Ensuring Multi Factor Authentication Services for Smart Card in the Network

[a]G.Rajeshwari, [b] Radhika Thalla [c]Swapna Motupally,
[a] Lecturer, Dept. of Computer Science, St. Francis College for Womens, Hyderabad, TS, India
[b] Lecturer, Vignana Jyothi Institute of Arts & Sciences, Secunderabad, TS, India
[c] Technical Trainer, TASK, Hyderabad, TS, India

Network Security issues are now becoming important as society is moving to digital information age. Data security is the utmost critical component in ensuring safe transmission of information through the internet. It comprises authorization of access to information in a network, controlled by the network administrator. The task of Network security not only requires ensuring the security of end systems but of the entire network. Authentication is one of the primary and most commonly ways of ascertaining and ensuring security in the network. In this paper, an attempt has been made to analyze the various authentication techniques such as Knowledge-based, Token-based and Biometric-based etc. Furthermore, we consider multi-factor authentications by choosing a combination of above techniques and try to compare them.

KEYWORDS— Authentication; Denial of service; Virtual Private Network; Passcode; Smart card; RSA; Secure-ID; Biometric

---

I. INTRODUCTION

In this digital era more and more people becoming active on the Internet for their personal and professional, because of this internet is growing rapidly. But, along with the evolution of Networking and Internet, several threats such as Denial-of-Service (DOS) attacks and Trojan Horses have also risen drastically. So the task of securing the Internet or even the Local Area Networks is now at the forefront of computer network related issues. Being on public network, serious security threats can be posed to an individual's personal information and also to the resources of companies and government. Providing confidentiality, maintaining integrity and assuring the availability of correct information are the primary objectives. These threats are primarily present due to the ignorance shown by the users, weak technology and poor design of the network. Sometimes there are many network services that are enabled by default in a personal computer or a router. Out of which many services may not be necessary and may be used by an attacker for information gathering. So it is better to disable these unwanted services to protect them from hackers and crackers More importantly, not only need to be concerned regarding the security at each end of the network rather the focus should be on securing the entire network.

While developing a secure network, the following need to be considered –

1. **Access** – Only authorized users are allowed to communicate to and from a particular network.

2. **Authentication** – This ensures that the users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.

3. **Confidentiality** – Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various encryption techniques.

Integrity – This ensures that the message has not been changed during transmission.

II. DATA SECURITY AND AUTHENTICATION

Data Security is a challenging issue in the field of data communications. For securing information from hackers and crackers, authentication is the major phase in network security. It is a concept to protect network and data transmission over wired as well as wireless networks. Authentication is one of the primary techniques of ensuring that the person who is transmitting the information is whom he says he is. It is thus the process of determining the actual identity of users, systems or any other entity in network. To verify someone's identity, password is mostly used. To authenticate user or machines, different techniques can be used to perform authentication between user and machine or machine and another machine too. Different types of attacks are possible during authentication.

III. AUTHENTICATION TECHNIQUES

Following are the primary authentication techniques used in the public network these days:

A. Password and pin based:

In this authentication technique, privacy and confidentiality can be maintained up to some extent. Users memorize there passwords and hence we can term these as Knowledge-based techniques. Passwords can be single words, numeric, phrases, any combination of these or personal identification number. But problem with this technique is that memorized passwords can be easily guessed or randomly searched by the hackers. Virtual Private Networks such as Point-to-Point Tunneling Protocol (PPTP) make use of both clear-text protocols such as Password Authentication Protocol (PAP) and MD5-based protocols like Challenge Handshake Protocol (CHAP). As it is clear, MD5 should be preferred due to sniffing attacks. Plain passwords must be avoided as far as possible. They should be used only with SSL certificates.

System catalogs like „pg-authid" are used to store password for each user in database where we issue commands like CREATE, CREATE USER and ALTER

ROLE to manage passwords. For example, CREATE USER jacks WITH PASSWORD info. If no password has been set up for a user, the stored password will be NULL and password authentication will always fail for that user.

