Information and Knowledge Management www.iiste.org
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.4, No.6, 2014

Security of Multifactor Authentication Model to Improve Authentication Systems

Mrs. Tamara Saad Mohamed
Lecturer, Department of Computer Science Cihan university \ Sulaimaniah \ Iraq
E-mail : tamara_ttt@yahoo.com

Abstract
Multifactor authentication (MFA) is a security system in which more than one form of authentication is implemented to verify the legitimacy of a transaction. The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a computer system or network. Multifactor authentication is achieved by combining two or three independent credentials: what the user knows (knowledge-based authentication), what the user has (security token or smart card) and what the user is (biometric verification). Single-factor authentication (SFA), in contrast, only requires knowledge the user possesses. Although password-based authentication is well-suited for website or application access, it is not secure enough for online financial transactions.
Keywords: authentication , multi-factor-authentication , biometric factor, knowledge factor . possession factor

1. Introduction

Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security, as described herein." This means the simple "username/password" combination for accessing your online banking is ineffective. And that banks should "adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts" and "financial institutions should implement more robust controls as the risk level of the transaction increases." This is where multifactor authentication comes in.
We can authenticate an identity in three ways: by something the user knows (such as a password or personal identification number), something the user has (a security token or smart card) or something the user is (a physical characteristic, such as a fingerprint, called a biometric).
All three authentication mechanisms have drawbacks, so security experts routinely recommend use a process called multi-factor authentication. But implementing multi-factor authentication requires expensive hardware and infrastructure changes. Therefore, security has most often been left to just a single authentication method.
Passwords are cheap, but most implementations offer little real security. Managing multiple passwords for different systems is a nightmare, requiring users to maintain lists of passwords and systems that are inevitably written down because they can't remember them.
Using security tokens or smart cards requires more expense, more infrastructure support and specialized hardware. Still, these used to be a lot cheaper than biometric devices and, when used with a PIN or password, offer acceptable levels of security, if not always convenience.
Biometric authentication has been widely regarded as the most foolproof - or at least the hardest to forge or spoof. Since the early 1980s, systems of identification and authentication based on physical characteristics have been available to enterprise IT. These biometric systems were slow, intrusive and expensive, but because they were mainly used for guarding mainframe access or restricting physical entry to relatively few users, they proved workable in some high-security situations. Twenty years later, computers are much faster and cheaper than ever. This, plus new, inexpensive hardware, has renewed interest in biometrics.
so we suggest in this project to design a multi factor authentication model which is carry a password model (first factor), then a wireless (Bluetooth-based tokens exist)(second factor) , then make a model more powerful by adding the new biometric's factor (ear biometric)(third factor) which is more advanced than the others biometrics factors according to the latest researches . a multi factor authentication carry the advantages of all the above authentication factors by selecting the strongest one from each authentication factor . we chose from the knowledge factor the regular password then pattern of array (add cells sequence) , then move to the second factor possession factor we chose smart card, then third factor ; biometric factor , we chose ear biometric .

2.Authentication :

The process of identifying an individual, usually based on a user name and password. In security systems, authentication is distinct from *authorization* , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

3.Proposed System :

We suggest to build system which has more than one factor authentication . Multi-factor authentication (three-factor-authentication) is an approach to authentication which requires the presentation of three authentication factors: a *knowledge* factor ("something only the user *knows*" password), a *possession* factor ("something only the user *has*" Bluetooth-based tokens exist), and an *inherence* factor ("something only the user is" ear biometric). After presentation, each factor must be validated by the other party for authentication to occur. Fig 1

