Network Security Analysis based on Authentication Techniques

Sreeja S. S.
Assistant Professor
Thakur Institute of Management Studies, Career Development and Research, Mumbai, India

Parasmani Pal
Research Scholar
Thakur Institute of Management Studies, Career Development and Research, Mumbai,India

Prabhat Pandey
Research scholar
Thakur Institute of Management Studies, Career Development and Research, Mumbai, India

ABSTRACT

Unique—Network Security issues are currently getting to be critical as society is moving to advanced data age. Information security is the most extreme basic segment in guaranteeing safe transmission of data through the web. It involves approval of access to data in a system, controlled by the system manager. The assignment of Network security not just requires guaranteeing the security of end frameworks yet of the whole system. Verification is one of the essential and most generally methods for finding out and guaranteeing security in the system. In this paper, an endeavour has been made to investigate the different verification systems, for example, Knowledge-based, Token-based and Biometric-based and so forth. Moreover, we consider multi-calculate confirmations by picking a mix of above procedures and attempt to compare them

1. INTRODUCTION

In this advanced time increasingly individuals getting to be dynamic on the Internet for their own and expert, in light of this web is becoming quickly. Be that as it may, alongside the development of Networking and Internet, a few dangers, for example, Denial-of-Service (DOS) assaults and Trojan Horses have additionally risen definitely. So the errand of securing the Internet or even the Local Area Networks is presently at the bleeding edge of PC system related issues. Being on open system, genuine security dangers can be postured to an individual's individual data furthermore to the assets of organizations and government. Giving privacy, keeping up honesty and guaranteeing the accessibility of right data are the essential destinations. These dangers are principally present because of the numbness appeared by the clients, powerless innovation and poor plan of the system. Once in a while there are numerous system benefits that are empowered naturally in a PC or a switch. Out of which numerous administrations may not be vital and might be utilized by an assailant for data gathering. So it is ideal to han1dicap these undesirable administrations to shield them from programmers and wafers More significantly, not just should be concerned with respect to the security at every end of the system rather the attention ought to be on securing the whole system.

While building up a safe system, the accompanying should be considered -

1.1. Get To

Only approved clients are permitted to impart to and from a specific system.

1.2 Verification

This guarantees the clients in the system are who they say they are. Genuine stream of data can begin simply after the client has been validated and permitted to impart to different frameworks in the system.

1.3 Secrecy

Data in the system stays private. This is done to guarantee that the data can be seen just by confirmed frameworks and it can be accomplished utilizing different encryption methods.

1.4 Honesty

This guarantees the message has not been changed amid transmission.

2. DATA SECURITY AND AUTHENTICATION

Information Security is a testing issue in the field of information correspondences. For securing data from programmers and wafers, confirmation is the real stage in system security. It is an idea to secure system and information transmission over wired and additionally remote systems. Confirmation is one of the essential methods of guaranteeing that the individual who is transmitting the data is whom he says he is. It is in this way the way toward deciding the genuine character of clients, frameworks or some other substance in system. To confirm somebody's personality, secret key is for the most part utilized. To validate client or machines, diverse strategies can be utilized to perform verification amongst client and machine or machine and another machine as well. Diverse sorts of assaults are conceivable amid confirmation

Attack Types	Description
Weak password recovery	Websites permit hackers to find a way to illegally obtain, modify or recover another user's password
Brute force attacks	By trial and error, hackers can guess username, password, debit cards numbers, etc. This technique is highly popular
Insufficient authentication	Some websites don‟t authenticate much so hackers attack sensitive content
Shoulder surfing attacks	Hackers directly observe user while typing passwords or by some hidden cameras.

3. AUTHENTICATION TECHNIQUES

Taking after are the essential verification systems utilized as a part of the general population organize nowadays:

3.1. Secret word and stick based

In this verification system, protection and secrecy can be kept up to some degree. Clients remember there passwords and consequently we can term these as Knowledge-based systems. Passwords can be single words, numeric, phrases, any blend of these or individual distinguishing proof number. However, issue with this strategy is that remembered passwords can be effectively speculated or haphazardly sought by the programmers. Virtual Private Networks, for example, Point-to-Point Tunnelling Protocol (PPTP) make utilization of both clear-content conventions, for example, Password Authentication Protocol (PAP) and MD5-based conventions like Challenge Handshake Protocol (CHAP). As it is clear, MD5 ought to be favoured because of sniffing assaults. Plain passwords must be kept away from beyond what many would consider possible. They ought to be utilized just with SSL declarations.

