Comparative Study of Authentication Techniques

Hafiz Zahid Ullah Khan
Institute of Information Technology University of Science & Technology, Bannu Khyber Pakhtoon Khwa, Pakistan
E-mail: iamzahid76@hotmail.com

***Abstract*-- The Internet has emerged as one of the most convenient and widely used media for exchanging information. The Internet of today is faced with many challenges. One of the most daunting challenges is to ensure security. Pursuing authentication through appropriate mechanisms becomes a complex issue. Like other network applications, security issues have become the core issues to be settled. Among other security issues, authentication and access control are the two main fields of security issues, which must be resolved to protect information and computing systems against unauthorized access. This paper explores three authentication techniques i.e.(i) Single Factor /Knowledge based (ii) Two Factor /Token based and (iii) Three Factor/Biometric based authentication and suggest/propose which technique will protect privacy to authenticate users in an appropriate manner.**

***Index Term*-- Access Control Attacks Authentication Biometrics Identification Privacy Web Security**

1. INTRODUCTION

In the early days of computing, major kinds of threats were viruses, worms and Trojans, but now a days these slowly propagating threats have been replaced by threats that propagate around the world within less than 15 minutes [10]. The nature of today's web threats is changing-current attacks are much more covert than they were in the past. Decision makers need to understand the nature of the threat they face. This made web, network and application security extremely difficult issues. Despite the growing array of threats, many organizations are not taking appropriate steps to safeguard their corporate networks, applications or data. As the number of online services are increasing day by day, their usage is also increasing in the same ratio. Users of online services have to register separately to each application and the overhead of remembering many ID/Password pairs has led to the problem of memorability. Wireless Internet Service Providers (WISPs) implemented web based authentication mechanism which gained popularity for the reason it allows a simple registration and authentication of customers [18].

Authentication is a direct need of each and every organization and so it is becoming paramount for an organization not because it copes with security threats only but for the reason it deals with and develops policies, procedures and mechanisms that provide administrative, physical and logical security. Whenever an individual requests an access to a pool of resources, to use them or update them as desired, then to authenticate such an individual is referred to as authentication [25]. Computer industry has created an array of identification and authentication technologies like userID/Passwords, One Time Password, Biometrics, Smartcards, Kerberos, Secure Socket Layer, Lightweight Directory Access Protocol, Security Assertion Markup Language(SAML), OpenID and CardSpace to address varying business and security requirements [11]. Each organization adopts one or more of these technologies to secure information against misuse and un-authorized access. In networked environment, users are granted access to the network only when they provide their access information (e.g. user name & password) securely to check and validate their identity. If a person can prove that who he is, also knows something that only he could knows, it is reasonable to think that a person is he who claims to be. The purpose of personal authentication is to ensure that the rendered services are being accessed only by a legitimate user.

Due to recent events of thefts and terrorism, authentication has become more important for an organization to provide an accurate and reliable means of authentication. Authentication interface is an example of security interface as used by electronic commerce (e-commerce) web sites [19]. In many applications such as e-voting and Internet banking, it is not necessary to know who an entity actually is, but to be sure that he/she possesses the proper rights to perform the desired action. Every user of such applications wants assurance that what he sees on the screen of a computer is really the content sent from a trusted provider or displayed by a trusted application. This is exactly the purpose of authentication and authorization infrastructures. In b2c e-commerce applications, it is not necessary to ask someone "Who are you?" but rather " Are you allowed to perform a certain request " [4].

Different organizations have different authentication requirements and so they employ different authentication techniques. But whatever the authentication technique is employed, the main goal of authentication is to increase the level of assurance of valid users and to stop the imposters/unauthorized users to access the system. This paper attempts to explore authentication techniques. Our proposed system will be more reliable than the authentication systems used so far and the secret information will be harder to be theft or stolen.