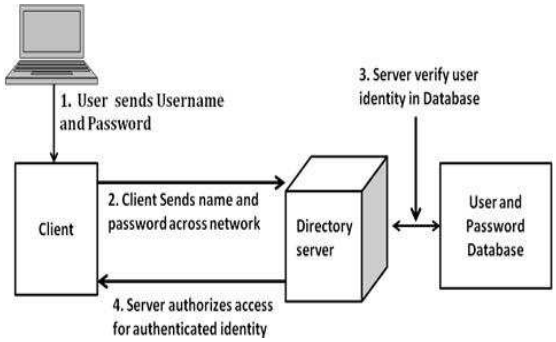

Fig. 1Directory Server based authentication

Fig.1 shows working of password based authentication technique. The user first enters a name and password. It is required that the Client application binds itself to the Directory Server with a distinguished Name. The client uses the name entered by user to retrieve domain name. Next the client sends these credentials to the Directory Server. The server then verifies the password sent by the client by comparing it against the password stored in database. If it matches, the server accepts the credentials for authenticating the user identity. Then the server allows client so authorized to access the resources.

In password-based authentication techniques, password policies are a set of rules that also have major roles in deciding how to administer password in the systems. There are multiple policies supported by directory servers. „Default" and „Specialized" are the two of them. The default password policy is part of the configuration for the instance, once modified, it cannot be replicated.

One time security tokens:

Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm uses one time security token, that is, secureID which reduces the risk as compared to a simple password as we may change our passwords according to our mood in every 60 to 90 days or may be longer. But secureID works differently as it changes every 60 seconds, which is generated by some mathematical algorithms and only known to security server. As user logs on to the company network, he enters his ID and then the some random number displayed on the screen. By encryption this information is sent to the security server. So user gets authenticated only when the number that display on the screen matches the mathematical algorithm and the ID. Combination of user ID known to the user and OTP makes this authentication much stronger. Fig 3 shows the sequence of events that normally occur during the process of OTP.

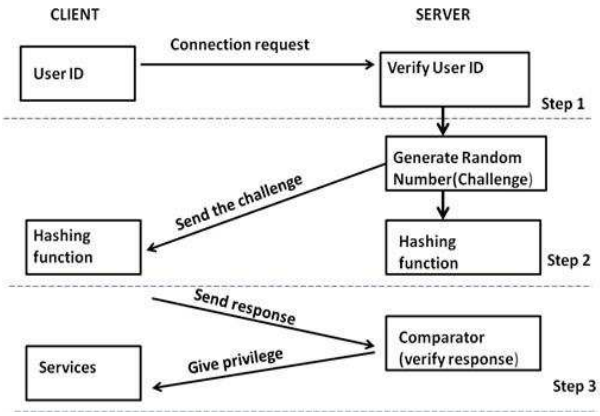

Fig.2 Mechanism for OTP method

Biometric Based:

Biometric authentication is the process of verifying if a user is whom he is claiming to be, using digitized biological signatures of the user. Biometric authentication can be classified into two groups: physiological and behavioural. In physiological authentication, faces, finger prints, hands, iris and retina follow. And in the case of behavioral, voice prints, signatures and keystrokes are used. This technique can term as ID based. This technique is safer as compared to password and token based techniques. Biometric authentication techniques are currently in operation in various enterprises. They are used for passports, visas, personal identification cards, accessing bank machines, doorway access control, and general computer desktop access.

IV. COMPARSION OF STRENGTH OF PARAMETER OF AUTHENTICATION MECHANISM

For comparing the above three authentications, we consider three important factors shown in the Graph 1 and finally calculate the composite of all those factors to determine the Binding strength which becomes the single point of comparison.

But, the model that we use to find out this value makes use of individual weaknesses rather than individual strengths where weakness = 1/strength. As a result, we get the following equation:

Binding Weakness = Discriminatory Weakness + Procedural Weakness + Technical Weakness

Having setup the above equation, we determine the individual strengths as per the following parameters:

1. Discrimination Strength: For passwords, number of attempts in a defined time period. In case of tokens, we consider their distinct number. Whereas, for Biometrics, we need to find out the number of different attempts feasible.

2. Technical Strength: For all the three authentication mechanisms, security evaluation process is carried out.

3. Procedural Strength: This is hard to determine as it may depend on many environmental factors such as site security and staff discipline. But, still we use a specific set of parameters to gauge the value such as length, randomness and frequency of change in the case of Passwords; physical security and user discipline in the case of Tokens and for Biometrics, inherent strength is sufficient.

Next, we substitute these values into the above equation and determine the Binding Strength for each authentication mechanism.

After analyzing the Fig.1, it can be summarized that technology characteristics of the three different authentication mechanisms including their ease of operation, hardware requirement, initial setup cost, running cost and vulnerability to attacks such as Denial-of-Service (DOS),technical strength and procedural strength. Password based authentication provides high key space and hashing which protects from host attacks. It is convenient and inexpensive technique. Token based authentications are significantly more robust against attacks because of twin password combination. In comparison to above two techniques, biometric cannot be easily stolen so it provides stronger protection but it is too expensive for personal use. So according to use people can choose the authentication technique as per their need and sensitivity of data and cost available, because no one method can be suggested as per the analysis done.