Framework lists like „pg-authid‟ are utilized to store watchword for every client in database where we issue charges like CREATE, CREATE USER and ALTER ROLE to oversee passwords. For instance, CREATE USER jacks WITH PASSWORD data. On the off chance that no watchword has been set up for a client, the put away secret key will be NULL and secret key validation will dependably come up short for that client.

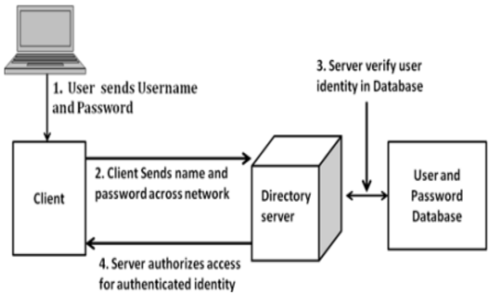
1. User sends Username and Password
3. Server verify user identity in Database
Client
2. Client Sends name and password across network
Directory server
User and Password Database
4. Server authorizes access for authenticated identity

Figure 1. Directory Server Based Authentication

Fig.1 indicates working of secret word based validation procedure. The client first enters a name and secret key. It is required that the Client application ties itself to the Directory Server with a recognized Name. The customer utilizes the name entered by client to recover area name. Next the customer sends these certifications to the Directory Server. The server then checks the secret key sent by the customer by looking at it against the watchword put away in database. On the off chance that it coordinates, the server acknowledges the accreditations for verifying the client personality. At that point the server permits customer so approved to get to the assets. In secret key based verification procedures, watchword arrangements are an arrangement of principles that additionally have significant parts in choosing how to oversee watchword in the frameworks. There are various arrangements bolstered by catalogue servers. „Default‟ and „Specialized‟ are both of them. The default secret key arrangement is a piece of the design for the example, once altered, it can't be recreated.

3.2 Token based

This is a physical device that performs authentication and hence can be termed as object based. Tokens can be compared with physical keys to houses that are used as a token but in digital tokens many other factors are present to provide information safety. In digital world, security tokens are used. Tokens themselves have password so even if they are lost, the hackers cannot modify the vital information. Bank cards, smart cards are security token storage devices with passwords and pass codes. Pass codes are same as password except that the former is machine generated and stored. There exist one-time security tokens and smartcards as shown in Fig. 2.

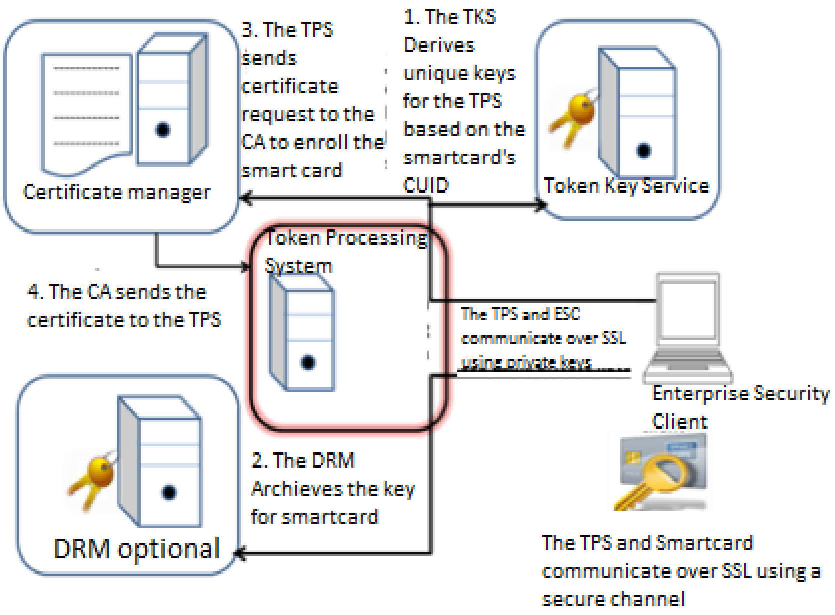
3. The TPS sends certificate request to the CA to enroll the smart card
1. The TKS Derives unique keys for the TPS based on the smartcard's CUID
Certificate manager
Token Key Service
Token Processing System
4. The CA sends the certificate to the TPS
The TPS and ESC communicate over SSL using private keys
Enterprise Security Client
2. The DRM Archieves the key for smartcard
DRM optional
The TPS and Smartcard communicate over SSL using a secure channel

Figure 2. Token Based Authentication

4. AUTHENTICATION IN SECURITY SYSTEM

4.1 One-time Security Tokens

Ron Rivest, Adi Shamir and Leonard Adleman (RSA) calculation utilizes one time security token, that is, secureID which diminishes the hazard when contrasted with a straightforward secret word as we may change our passwords as indicated by our temperament in each 60 to 90 days or might be longer. In any case, secureID works contrastingly as it changes like clockwork, which is created by some scientific calculations and just known to security server. As client logs on to the organization arrange, he enters his ID and afterward the some arbitrary number showed on the screen. By encryption this data is sent to the security server. So client gets verified just when the number that show on the screen coordinates the numerical calculation and the ID. Mix of client ID known to the client and OTP makes this confirmation much more grounded. Fig 3 demonstrates the succession of occasions that ordinarily happen amid the procedure of OTP.