The rest of the paper is organized as follows: section 2 defines some basic terminologies, section 3 discusses various types regarding authentication, section 4 discusses authentication schemes, section 5 compares authentication schemes, section 6 summarizes the comparison, section 7 presents limitations and weaknesses, section 8 concludes and section 9 is about acknowledgement.

2. BASIC DEFINITIONS

Before delving into authentication schemes used so for, it will be useful to establish some basic definitions here.

2.1 AUTHENTICATION: Authentication means enabling the network to only admit the authorized users to have access to its resources. It provides the way where the claimed identifier is verified by the access control mechanisms through some means.

2.2 ACCESS CONTROL: The discipline in which mechanisms and policies are established that restrict access to the computer resources only to correct users.

2.3 IDENTIFICATION: It is a way where a resource claims (or is identified through other means) a specific and unique identifier.

2.4 AUTHORIZATION: Which determines the privileges associated with authenticated identity.

2.5 SECURITY: The ability of a system to protect data, services and resources against misuse by un-authorized users.

2.6 PRIVACY: The ability of a system to protect the identity and location of its users from un-authorized disclosure.

2.7 SMART CARD: A small pocket sized plastic card used to make payments and store personal information and which can be read when connected to computer system. It is widely used as hardware token in financial transaction systems especially in Internet based.

2.8 E-VOTING: E-voting is also known as Electronic Voting, is electronic means of casting a vote and electronic means of counting votes. It can involve transmission of ballots and votes via telephone's private computer network or the Internet.

3. AUTHENTICATION ATTACKS

Attacks regarding authentication are those which target a web site's method of validating the identity of a user, service or application. These are of the following types.

3.1 BRUTE FORCE ATTACK: It is an automated process of trial and error used to guess a person's user name, password, credit card number or cryptographic key. A normal brute force attack uses a single user name against many passwords. A reverse brute force attack uses many user names against one password. When a guessed password allows access to the system, the brute force attack has been successful and the attacker is able to access the account.

Brute Force techniques are highly popular and often successful in systems with millions of user accounts.

Example:

Username = Michael

Passwords = Faraday, Jordan, Osterman, [pet names], [birthdays], [car names]

Usernames = Dad, Jon, Barbara, Ed, Sara

Password = 12345678

3.2 INSUFFICIENT AUTHENTICATION: This type of attack occurs when a website permits an attacker to access sensitive content or functionality without having to properly authenticate. Web based administration tools are a good example of web site providing access to sensitive functionality.

Example:

Many web applications have been designed with administrative functionality location directory off the root directory (/admin/). This directory is usually never linked to anywhere on the web site, but can still be accessed using a standard web browser.

3.3 WEAK PASSWORD RECOVERY VALIDATION: When a website permits to illegally obtain, change or recover another user's password. Conventional web site authentication methods require users to select and remember a password. The user should be the only person that knows the password and it must be remembered precisely. With the passage of time, a user's ability to remember a password fades. The complication increases further when the average user visits 20 or more sites requiring them to supply a password. A website is considered to have Password Recovery Validation when an attacker is able to foil the recovery mechanism being used. This happens when the information required to validate a user's identity for recovery in either easily guessed or can be circumvented. Password recovery systems may be compromised through the use of brute force attacks, inherent system weaknesses or easily guessed secret questions.

Example of automated password recovery processes include requiring the user to answer a "secret question " defined as part of the user registration process. The second mechanism in use is having the user provide a " hint " during registration that will help the user remember his password.

Example:

(Weak methods of Password Recovery)

3.3.1 Information Verification:

Many web sites only require the user to provide their e-mail address in combination with their home address and telephone number, which can be obtained from any number of online white pages easily.

3.3.2 Password Hints:

Password hint aids Brute Force attacks. An attacker can glean about user's password from the hint provided.

3.3.3 Secret Question and Answer:

A user's password could be "KARACHI" with a secret question of "Where were you born?" which helps an attacker to limit a secret answer Brute Force Attack to city names. Besides this, if the attacker knows a little about the target user, learning their birthplace is also an easy task.

