NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATION IN ENGINEERING, RESEARCH AND TECHNOLOGY [IJIERT]
NATIONAL CONFERENCE ON INNOVATIVE TRENDS IN ENGINEERING & TECHNOLOGY-2016
11TH & 12TH MARCH 2016
CONFERENCE PROCEEDINGS ISSN NO - 2394-3696

Paper ID: NITETCSE01

A SURVEY AND COMPARISON ON USER AUTHENTICATION METHODS

Prof. Jyoti I. Nandalwar
Assistant Professor, Computer Scienc & Engineeringe, Bharat Ratna Indira Gandhi College of Engineering, Kegaon, Solapur, Maharashtra, India royaljyo@gmail.com

Prof. Viteshkumar Gaikwad
Assistant Professor, Computer Scienc & Engineeringe, Bharat Ratna Indira Gandhi College of Engineering, Kegaon, Solapur, Maharashtra, India vkdgaikwad@gmail.com

Prof. Shripad Kulkarni
Assistant Professor, Computer Science, A. G. Patil Institute of Technology, Solapur, Maharashtra, India svkulkarni1203@gmail.com

ABSTRACT

Today security concerns are on the rise in all area such as banks, government organizations, business organizations, educational institute etc. The number of frauds and abuses are literally exploding with the increase use of internet in every field. Among all frauds and abuses, the most serious is the theft of identity which causes grave damage to the victim. The protection of digital identities is getting more and more crucial. The use of password for authentication is no longer sufficient and stronger authentication schemes are necessary factor in keeping security of your system. Authentication scheme is a fundamental and important subject for network security, because it is usually used to protect sensitive and important information to restrict the access of precious resources for legal users only. Several authentication strategies have been proposed, soma of which are very difficult to use and others might not meet company's security concern. So it has become crucial to have in depth knowledge of all authentication schemes so that user can choose best among them as per user's requirement. In this paper we have first studied different types of accounts user can have based on their sensitivity, then we have studied what is authentication, threats to the authentication. Second part of paper describes different types of authentication schemes and their applicability by studying on their pros and cons.

KEY WORDS: authentication, token, biometric, and security attacks

INTRODUCTION

Now a day's people have become habitual of net, with increased use of internet, cybercrimes have also increased to a great extent and security has become a vital issue. Cybercrime is the combination of cyber and crime. Applications with major security and usability issues are being used by more and more people who are less and less technically savvy. The move toward e-commerce, e-services has seen many institutions put special focus on the need for more and more stronger security need; especially that of user authentication on web. Password based end user authentication scheme have continued domination on all other authentication scheme, as user have become habitual of it. As in every area web technology moves ahead by leaps and bounds, research have demonstrated that passwords are plagued by security problems. With increased need for more and more security many alternatives to traditional password schemes have been emerged. To progress, we must better systematize the knowledge that we have regarding all authentication methods we have as an alternative to our traditional password based scheme. This paper will detail, discuss and compare benefits and challenges of available authentication schemes. So that user can better understand which scheme can better fulfil his security needs. In IInd part of paper we will discuss Problem Definition: different types of accounts user can have and we will divide the spectrum of accounts by value. What is Authentication? And common threats to the authentication methods. In the IIIrd part of paper we will discuss different Authentication Techniques and their types. In IVth part of paper will conclude the paper.

PROBLEM DEFINITION

Before discussing Threats to authentication, first we will discuss types of accounts user may have and their security requirements.