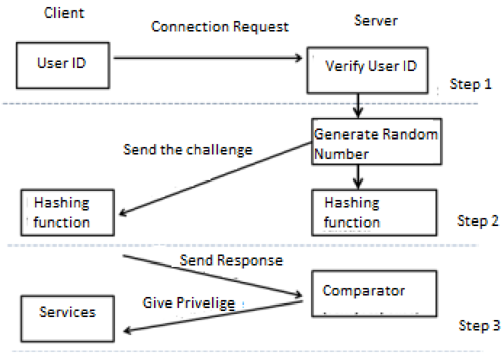

Figure 3: Mechanism for OTP method

4.2 Biometric Based

Biometric verification is the way toward checking if a client is whom he is guaranteeing to utilize, digitized organic marks of the client. Biometric validation can be characterized into two gatherings: physiological and behavioural. In physiological verification, confronts, fingerprints, hands, iris and retina take after. What's more, on account of behavioural, voice prints, marks and keystrokes are utilized. This system can term as ID based. This procedure is more secure when contrasted with secret key and token based strategies. Biometric confirmation procedures are as of now in operation in different endeavours. They are utilized for international IDs, visas, individual distinguishing proof cards, getting to bank machines, entryway get to control, and general PC desktop get to.

Technology Characteristics	Facial	Hand	Iris	Finger Print
Work	Capture facial pattern and compare it	Measures dimension of hand and compare it	Capture iris pattern and compare it	Capture fingerprint pattern and compare it
Effect with Age	Variable	Constant	Constant	Constant
Performance	Low	Medium	High	High
Performance Affected by	Lighting and sunglasses	Hand injuries.	Poor eyesight	Poor eyesight
Device Cost	Moderate	Moderate	High	Low

Advantage	Can capture the sample from distance	Easy only compare dimension of hand	Most accurate, one sample can last for lifetime	Economic and easy
Disadvantage	poor light can cause difficulty in matching the sample	User acceptance issue is hygiene concern	Expensive	Time taking

5. COMPARSION OF STRENGTH OF PARAMETER OF AUTHENTICATION MECHANISM

For looking at the above three verifications, we consider three vital elements appeared in the Graph 1 and at last figure the composite of each one of those components to decide the Binding quality which turns into the single purpose of correlation. However, the model that we use to discover this esteem makes utilization of individual shortcomings as opposed to person qualities where shortcoming = 1/quality. Accordingly, we get the accompanying condition:

Restricting Weakness = Discriminatory Weakness + Procedural Weakness + Technical Weakness

Having setup the above condition, we decide the individual qualities according to the accompanying parameters:

5.1. Segregation Strength

For passwords, number of endeavours in a characterized day and age. If there should be an occurrence of tokens, we consider their unmistakable number. While, for Biometrics, we have to discover the quantity of various endeavours practical.

5.2. Specialized Strength

For all the three validation instruments, security assessment process is done.

5.3. Procedural Strength

This is difficult to decide as it might rely on upon numerous ecological components, for example, site security and staffs teaches. In any case, still we utilize a particular arrangement of parameters to gage the esteem, for example, length, arbitrariness and recurrence of progress on account of Passwords; physical security and client train for the situation of Tokens and for Biometrics, inalienable quality is adequate. Next, we substitute these qualities into the above condition and decide the Binding Strength for each validation instrument.