3.4 SHOULDER SURFING ATTACK: It is that type of attack when the attacker tries to guess the password by direct observation or by using spy cameras to capture the user entering the password.

3.5 PHISHING ATTACK: It is the attempt to criminally and fraudulently get/acquire sensitive information i.e. user name, password and credit card details etc.

3.6 RECONNAISANCE ATTACK: The act of learning information about the target using publicly available information.

4. SCHEMES OF AUTHENTICATION

Usually user authentication involves confirming with a certain degree of confidence that the electronic form of user's identity represented in the IT System corresponds to the real life identity of the user. There are three factors of user authentication that may be used in combination to increase the level of confidence in the claimed identity of a user.

4.1 SINGLE FACTOR/KNOWLEDGE-BASED AUTHENTICATION:

This type of authentication technique consists of text base that uses passwords or Personal Identification Numbers (PINs) and graphic based authentication that uses graphics for authentication.

Knowledge based authentication uses secret information. When user provides some information to authenticate himself as a legitimate user, the system processes this information and suggests whether the user is legitimate or not.

Knowledge based authentication is based on " Something You Know " assumption, in which the user types a password to login to a computer or enters his Personal Identification Number (PIN) to access his/her bank account from an ATM. The classic form of single factor authentication is userID and Password. Where the user claims his/her identity by presenting a userID to the IT access control system. The system then checks the password for the claimed identity against its secure list of known identities and passwords.

If the userID and Password pair, entered by the user, match the UserId and password stored in the IT access control system, then the user is judged to be authentic and given access to the system.

4.2 TWO FACTIOR/TOKEN BASED AUTHENTICATION: This scheme uses some physical items called tokens such as smart cards, passports and physical keys. Authentication token or simply a token may be a physical device that an authorized user of computer is given to aid in authentication. Such a token may be physically connected or plugged into the client system. The term may refer to software token as well. Hardware tokens are typically small enough to be carried out in a pocket or purse and often are designed to attach to the user's keychain. Some may store cryptographic keys such as a digital signatures or biometric data such as a fingerprint. Other may include small keypads to allow the entry of a PIN.

Token based authentication is based on " Something You Have " assumption, in which the user carries a wallet full of credentials (a driver's license, credit card, a university ID card) to certify his/her identity (as a driver, as a credit worthy consumer, or as a student). This system uses both forms of authentication. i.e. it involves using " Something You Know"(i.e. a PIN) and " Something You Have"(i.e. a token). Most widely used forms of two factor authentication are.

(i) Automated Teller Machine(ATM) or Cashpoint Machine Card and PIN.

(ii) Access Control Token and PIN.

At an ATM, the user puts his/her Cashpoint/ATM card into the ATM and the ATM requests the user to enter his/her PIN. The information held on magnetic stripe of the card together with the PIN, encrypted in a secure block of data, is sent to the Bank's Central Authentication System, where the PIN entered by the user, is compared with the PIN held on file against the user's account number and details.

However, in this scheme, personally designed unique information is used as token. Each user is registered against that unique token which becomes his identifying label of the token. Stored information is presented to the system (e.g. ATM card) as well as PIN code to authenticate a user.

4.3 THREE FACTOR/BIOMETRIC-BASED AUTHENTICATION: Three factor authentication or Biometric based authentication involves using an access control token such as smart card, a PIN to access the smart card and a biometric value held in the central database. The card is entered into a reader, the PIN is entered, the biometric is read and encrypted under a cryptographic key held on the smart card. The userID read from the smart card together with the encrypted biometric are sent to the central database, where the biometric can be decrypted and compared with the value on the central access control system/database. It is to be noted that the user's PIN is not sent to the central access control system but is checked locally by the smart card.

Biometrics is the technologies that analyze human characteristics for automated personal authentication. In this scheme, behavioral characters (i.e. voice signature, gait of a human) as well as psychological characters (i.e. fingerprint, hand, iris, retina, face) describing human characteristics are used for authentication. Biometric based authentication is used for both authentication as well as for identification. In short, this system uses some physical or behavioral traits of a human for authentication.