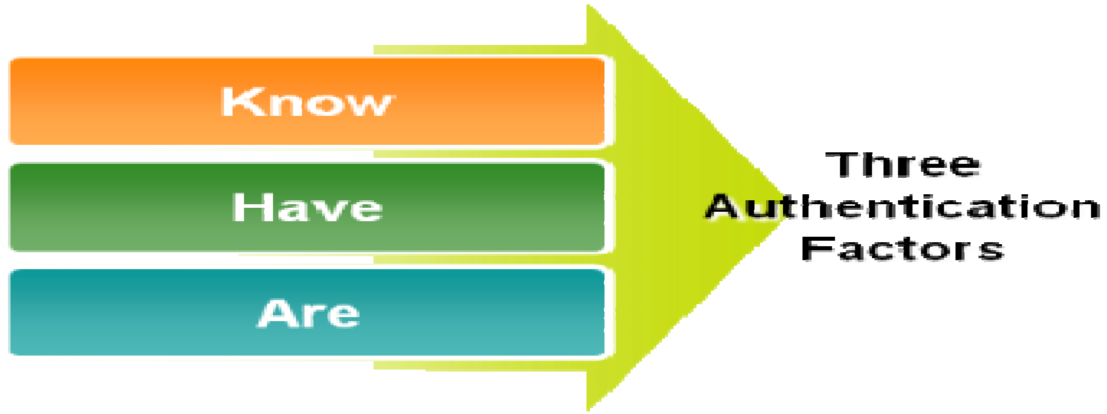


Fig 1 , three authentication factors

3.1 Background :

The number of factors is important, as it implies a higher probability that the bearer of the identity evidence indeed holds that identity in another realm (e.g., computer system vs real life). In reality, there are more variables to consider when establishing the relative assurance of truthfulness in an identity assertion than simply how many "factors" are used.

The factors are identified in the standards and regulations for access to U.S. Federal Government systems. These factors are:

- Something only the user knows (e.g., password, PIN, pattern);
- Something only the user has (e.g., ATM card, smart card, mobile phone); and
- Something only the user is (e.g., biometric characteristic, such as a fingerprint ,face , ear , voice).fig2

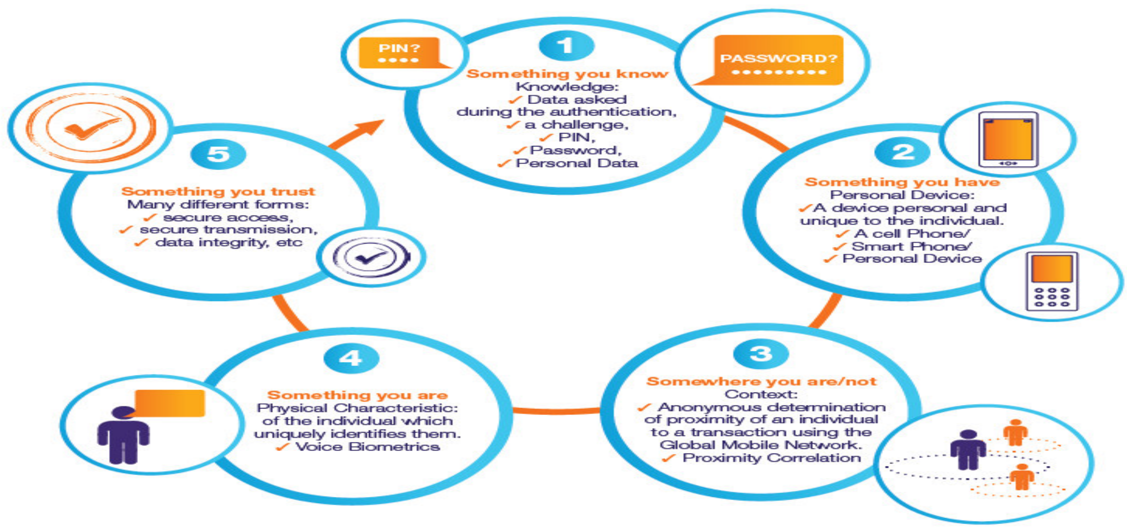


Fig 2 different five authentication factors

3.2 Knowledge factors : something only the user know

3.2.1 Password :

A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many two factor authentication techniques rely on password as one factor of authentication.

3.2.2 PIN :

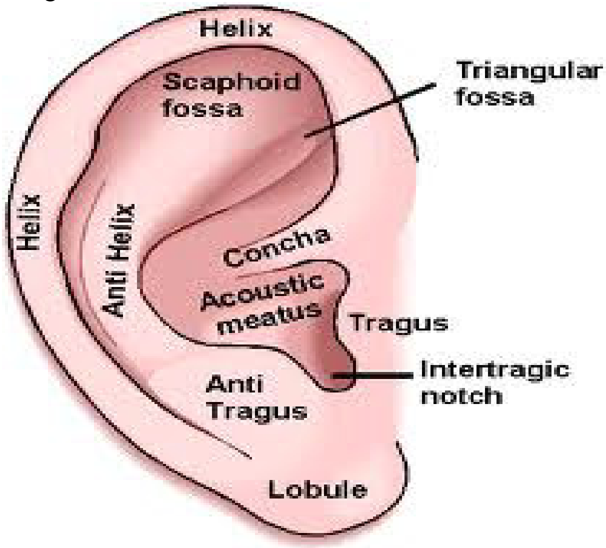
A personal identification number (PIN) is a secret numeric password and is typically used in ATMs. Credit and ATM cards do not contain the PIN or CVV on the magnetic stripe. This aligns with the principle that the PIN is not part of "something the user has" for this use.