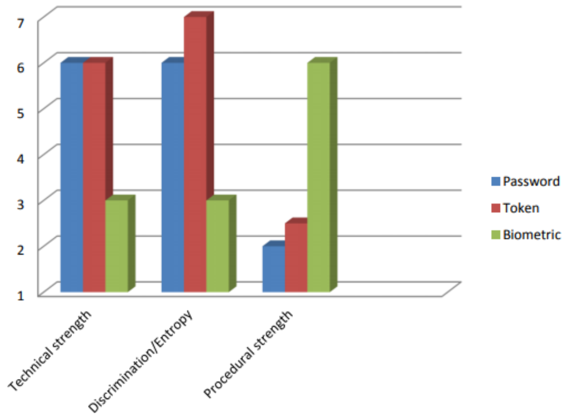

Figure 4. Comparison of Strength of Various Parameters

Technology Characteristics	Password Based	Token Based	Biometric Based
Ease of operation	Simple	Simple	Simple
Hardware Used	No need of extra hardware	Require smart card for each services	No need of extra hardware
Initial Cost	Moderate as it requires simple computer system, laptop and mobile	Moderate because only smart cards are required.	High as it requires specialized hardware, which is also difficult to install in normal systems
Running Cost	Expense on system maintenance	Expense of card maintenance	Expense of maintaining and managing special hardware
Changes	Changed as per user convenience	Can be changed	Never changed
Client Attacks	Guessing the password by trial and error	Exhaustive search	False match
Host Attacks	Plaintext theft	Pass code can be stolen	Template can be stolen
Denial of service	Lockout by multiple failed authentication	Lockout	Lockout

In the wake of breaking down the Fig.4 and Table III, it can be condensed that innovation attributes of the three distinctive validation systems including their simplicity of operation, equipment prerequisite, beginning setup cost, running expense and powerlessness to assaults, for example, Denial-of-Service (DOS), technical quality and procedural quality. Watchword based confirmation gives high key space and hashing which shields from host assaults. It is helpful and reasonable procedure. Token based validations are essentially heartier against assaults on account of twin secret key blend. In contrast with above two procedures, biometric can't be effectively stolen so it gives more grounded insurance yet it is excessively costly for individual utilize. So as indicated by utilize individuals can pick the verification procedure according to their need and affectability of information and cost accessible, on the grounds that nobody strategy can be proposed according to the examination done.

6. MULTIFACTOR AUTHENTICATION

To make organize more secure, a blend of above methods should be utilized as appeared as a part of Table 4. This is alluded to as multi-element confirmation. For system security, every authenticator result must be fulfilled. As a Boolean AND operation is performed for each factor’s verification comes about, so all must be agreed. Two figure confirmations ATM cards are the card itself and its secret word. So regardless of the possibility that the card was lost or stolen, we can guarantee that the wellbeing is kept up until programmers don’t know cards secret word. This case of token in addition to secret key are generally actualized today. Different mixes of token and biometric ID are additionally considered as secure procedures if it’s troublesome for client to recollect passwords, however they require exorbitant machines. Be that as it may, the blends of biometric and passwords execution is not all that basic in light of the fact that biometric for the most part incorporates purpose for accommodation. Blend of every one of the three components is required where there is a high need of security. Till now such a blend is not very connected. Mixes of various strategies are appeared in Table IV.

Authenticator combination	**Password-token based**	**Password-biometric base**	**Token-biometric based**	**Password-token-and biometric based**
Security	Good	Better	Better	Best
Cost	Moderate	High	High	High
Advantage	Lost token is secure, as protected by password	Biometric provide security if password is forgotten also.	Lost token is secure as protected by biometric ID	Three factors provide add on security.
Drawback	Memorize password and always carry token	Memorize password and have biometric ID	Always have to carry id, but not if it is a Biometric	Have to memorize password, carry Token and have Biometric ID
RealLife Example	ATM cards	Password-Biometric for any machine access	Photo ID prop as driving license	Where high security require like MILITARY,PARLIAMENT etc.

7. CONCLUSION

Network security can be kept up by making utilization of different verification procedures. Client needs to utilize verification procedure relying upon necessity. Watchword based strategy is ideal in the event that you need to recollect a solitary secret word. Be that as it may, issues happen when we need to recollect numerous passwords so we utilize those passwords that are anything but difficult to recall. Token based systems give included security against foreswearing of administration (DoS) assaults. In contrast with above two, systems biometric can't be effortlessly stolen so it gives more grounded security. As signs, biometric can be effortlessly duplicated by assailants so it ought not be sent in single variable mode. Besides we can pick a mix of above system as examined previously. Every one of the methods have their advantages and disadvantages. We must be savvy to pick according to our necessity of security of systems and data by considering cost calculate moreover.

8. ACKNOWLEDGMENT

It gives us immense pleasure to present this Research Paper. We grab this opportunity to express our heartfelt obligation towards the people without whom completion of this Research

Paper have not been possible. We would like to thank our guide Prof. Sreeja.S.S for her immense support and continuous encouragement to our team.

9. REFERENCES

[1] http://www.authenticationworld.com/Token-Authentication.

[2] http://www.authenticationworld.com/Authentication-Biometrics.

[3] http://www.duosecurity.com.

[4] http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication%20Technique.pdf