ACCOUNT TYPES

As per survey conducted it is concluded that, a normal internet user, on an average have at least 5 to 6 accounts intended for different needs. All accounts don't have requirement for stronger authentication. As per need, frequency of use and value of account, we can divide the spectrum of accounts by value. Requirements of increased complex implementations for trusted authentication and authorization of users in local and web-based services due to higher amount of participating components (e.g. service providers, databases, security etc.) are increasing now a day. The four levels of authentication [1] defined by NIST are given as below:

■ Level 0- Special Purpose accounts: user may create it for testing, participating in a pseudo-anonymous conversation thread, or making a one-time purchase without saving payment credentials

■ Level 1- Routine accounts: They are intended to be long-lasting and to protect something of value but do not carry a risk of large financial or reputational loss. An example would be a subscription to an online newspaper. Little or no confidence for identity credentials is required (there is no need for identity proofing, it is sufficient with a simple password challenge response protocol.)

■ Level 2- Identity accounts: They are widely understood to represent users. Examples include a blog with a moderately large following or an account at an online store with saved credit card numbers. It requires some confidence in identity credentials. It provides single factor remote network authentication. At this level there is a need for identity proofing and secure authentication protocol to prove the identity.

■ Level 3- Sensitive accounts: An individual's primary email or online banking accounts are included. It may have severe and unforeseen consequences in case of loss of data, either by deletion or public exposure. High confidences in identity credentials are required.

■ Level 4- Very high-value transaction accounts: They are specialized systems used for irrevocable actions such as cross border monetary flow and weapons release. Such accounts require very high protection. Very high confidence in identity credentials is required

COMMON THREATS

People are reactive about security; it's important to invest only as much effort as necessary to reduce risk to an acceptable level. There are possibilities to have an alternative to passwords, but transition costs would be difficult. So, we systematically list the common attacks used in the wild [2].

- Dictionary attack: The attackers have access to a relatively small dictionary of words that likely includes the secret password. The attacker records past communications and searches for a word in the dictionary that is consistent with the recorded communications.
- Phishing : attackers displays a login page to user that looks like one they're used to, and trap user to enter their credentials (username, password, credit card number , etc.) at that fraudulent website that looks exactly same as the original website. When user enters credentials to the fraudulent site, attacker record the user's credentials and use then for illegal purpose.
- Brute-force Attack: Attacker generates every possible password permutation and uses it to attack on real passwords. With respect to dictionary attack, brute force attack offers better coverage but require more time or processing power.
- Shoulder-surfing: Attackers acquire knowledge of a particular user's credentials through direct observation, or through external recording devices such as video cameras.

Table -1: Attacks, Attack Enablers and Countermeasures

Authentication Attack	Enablers of Attack	Countermeasures to attacks
Dictionary Attack	- Unlimited authentication attempts - Weak credential policy	- Account timeout/ Auto lock - Restricted no. of authentication attempts
Phishing Attack	- Static authentication	- Non-Static authentication
Shoulder surfing Attack	- Low alertness of user	- Awareness of user about security policies
Brute-Force Attack	- Access to credential resources - Weak credential Policy	- Enforce file access permission
Man –In-The-Middle Attack	- Clear text communication channel - Weak cryptography	- Encrypted communication channel
Replay Attack	- Clear text communication channel	- Encrypt and Time-stamp authentication information
Credential Decryption Attack	- Weak Cryptography - Weak Credential Policy - Incorrect Implementation of cryptography	- Strong Cryptography - Strong Credential Policy - Credential Implementation Check

- Social Engineering: Social engineering includes any technique used to trick people into divulging their credentials or private information to untrusted parties. Social engineering can also be done using other means, such as through phone calls claiming to be from the user's bank, credit card Company, or tech support.
- Malware: Malware (i.e., malicious software) includes any unauthorized software that is installed without a user's informed consent. Such software has a malicious purpose, and can include viruses, worms, and ActiveX or JavaScript components. One category of malware is intended to gather confidential information, including user credentials, from the computer on which it is installed. For example, key-loggers record keyboard input, while mouse-loggers and screen scrapers capture mouse actions and the contents of screen memory, then either send this information back to the attacker or otherwise allow attackers to retrieve it.
- Replay Attack: Attacker captures an authentication sequence transmitted through the network by an authorized user and then replays the same sequence to the server to get himself authenticated.
- Credential Decryption Attacks: Attacker use tools whose aim is to break the encryption algorithm that was used to encrypt credential information. Later he uses these credentials for fraudulent use.
- Man-in-the-middle attack: Attacker captures information as it flows between a client and a server. Usually attacker attempts to capture TCP/IP transmissions, because they may contain information such as username, passwords or content of an email message.