3.2.3 Pattern :
Pattern is a sequence of cells in an array that is used for authenticating the users. e.g. Pattern based authentication is used in Android devices at login.
3.3 Possession factors : something only the users has
3.3.1 Tokens with a display (disconnected tokens) :
A number of types of pocket-sized authentication token are available which display a changing passcode on an LCD or e-ink display, which must be typed in at an authentication screen, thus avoiding the need for an electronic connection. The number is derived from the shared secret by a cryptographic process which makes it infeasible to work out the secret from the sequence of numbers.
3.3.2 Magnetic stripe cards:
Magnetic stripe cards (credit cards, debit cards, ATM cards, loyalty cards, gift cards, etc.) are easily cloned and so are being or have been replaced in various regions by smart cards, particularly in banking.
3.3.3 Smartcards:
Smart cards are the same size as a credit card. Some vendors offer smart cards that perform both the function of a proximity card physical access device and network authentication. Users can authenticate into the building via proximity detection and then insert the card into their PC to produce network logon credentials. In fact, they can be multi-purposed to hold several sets of credentials, as well as electronic purse functionality, for example for use in a staff canteen. They can also serve as ID badges
3.3.4 Wireless:
RFID-based tokens exist . Bluetooth-based tokens exist. Contactless smart cards (a wireless version of the traditional smartcard) exist.
3.3.5 USB tokens:
A USB port is standard equipment on today's computers, and USB tokens generally have a large storage capacity for logon credentials, and perhaps user data as well. However, they may be relatively costly to deploy and support, are vulnerable to theft and fraud, and have met user resistance. Any USB memory device can be used as a token simply by storing a secret (possibly an X.509 certificate) on it, but then there is nothing to stop it from being copied.
3.3.5 Mobile phones:
There is presently only limited discussion on using wired phones for authentication; most applications focus on use of mobile phones instead. A new category of TFA tools transforms the PC user's mobile phone into a token device using SMS messaging, an interactive telephone call, or via downloadable application to a Smartphone .
3.4 Inherence factors : something only the user is
Biometric technologies" are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic .
3.4.1 Types of Biometrics:
A number of biometric methods have been introduced over the years, but few have gained wide acceptance.
3.4.1.1 Typing patterns. Similar to signature dynamics but extended to the keyboard, recognizing not just a password that is typed in but the intervals between characters and the overall speeds and pattern. This is akin to the way World War II intelligence analysts could recognize a specific covert agent's radio transmissions by his "hand" -- the way he used the telegraph key.
3.4.1.2 Eye scans. This favorite of spy movies and novels presents its own problems. The hardware is expensive and specialized, and using it is slow and inconvenient and may make users uneasy.
In fact, two parts of the eye can be scanned, using different technologies: the retina and the iris.
3.4.1.3 Fingerprint recognition. Everyone knows fingerprints are unique. They are also readily accessible and require little physical space either for the reading hardware or the stored data.
*3.4.1.4 Hand or palm geometry***.** We're used to fingerprints but seldom think of an entire hand as an individual identifier. This method relies on devices that measure the length and angles of individual fingers. Although more user-friendly than retinal scans, it's still cumbersome.
3.4.1.5 Voice recognition. This is different from speech recognition. The idea is to verify the individual speaker against a stored voice pattern, not to understand what is being said.
3.4.1.6 Facial recognition. Uses distinctive facial features, including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes. Most technologies avoid areas of the face near the hairline so that hairstyle changes won't affect recognition.
Often the using of one biometric features like fingerprint or face detection has some disadvantages like :
1. There is a large variation of the quality of the fingerprint over the population. The appearance of a person's print depends on age, grease, and cut or worn fingers, i.e., on occupation and lifestyle in general.
2. Elastic distortion of the skin of the finger due to touch sensing methods and potential problems

with cleanliness of the sensor and public hygiene.