V. MULTI FACTOR AUTHENTICATION

To make network more secure, a combination of above techniques need to be used as shown in Table 4. This is referred to as multi-factor authentication. For network security, each authenticator result must be satisfied. As a

Boolean AND operation is performed for each factor‟s authentication results, so all must be affirmative. 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 hackers don‟t know cards password. This example of token plus password are mostly implemented today. Other combinations of token and biometric ID are also considered as secure techniques if it‟s difficult for user to remember passwords, but they require costly machines. 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. Till now such a combination is not highly applied. Combinations of different technique are present.

CONCLUSION

Network security can be maintained by making use of various authentication techniques. User has to use authentication technique depending on requirement. Password based technique is best if you have to remember a single password. But problems occur when we have to remember many passwords so we use those passwords that are easy to remember. Token based techniques provide added security against denial of service (DoS) attacks. In comparison to above two,

techniques biometric cannot be easily stolen so it provides stronger protection. As signals, biometric can be easily copied by attackers so it should not be deployed in single factor mode. Furthermore we can choose a combination of above technique as discussed above. All the techniques have their pros and cons. We have to be smart to choose as per our requirement of safety of networks and information by considering cost factor also.

REFERENCES

[1] Lawrence O"Gorman, "*Comparing Passwords, Tokens, and Biometrics for User Authentication*", Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.

[2] Hafiz Zahid Ullah Khan, "*Comparative Study of Authentication Techniques"*, IJVIPNS-IJENS Vol: 10 No: 04.

[3] [Online]Available: http://www.authenticationworld.com/Token-Authentication.

[4] [Online]Available: http://www.authenticationworld.com/Authentication-Biometrics.

[5] Jae-Jung Kim and Seng-Phil Hong, "*A Method of Risk Assessment for Multi-Factor Authentication*", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[6] Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast *Authentication in the Smart Grid with One Time Signature*", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.

[7] [Online]Available: http://www.duosecurity.com.

[8] [Online]Available:http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication%2 0Technique.pdf.

[9] Stamati Gkarafli, Anastasios A. Economides, "*Comparing the Proof by Knowledge Authentication Techniques*", international Journal of Computer Science and Security (IJCSS), Volume (4): Issue (2).

[10] Roger Meyer, "*Secure authentication on the internet*"As the part of security reading room, SANS institute 2007.

[11] R. Dhamija, and A. Perrig,"Déjà Vu: "*A User Study Using Images for Authentication*", 9th USENIX Security Symposium, 2000.

[12] R. Morris, K. Thompson, "*Password security: A case history*," Comm. ACM, Vol.22, no. 11, Nov. 1979, pp. 594-597.

[13] B. L. Riddle, M. S. Miron, J. A. Semo, "*Passwords in use in a university timesharing environment*,"
Computers and Security, Vol. 8, no. 7, 1989, pp. 569-579.

[14] S. M. Bellovin, M. Merritt, "*Encrypted key exchange: Password-based protocols secure against dictionary attacks*," Proc. 1992 IEEE Computer Society Conference on Research in Security and Privacy, 1992, pp. 72-84.

[15] R. Pond, J. Podd, J. Bunnell, R. Henderson, "*Word association computer passwords: The effect of formulation techniques on recall and guessing rates"*, Computers and Security, Vol. 19, no. 7, 2000, pp. 645-656.

[16] S. M. Furnell, P. S. Dowland, H. M. Illingworth, P. L. Reynolds, "*Authentication and supervision: A survey of user attitudes*," Computers and Security, Vol. 19, no.6, 2000, pp. 529-539.

[17] Harbitttr, A. and Menasce, D.A., "*A Methodology for Analyzing the Performance of Authentication Protocols*", November 2002.

[18] Haq, I. U. and Yahya, K. M. "*Heterogeneous Networks: Challenges and Future Requirements"*.

[19] TSENG, Y.M., YANG, C.C. AND HAUR SU, J. *"Authentication and Billing Protocols for the Integration of WLAN and 3G Networks*", 2004.

[20] Li, S., Zhou, J., Li, X. and Chen, K. "*An Authentication Protocol for Pervasive Computing"*.

[21] Misbahuddin, M., Premchand, P. and Govardhan, A. "A *User Friendly Password Authenticated Key Agreement for Multi Server Environmen*t", November 2009.