AUTHENTICATION TECHNIQUES

Authentication is a vital subject for network security, because it is usually used to protect sensitive and important information or restrict the access of precious resources for legal privileged users only. Authentication is defined as the verification of the "identity of a user, process, or device, often as a prerequisite to allow access to resources in an information system" Authentication is a component of Information Assurance (IA), confidentiality, integrity, and availability .CIA triad which constitutes the core principles of information security. We classify authentication mechanisms according to the following categories; Strong authentication can combine one or more of the following authentication options:

I. KNOWLEDGE BASED AUTHENTICATION

Knowledge based authentication techniques further gets divided into:
Something you know (recall based): Users must recall and correctly enter their secret to authenticate themselves. e.g. Passwords, PIN
Something you recognize (recognition based): The user and the system share a secret. The system provides clues and the user must correctly recognize the secret. It includes Graphical passwords where users must recognize pre-selected images from a set of decoys fall into this category. On successful selection of proper images user is allowed to log in to the system

A. TEXTUAL BASED AUTHENTICATION SYSTEM

Textual passwords are easy to use and are commonly used. Depending upon application where we need authentication, they are generally alphanumeric passwords derived from a character set for ex: ASCII character coding scheme based on the ordering of the English alphabet and includes 128 characters: 33 are nonprinting control characters. It has two conflicting requirements: the selection of passwords that are easy to remember and, at the same time, are hard to guess.

B. GRAPHICAL AUTHENTICATION SYSTEM

Graphical passwords are based on the idea that people are better at memorizing graphical passwords than text-based passwords. It is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. The graphical user authentication (GUA) system requires a user to select a memorable image and the specific sequence of click locations. Images with meaningful content will support the user's memorability. Graphical passwords can be divided into four categories, following table summarizes all the schemes ordered by their date as follows[3]:

i. Pure Recall based Technique (Drawmetric scheme):

In this system user creates his password having pictures, and while login user reproduce his password, without using reminder marks of the system. He has to reproduce his password by memorizing it. It includes various pass points. Pass points are the various points which are used to create one particular shape. The shape which user enters while login must be correct as he entered while creating account to access the account. It may include visual drawing on predefined grid cells. Draw-A-Secret (DAS) is one such earliest scheme. In DAS, a user is

asked to draw a simple picture using a mouse or stylus. For a successful login, the user needs to re-draw the picture. However, there are some restrictions on drawing which impact on the usability performance of DAS, such as ensuring every stroke is off the grid lines and redrawing in the exact position. However, the password space of such schemes is small as users prefer to draw symmetric images and with less number of strokes.

ii. Cued Recall Based Techniques(Locimetric scheme):

Here, the system provides a framework of reminders, hints and gestures for the users, i.e. system provides images to user, and user selects locations within one or more images to reproduce their passwords or make a reproduction that would be much more accurate. To create password in such systems, users is given with an images and user select locations within one or more images. The location which user chooses is in specified zone in image which is termed as a password click point. The right clicks points and their correct order are required for successful authentication.

iii. Recognition based schemes (Cognometrics schemes):

In Cognometric schemes [4][5], during registration phase, the system provides a large portfolio of images and the user creates a password by randomly choosing several images. The set of selected images by user becomes the user's password. During authentication, the user must successfully identify his/her password images from the challenge set of password images and decoy images displayed by the system. Research has shown that "90% of users can remember their password after one or two months"

iv. Hybrid Schemes

Hybrid schemes are typically the combination of two or more schemes or other authentications. For example, it may have combination of textual and password based authentication techniques. These schemes are used to overcome the limitations of a single scheme, such as shoulder surfing, hidden camera, or spyware and so on. We will provide a detailed description of these schemes, as given below:

