file
5	Dictionary Attack	Passing the password through the hash function and trying to attain the required password without knowing the id

Table 2:

B. Challenge-Response:

In this authentication technique the first party proves its knows a secret without sending it to the second party. The challenge here is a time varying random number sent by the second party and the response is the result of the function applied on the value. The response shows that the first party knows the secret.”CAPTCHA” is quoted as the best example of challenge response authentication test used in computing to determine whether or not user is a human. Eventually this technique has received many criticisms from disabled people and also from other people due to the distorted words that are illegible to users even with no disabilities that slow down the processing.

C. Zero-knowledge:

In this authentication technique the first party does not reveal anything that might endanger the confidentiality. The first party proves to the second party of knowing the secret, without revealing it. The technique is so designed that it does not lead to revealing or guessing the secret. After the information exchange only the second party knows that the first party does or does not have the secret, nothing more. The result is a single bit of information indicating a yes / no.

IV. ADVANCED METHODOLOGIES OF ENTITY AUTHENTICATION

The Advanced techniques of authentication are as follows:

A. Security-Tokens and Smart Cards:

Tokens can be compared with the keys of houses. In true sense tokens have many other factors are present along with them to provide information safety. In digital world security tokens used have passwords, so even when a token is lost no vital information can be modified. Bank cards, smart cards are security token storage devices with passwords and pass codes. Pass codes are same as password except that the former are machine generated and stored. There exist one time security tokens and smartcards also.

B. Biometrics:

Biometric Authentication is the process of verifying a user’s identity who they claim to be, using characteristic features of the users that cannot be guessed, stolen or shared. This can include finger prints, iris scans, face scans, voice recognition, retina scan, signature scans, vein scans and DNA. Biometric authentication requires:

1) Capturing devices, processors and storage devices
2) Database consisting of biological features of every individual
3) Authentication done either by verification or identification where in verification a person’s feature is matched against one record and in identification a person’s feature is matched against all records
4) Measuring the correctness using two parameters: False Rejection Rate and False Acceptance Rate

Biometric techniques can be broadly categorized into Physiological and Behavioural techniques. Physiological techniques consider and measure the biological traits of the human body for verification and identification. Behavioural techniques measure human behaviour trait. There are several Challenges that needs to be faced with Biometrics which are as follows:

1) Registration process must be done in a clean and safe environment.
2) Higher accuracy is needed when collecting the data from the users.
3) Data needs to be properly secured after being collected.
4) To keep a check on forgery of data.

Like every technology has it own loopholes, biometric also has. A few of it drawbacks that can be listed below in Table-3:

S.No	Technology	Drawbacks
1)	Voice Recognition	An illness can change an individual’s voice making the authentication cumbersome
2)	Retina	Carries a stigma along with it of being harmful to the eyes
3)	Iris	Requires a lot of memory for the data to be stored and is far too expensive.
4)	Finger Prints	Mistakes made when the skin or finger is dry or cracked

Table-3

V. Fuzzy Extractor: Advancement in Biometrics and Security

Recent research on biometrics deals with the concerns of safeguarding the data that is collected from the individuals and stored on the server. A way to deal with the security and privacy concerning the biometrics is the Fuzzy Extractors. They basically convert biometric data into random strings, to which cryptographic techniques can be applied for biometric security.

Fuzzy extractor is being considered a biometric tool which authenticates a user using its own biometric template as a key. They extract uniform and random string from its input .Due to some amount of noise if the input after being changed is close to the original value the random string can still be re-construct which outputs a helper string which can be made public without altering the security of the random string. The helper string is stored so that it can be used later to recover the random string. As fuzzy extractors deal with how to generate strong keys from Biometrics it applies cryptography techniques to biometric data by making little assumptions about the biometric data and applying cryptographic techniques to the input

Drawbacks: Because of the complexity in the method of data collection and data usage, information from the fuzzy extractor cannot be used to reconstruct a fingerprint or trace a user.

VI. Multifactor Authentication: A Trending Alternative to Safeguard the Network to its Maximum

Multifactor authentication is a method in which a user gets the access only after successfully presenting several evidences to authentication mechanism. To make network more secure, a combination of the authentication techniques are to be used. This is referred to as multi-factor authentication. Two factor authentications in ATM cards are the card itself and its password. So even if the card was lost or stolen, we can ensure that the safety is maintained until hacker's don't know the password. This is an example of combination of token and password authentication technique. But the combinations of biometric and passwords implementation are not so common because biometric usually includes sake for convenience. Combination of all three factors is required where there is a high need of security.

VII. Advent of Multifactor Authentication

Azure multifactor authentication is a method of verifying the identity that uses more than just a username and password. It provides a second layer of security to user sign-ins and transactions through the following easy verification options: Phone call, text message, notification, verification code. it helps protect access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication.

1) Features: Easy and simple to set up and use
2) Scalable: Utilizes the power of cloud
3) Always protected: Strong authentication using the highest industry standards
4) Reliable: Ensures all time availability

VIII. Challenges in Accomplishment of a Secure Network Environment

1) Developing a secure mechanism or an algorithm when considering the major hindrances to security.
2) Distribution of encryption information when security is attained using more than one algorithm or protocol.
3) An efficient implementation of the various security mechanisms.
4) Constant monitoring of an overloaded environment to attain security.
5) A highly secure environment should escalate a user friendly environment.

IX. Future Scope

Now a days there is a boon about having highly secured networks. These kind of networks can be attained by making use of more than one authentication techniques simultaneously. Henceforth in future an analysis can be done on the emerging and fascinating multi factor authentication techniques implemented.

X. Conclusion

Network or Information Security is unbelievably complicated. There is a requirement of technology that could make things easier and more convenient. Until then vigilant steps must be taken. Network security can be maintained by the user by making use of various authentication techniques that are present. The user can choose an appropriate authentication technique depending on the requirement. Of all the techniques the conventional Password based technique is best because it requires remembering of just a single password. But problems occur when we have to remember many passwords so we use those passwords that are easy to remember thereby compromising with the security. A token based technique provides added security against several service attacks. Similarly when it comes to Biometric technique it cannot be easily stolen so it provides stronger protection. But having the desire of a completely secure network is everyone's dream. To attain this a combination of several authentication techniques can be used simultaneously. Like it is said everything has it own advantages and disadvantages similarly all the authentication techniques also have their pros and cons. We have to be smart and wise enough to carefully choose an appropriate technique as per our requirement of safety of networks and information by considering the cost factor also.

Acknowledgement

I would like to sincerely express my gratitude to Dr. Arjumand Sattar and Mrs. Rehana Sultana for their consistent support and invaluable suggestions. I am also grateful to my family and my husband for having encouraged me on every step of mine to take this initiative of doing research.

References

[1] Anupriya Shrivastava, M A Rizvi ,"Network Security Analysis Based on Authentication Techniques", vol. 3,June 2014, pp.11-18

[2] Yevgeniy Dodis , Leonid Reyzin , Adam Smith , “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”
[3] Behrouz A. Forouzan ,Debdeep Mukhopadhyay ,Cryptography and Network Security, Tata McGraw Hill education Pvt. Ltd
[4] William Stallings, Cryptography and Network Security Principles and Practise, Pearson
[5] William Stallings, Network Security Essentials, Pearson
[6] www.wikipedia.com