5. COMPARISON AMONG AUTHENTICATION SCHEMES

Knowledge based authentication has the following flaws.

(i) It is harder to remember passwords for a long time. With the passage of time, as the user's need, when user involves in more than one password based authentication systems, it becomes difficult for the user to distinguish among passwords used for different applications and to correctly remember those passwords. As time passes on, and by using many password based applications, forgetfulness of passwords is more probable to occur.

(ii) When a user may have more than one account with different passwords, the leakage of one or more of them are just possible.

(iii) A password that is written down can be seen by others and can be stolen.
(iv) Passwords invented by people are devised to be easy to remember- a word in dictionary or a loved one's name, a telephone number or a keyboard pattern (i.e. "asdf") or some combination thereof. Unfortunately, a password drawn from that significantly smaller space will be considered easier to guess.

This form of authentication is relatively weak because, the same password is used over and over again, giving many opportunities for it to be illicitly captured.

Two factor/ Token based authentication is considered to be stronger than Single factor/Knowledge based authentication system, where user's confidence can be increased beyond what Single factor/Knowledge based authentication method provides by requiring that multiple independent method be used to authenticate individuals. This is known as multi factor authentication and the combination of two independent methods is known as Two Factor authentication.

Here ignorance of the " Something You Know" (a PIN) makes it difficult for an attacker to benefit from stealing the " Something You Have"(a bank card).

As knowledge based and token based authentication techniques are considered to be very effective, but for the reason that passwords and tokens are liable to be stolen, forgotten or shared with some un-authorized users due to which credibility reduces.

On the one hand, software tokens are flexible and less expensive than the hardware based solution. But on the other hand, software tokens have the following flaws.
(i) Software tokens are inherently vulnerable to maleware and keylogger attacks. They typically try to retrieve the user's credentials when they are typed in.
(ii) Software tokens are vulnerable to visual spoofing attacks.
(iii) They need installation of token driver on the system.

These problems are difficult to solve. However, keylogger attacks can be partially solved by displaying a keyboard on the client's screen having the user type in his credentials using this keyboard in a client-server architecture.

Taking hardware token in consideration, carrying token all the times is inconvenient for users. Since biometric data cannot be readily changed, a user whose data has been leaked might be compelled to use different finger for authentication (e.g. in fingerprint authentication system) and so the possibility of reuse due to leakage of enrolled data is impossible as to impersonate the legitimate user for illegitimate purposes.

6. COMPARASION SUMMARY

Three Factor or Biometric based authentication is considered to be the best and strongest form of authentication techniques. It is far better than traditional authentication systems like knowledge based and token based authentication systems because psychological or behavioral traits/ characteristics of a human cannot be easily stolen. Biometrics is the only form of authentication that assures the physical presence of the user.

7. WEAKNESSES AND LIMITATIONS

In biometric systems, each stage is independent to transform the input and so sometimes due to poor quality of image, some of the stages could not utilize the entire input data, which becomes the drawback of the proposed system.

8. CONCLUSION

In this paper, the author overviewed the authentication techniques and concludes that Three Factor/Biometric-based authentication technique is convenient, safe and reliable. This system is pattern recognition system in which a person is recognized based on features derived from specific psychological or behavioral characteristics that the person possesses, which are harder to be theft or stolen.

9. ACKNOWLEGEMENT

All glory be to Allah, the most Merciful and Almighty, Who enabled me to complete my research work. After this I am greatly thankful to my respected teacher Mr. Ihsan Rabbi lecturer USTB for his proper guidance, constant help and fruitful discussions. I thank Dr. Akhtar Ali, who provided me required feedback and necessary material. I thank Mr. Aurang Zeb, the coordinator IIT for his kind supervision. I also thank my all MS-CS (batch-1st & 2nd) class fellows. The author would like to thank anonymous reviewers for their useful comments.
May God bless them all and brighten their future.