II. TOKEN BASED AUTHENTICATION SYSTEM

A Token based system [6] is based on "something you have". The term may also refer as an identity token, hardware token, authentication token, security token, access token, cryptographic token or simply token. It is used to prove one's identity electronically to access resources. It can be used in combination with passwords or it can replace passwords totally. E.g. Smart Cards, a bankcard, remote garage door opener, a driver's license, credit card, a university ID card etc. The token based system offers two factor authentications, which uses elements or devices such as tokens and ATM cards. Token is a portable, tamper resistant, secure storage device or an electronic key accessed at the client end via a password to obtain a passcode that is transmitted to the host for authentication. Like a password, a passcode is a machine-generated and machine-stored secret number. Some system can use token as a secure storage device containing passwords, such as smart card. Some systems can use token as an active device like small keypads to allow entry of pin or can yields one-time passcodes i.e. generate a key which can be either time-synchronous or challenge-response . Some token based systems are also designed with extra features like having USB connector, RFID functions or Bluetooth which provides wireless interface between token and client system through which generated key number sequence can be transfer. Token security defences include tamper-resistant packaging and special hardware that disables the token if it is tampered with or if the number of failed authentication attempts exceeds a chosen threshold. Uses of knowledge based techniques to enhance the security are commonly involved in Strong authentication solutions. For example, ATM cards are used together with a PIN number. A token can provide three major advantages when combined with a password.

1. Token can store or generate multiple passwords. So user gets free from remembering multiple, changing passwords, he have to remember only single password needed to access the token i.e. A single sign-on device.
2. Token provides loss or theft detection as its absence is observable.
3. Token provides added protection against man in the middle attack and denial of service attacks. For a password based system, an attacker can dictionary for number of passwords to crack system, but with token, he have to steal token as well, this is more difficult.

Main disadvantages of a token are inconvenience and cost.

1. Equipment cost is higher than a password as it requires a reader. Because of vulnerability to theft, a single-factor token cannot be used in wide.
2. A token plus biometric combination has similar security characteristics to a token plus password. However, this combination is more costly due to two required readers, and it may be less convenient.

Here we have mention different forms of token, we can use as per our requirements:

i. Smart Cards

Smart cards are small sized cards that have embedded integrated circuit with dedicated cryptographic operation and highly secure storage of user credentials and keys.. Smart cards are used for identification and authentication. Smart cards may include household utility prepayment cards, fuel cards, authorization cards, ATM cards, Credit cards, SIM cards etc., which has tamper resistant security system with provided security

services. Smart card based scheme has been widely utilized for various transaction-oriented services such as electronic currency exchange, social insurance payment and e-commerce payment. As an electronic wallet smart cards can be used by loading funds to pay to vending machines, merchants.

ii. Software Tokens :

It do not require dedicated physical device to provide strong authentication. This provide more secure two factor authentication without carrying any additional hardware device. These tokens are software programs that can be stored on a user's computer, or on mobile devices such as a cellular phone or PDA. Based on a secret key, the token generates a one-time password that is displayed on the computer or mobile device. Software OTP tokens are also available for use with mobile devices.

- OTP (SMS): A One Time Password sent to mobile phones through carrier short messages.
- OTP (Soft-Token): A type of One Time Password that is generated by software application usually installed on smart phones.