3. In some very rare cases, there are people without fingers, or without a full set of fingers. Obviously, these individuals cannot be fingerprinted.

3.4.1.7 Ear biometrics . it is a new technique and advanced one The possibility of identifying people by the shape of their outer ear was _rst discovered by the French criminologist Bertillon, and re_ned by the American police o_cer Iannarelli, who proposed a _rst ear recognition system based on only seven features. The detailed structure of the ear is not only unique, but also permanent ,as the appearance of the ear does not change over the course of a human life. Additionally, the acquisition of ear images does not necessarily require a person's cooperation but is nevertheless considered to be non-intrusive by most people. Because of these qualities, the interest in ear recognition systems has grown signi_cantly in recent years. In this survey, we categorize and summarize approaches to ear detection and recognition in 2D and 3D images. Then, we provide an outlook over possible future research in the _eld of ear recognition, in the context of smart surveillance and forensic image analysis, which we consider to be the most important application of ear recognition characteristic in the near future.



4.Working of suggested system :

We suggest to produce system work as three-factor-authentication . first the user have to login password, we prefer to use a PASSWORD as a knowledge factor than using of pin or pattern because of shoulder surfing attacks password more safe . then user have to enter his\her wireless BLUETOOTH-BASED TOKEN EXIST , we prefer to use this technique because it is more secure against shoulder surfing attacks and other attacks , then the system have to check the EAR_BIOMETRIC factor fig 4 , we prefer to use the ear biometric factor because of its uniqueness and advantages over the others types of biometrics . so that mean we takes the advantages of the strongest factors to build a powerful authentication system . fig 3

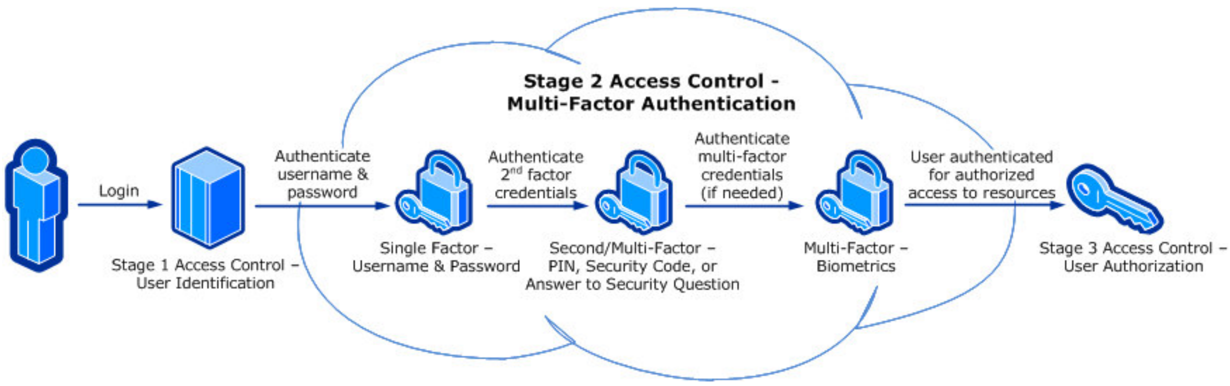


Fig 3 proposed system (multi-factor-authentication)

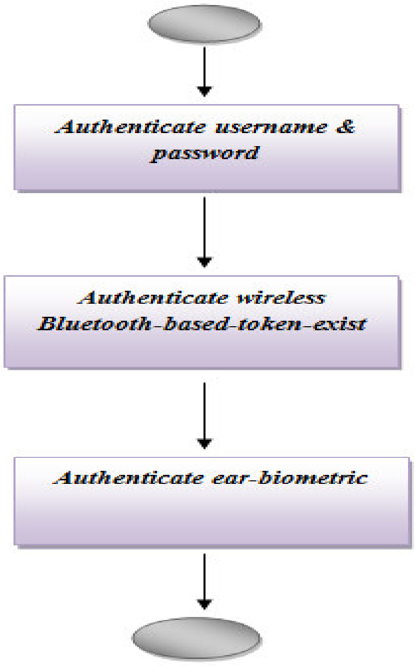


Fig 4 proposed system diagram

5.Implementations' Fields :

5.1 Critical server: Many large organizations have critical Servers that are usually protected by a textual password . A multi factor authentication proposes a sound replacement for a textual password.