REFERENCES

[1] Ramamohanarao, K., Gupta, K. K., Peng, T. and Leckie, C. **" The Curse of Ease of Access to the Internet "**, 2007
[2] Oppliger, R., Hauser, R., Basin, D., Rodenhaeuser, A. and Kaiser, B.**" A Proof of Concept Implementation of SSL-TLS session Aware User Authentication (TLS-SA) "**
[3] Newman, R. and Beyah, R. **" A Permormance Analysis of Authentication using Covert Timing Channels "**
[4] Schlaeger, C. and Pernul, G. **" Authentication and Authorization infrastructures in b2c e-commerce"**
[5] SHU-ren, Z. **" Authentication based on Feature of hand-written signature",** 2007
[6] Sakata, K., Maeda, T., Matsushita, M., Sasakawa, K. and Tamaki, H. " **Fingerprint Authentication Based on Matching Scores with other Data"**, 2005
[7] ZHANG, Y. and ZHANG, D. **" Authentication and Access Control in P2P Network"**, 2003
[8] Agostini, P.L. and Naggi, R**." Selecting Proper Authentication Mechanisms in Electronic Identity Management (EIDM): Open Issues"**
[9] "**Web Application Security Consortium: Threat Calssification",** www.webappsec.org, version 1.00
[10] "**The Web Security Report**" www.websecurityreport.com , May 2007 Edition
[11] Noor, A. **" Identity Protection Factor (IPF)"**

[12] Mc Cune, J. M., Perrig, A., Reiter, M.K. **"Seein-is-Believing: Using Camera Phones for Human Verifiable Authentication"**, November 2004.
[13] Misbahuddin, M., Premchand, P. and Govardhan, A. **" A User Friendly Password Authenticated Key Agreement for Multi Server Environment",** November 2009.
[14] HARBITTER, A. and MENASCE, D.A. **" A Methodology for Analyzing the Performance of Authentication Protocols",** November 2002
[15] Li, S., Zhou, J., Li, X. and Chen, K. **"An Authentication Protocol for Pervasive Computing"**
[16] Bhargavan, K. and Corin, R." **Cryptographically Verified Implementations for TLS",** 2008
[17] TSENG, Y.M., YANG, C.C. AND HAUR SU, J." **Authentication and Billing Protocols for the Integration of WLAN and 3G Networks**", 2004
[18] Martinovic, I., Zdarsky, F. A., Bachorek, A., Jung, C. and Schmitt, J. B. "**Phishing in the Wireless: Implementation and Analysis",** 2007
[19] Halpert, B. J." **Authentication Interface Evaluation and Design for Mobile Devices",** 2005
[20] Abe T., Itoh, H. and Takahashi, K. " **Implementing Identity Provider on Mobile Phone",** November 2, 2007.
[21] Saxena, N., Uddin, Md. B. and Voris, J. " **Universal Device Pairing using an Auxiliary Device**", 2008
[22] Teranishi, I., Furukawa, J. and Sako, K. "**K-Times Anonymous Authentication(Extended Abstract)"**
[23] Haque, M. M., Ahmad, S. I., Li, H. and Asif, K.M. **"An Authentication based Lightweight Device Discovery (ALDD) Model for Pervasive Computing Environment",** COMPSAC 2007
[24] Sharifi, M., Saberi, A., Vahidi, M. and Zorufi, M." **A Zero Knowledge Password Proof Mutual Authentication Technique Against Real-Time Phishing",** ICISS 2007, LNCS 4812.pp.254-258. 2007
[25] Khan, M. A. and Hassan, M. H." **Personal Authentication System using Hybrid Coding Technique"**
[26] Qayum, A. and Latif, R." **Possible Attacks against GSM System Security"**
[27] Haq, I. U. and Yahya, K. M." **Heterogeneous Networks: Challenges and Future Requirements"**