iii. USB Tokens

USB tokens are small handheld devices which uses USB ports for authentication. USB token are connected to USB ports, after plugging into USB port and entering token password, Users are granted access. After successful authentication a physical connection between the token and the computer get established. Now user can use multiple security applications such as secure local and remote network access, web access, file encryption, user credential management, and secure transactions

iv. Smart-card-based USB Tokens

These tokens contain a smart card chip having the advantages of both USB tokens and smart cards. These token uses the USB Protocol, CCID (Chip Card Interface Device), which allows a smartcard to be connected to machine using USB port. These tokens are connected to USB ports, after plugging into USB port and entering token password, Users are granted access. After successful authentication a physical connection between the token and the computer get established. Now user can use secure local and remote network access, web access, file encryption, user credential management, and secure transactions. It provides all benefits of smart card and reader without requiring the separate reader. The main advantage of it is that it provides the greatest level of security, versatility, and they enable a broad range of security solutions. It not only provides physical control but also provide privacy protections.

v. Hybrid Tokens

Hybrid tokens provide multiple types of functionality, which increases flexibility. Hybrid USB and OTP tokens allow full USB-based strong authentication and security solutions, as well as OTP based strong authentication in detached mode when needed. Smart-card-based hybrid tokens that use the smart card chip for both USB and OTP functionalities provide maximum security.

III. BIOMETRIC BASED AUTHENTICATION SYSTEM

Biometric is uniquely recognizing a person based on their physiological or behavioural characteristics. Biometric schemes are characterized by uniqueness of a person depending on his physiological and behavioural characteristics that can be used for verification or identification of person. Other authentication schemes have demerits such as thefts of identity; something you know or have can be stolen or predicted or can be hacked. Use of Biometric prevents stealing of possessions that mark the person's identity such as Persons ID cards, license etc. Biometric authentication process includes acquisition of characteristics, creation and storage of master characteristics while making initial database, while authentication process, it includes acquisition of characteristics, comparison between earlier stored and currently entered characteristics, and based on comparison giving decision about identity authentication. Several Biometric technologies are available in market like fingerprints, palm prints, hand geometry, face recognition, voice recognition, iris recognition, and retina recognition.

A Biometric system can provide following major advantages:

- User convenience, Non repudiation
- Supports wide range of applications such as data protection, transaction and web security and Provides the highest level of security and the dominant security defence is that they are difficult to copy or forge.

The major drawback of this approach is that:

- Such systems can be expensive, and the identification process can be slow and often unreliable.
- Applying biometrics is its intrusiveness upon a user's personal characteristic. Moreover, retina biometric recognition schemes require the user to willingly subject their eyes to a low-intensity infrared light.
- In addition, most biometric systems require a special scanning device to authenticate users, which is not applicable for remote and Internet user

Biometrics is usually classified as physiological or behavioural types.

- The physiological type includes biometrics based on stable body features, such as fingerprint, face, iris, and hand.
- The behavioural type includes learned movements such as voice, handwritten signature, keyboard dynamics (typing), and gait.

The essential characteristics of biometric systems include aliveness testing, should be tamper resistance and provide secure communication. They should provide security threshold level. In market numbers of biometric systems are present now a day; we have listed few of them below:

PHYSIOLOGICAL BIOMETRIC SYSTEMS:

i. Fingerprint Recognition: Take prints using infrared light refracted through prism of fingertip. It divides print into loops, whorls and arches. Minutiae points are calculated.
ii. Face Recognition: User faces a camera and neutral expressions are recorded with required lighting and position but it has high environmental impact.
iii. Hand Geometry: Geometry of user hand is used for identification. It maintains balance in performance and usability and it is more reliable than fingerprinting but requires large scanner.
iv. Retina Scan: User has to look straight into retinal reader for retina scan. Reader scans retina using low intensity light into database.
v. Iris Scanner: Iris is colour and visible from far. Scanner scans unique pattern of iris and it overcomes some demerits of retinal scanner.
vi.