5.2 Nuclear and military facilities: Such facilities should be protected by the most powerful authentication systems. The A multi factor authentication has a very large probable password space, and since it can contain token, biometrics, recognition, and

Knowledge-based authentications in a single authentication system, it is a sound choice for high-level security locations.

5.3 Airplanes and jetfighters: Because of the possible threat of misusing airplanes and jetfighters for religion-political agendas, usage of such airplanes should be protected by a powerful authentication system. The A multi factor authentication is recommended for these systems.

5.4 Banking : some countries start working with A multi factor authentication. for security of users who wants to buy online or pay online. And who want to add security to their accounting bangs .

6.Analysis Of Multi Factor Authentication :

6.1 Attacks & countermeasures:

As mentioned earlier voiced 3D password is most secure authentication. We will see different kinds of attacks & how voiced 3D password scheme is more secure against different attacks.

6.1.1 Timing Attacks :

This attack is based on how much time required completing successful sign-in using multi factor authentication. Timing attacks can be very much effective while Authentication scheme is not well designed. But, as our system is designed more securely, these kinds of attacks are not easily possible on multi factor authentication also not much effective as well.

6.1.2 Brute force Attacks :

In This kind of attacks the attacker has to try n number of possibilities of multi factor authentication. As these attacks considers following two points.

- Required time to login: as in multi factor authentication time required for successful login varies & is depend on number of actions & interactions, the size of multi factor authentication.
- Cost required to attack: as multi factor authentication scheme requires environment of multi factor authentication & cost of creating such a environment is very high.

6.1.3 Well-studied attacks :

In this attack attacker has to study whole password scheme. After studied about scheme the attacker tries combination of different attacks on scheme. As multi-factor & multi-password authentication scheme, attacker fail to studied whole scheme. this attacks also not much effective against multi factor authentication.

6.1.4 Key logger :
In this attack attacker install as software called key logger on system where authentication scheme is used . This software stores text entered through keyboard & those text are stored in text file. In this way this attacks is more effective & useful for only textual password. So that this kind of attacks are not much effective in this case .
6.1.5 Shoulder Surfing attacks :
Attacker uses camera for capturing & recording of multi factor authentication. This attack is more effective than any other attacks on possession factor . So that possession factor must be performed in a secure place where this attack can‘t be performed.

7. Conclusion
Multi-Layered Security for Increased Protection and user Confidence Improving the overall security of consumer-facing services is vital to financial institutions , Nuclear and military facilities, transactions , banging , airplane and jetfighters . The risk of doing business with unauthorized or incorrectly identified persons in an Internet environment can result in financial loss and reputation damage. Online financial services customers need confidence that their financial institution is protecting confidential personal information and account access. Financial and business institutions therefore need to not only improve security, but bolster customer confidence in order to drive adoption of their online brokerage channel. multi-factor authentication and risk evaluation services that improve security without increasing complexity for users . Multi-factor Authentication & Security applications offer rapidly deployable options that can be configured to meet your most demanding online security needs. Our solutions are designed to ensure that users feel safe and secure every time. Through the use of secure, multi-factor user and transaction authentication able to monitor and enforce business rules to prevent fraud, protect privacy and support regulatory compliance. All above are the advantages of multi-factor-authentication .

Drawback of the proposed system :
- Costly to achieve like that system .
- Required a professional programmers and experts , so it is more suitable for big organizations like a military organizations , bangs , nuclear organizations.

References
http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
http://www.infosecisland.com/blogview/15593-The-Benefits-of-Multifactor-Authentication.html
http://en.wikipedia.org/wiki/Multi-factor_authentication
Ear Biometrics: A Survey of Detection,Feature Extraction and RecognitionMethodsAnika Pug, Christoph Busch _July 2, 2012
SECURED AUTHENTICATION: 3D PASSWORD* Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita Department of Computer Science and Engineering, Dronacharya College Of Engineering, Gurgaon ISSN 2229-600X
Alsulaiman, F.A.; El Saddik, A., "Three- for Secure," IEEE Transactions on Instrumentation and measurement, vol.57, no.9, pp 1929-1938.Sept. 2008.
Grover Aman, Narang Winnie, ―4-D Password: Strengthening the Authentication Scene‖, International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October-2012.
http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
http://www.computerworld.com/s/article/100772/Biometric_Authentication?taxonomyId=17&pageNumber=2