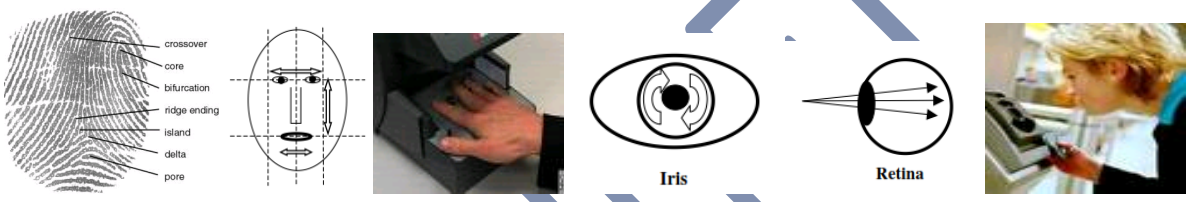

Figure-1: Physiological Biometric Systems:

Behavioural Biometric Systems: These systems are based on signals which get captured from behavioural characteristics of a person.

i. Voice: Speech is taken as an input from the speaker with recorded frequency, duration and cadence. It is user friendly system and speech is recorded in neutral tone. Some of factors like background noise, device quality, local acoustics etc. have an impact on the input speech.
ii. Signature Recognition: It measures dynamic factors while making signature such as speed, velocity, pressure. But signature pattern can be variable with age, illness and emotions.

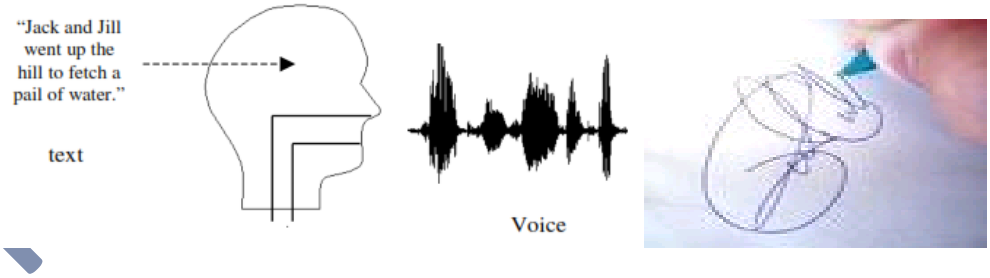

Figure 2: Behavioural Biometric Systems:

CONCLUSIONS

In this paper, we have studied three main types of user authentication schemes.

Knowledge Based Scheme: it commonly referred to as having password Pin or secret. It support authentication by secrecy or obscurity for example combination lock or computer password. Its security defence is by keeping it close. This scheme is easy to use, more acceptable, widely used for almost every application but at the same time it is less secret with each use.

Token Based Scheme: It support authentication by possession of a token, for example a metal key or ATM card. Its security defence is by holding it closely. It provides more security than passwords as attackers have to steal it physically, and its appearance is visible, so in case of theft, user can take appropriate actions immediately.

Biometric Based Scheme: It is based on identification of person and it supports authentication by uniqueness and personalization. Forge resistant is its security defence. Examples of biometric are fingerprint, iris scan etc. We can say that the security drawback is it is difficult to replace.

REFERENCES

[1] National Institute of Standards and Technology (NIST) U. S. Department of Commerce: Electronic Authentication Guideline- Information Security, Special Publication 800-63-1, December 8, 2008.
[2] Authentication at Scale by Eric Grosse and Mayank Upadhyay, Published by IEEE Computer and Reliability Societies, 1540-7993/13, January/ February 2013
[3] User Authentication By Secured Graphical Password Anil H.Rokade, Dr.Santosh S.Lomte,, Prof.Rajesh.A.Auti, Yogesh R. Ngargoje, ijsae, July 2014
[4] A Survey on the Use of Graphical Passwords in Security Haichang Gao, Wei Jia, Fei Ye and Licheng Ma Institute of Software Engineering, Xidian University, Xi'an, P.R.China, JOURNAL OF SOFTWARE, VOL. 8, NO. 7, JULY 2013
[5] Graphical Passwords: A Survey, Xiaoyuan Suo Ying Zhu G. Scott. Owen Department of Computer Science Georgia State University, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013
[6] Survey on Authentication Password Techniques by Priti Jadhao, Lalit Dole