An Alternative Authentication Methodology in Case of Biometric Authentication Failure : AAP Protocol

K. Sharmila Reddy [1], Dr. V. Janaki[2], K. Shilpa[3]

[1] *CSE Department, Aurora's Research & Technological Institute, Andhra Pradesh, India*
[2]*CSE Department, Vaagdevi College of Engineering, Andhra Pradesh, India*
[3]*CSE Department, Aurora's Research & Technological Institute, Andhra Pradesh, India*

Abstract

In today's world of increased connectivity, authentication issues are becoming more important. The process of verifying a user's identity is typically referred to as user identification and authentication. There are many authentication factors available for proving one's identity like one factor authentication, two factor authentication, three factor authentication etc. When the third authentication factor fails, where the procedure of submitting human biometric characteristics to provide authentication leads to a disaster, this paper gives a solution by generating a key using Diffie-Hellman key exchange algorithm.

Key Words — Authentication, biometrics, key, passwords, smartcard, security, tokens.

I. Introduction:

Authentication is the process of identifying whether a person or a thing is in reality, who or what it is stated to be. This process of identifying an individual is generally based on providing username and password. Authenticating a thing may be done by provision of its attributes, whereas authenticating a person normally involves verifying the validity by at least one characteristic of identification. Authentication depends on one or more authentication factors [1].

In general the authentication factors are categorized in to the following based on the characteristics they exhibit like one factor authentication, where the user has to provide a valid user name and password. Two factor authentication where the factor of authentication used is the Smart Cards and three factor authentication where authentication is done based on Biometric factors.

Since Information over the Network passes in a digital format, it has to be provided more security since it may be eavesdropped. Hence, authentication is the process of verifying the digital identity of the sender while communicating over the network. This process may start with an initial request from the user to log in to the system. The sender who is authenticated may be a person alone (human being) or a computer (Device) or even a computer program (Software).

In today's internet environment which is considered as web of trust, authentication is a means of segregating legitimate users from that of illegitimate users. Authentication also overcomes impersonation, where an unauthorized user attempts to access the system by claiming himself as authorized.

II. Previous Work

Information technology systems and the data they store within are considered as valuable resources which have to be protected from many types of attacks prevailing in the network. The first and foremost step towards protecting a system is the ability to verify the identity of its users [6]. The process of verifying a user's identity is normally referred to as user identification and authentication. In many organizations, using passwords is the primary means of authenticating a user. It is a traditional method used in general for authenticating computer users. Unfortunately, in today's World Wide Web, the means to bypass this form of security is on the finger tips of the hackers. The tools used by the cyber criminals are very easy to implement, hack or crack the passwords.

There are many authentication techniques and principles existing today, but not all of them are easy to be implemented, particularly by the end users. While analyzing the system from a technical perspective, it may be possible to frame the security policies to increase the strength of the encryption algorithms. However, when the system is used by multiple users or a single user accesses multiple systems with identical passwords, the system is likely to become less secure. Moreover, phishing attacks are becoming quite popular, where the password entered by the users on a website is

captured by the intruder, which results in compromising the system and the sensitive data of the user.

III. Related Work

A. Authentication Factors:

The authentication factors of humans are generally classified into three categories:

One Factor Authentication (Information Knowledge) - a password or a personal identification number (PIN). Two Factor Authentication (Thing of Possession) - ID card, security token, software token or cell phone[2]. Three Factor Authentication (Human Biometrics) – fingerprint, Iris, DNA, voice recognition etc.

1) ***One Factor Authentication:*** Authentication by password is the most commonly used mechanism but also considered the most vulnerable form of authentication. Significant effort has been put for developing the system of password administration with different levels of password complexity [6]. But still obtaining the password by an attacker is only a matter of hacking tools and time for cracking them.

The usage of password system has two main disadvantages: the passwords are either simple or easily guessable. Many users note them down in common places and put at risk the security of password. Even if the system administrators force the users to periodically change the passwords, the probability that an attacker will obtain the password by guessing or by brute force attack are high. Yet, many companies are using this system as the only way of protecting their data. The use of password authentication is weakened by software attacks. Therefore Password strength has to be increased.

2) ***Two Factor Authentication*:** Two-factor authentication expects the use of two authentication factors i.e a software token (PIN) and a hardware token (Smart Card). Hardware authentication tokens are used to improvise the security in user authentication. Smart-card-based password authentication provides two-factor authentication, where a successful login needs to have a valid smart-card and a valid password.

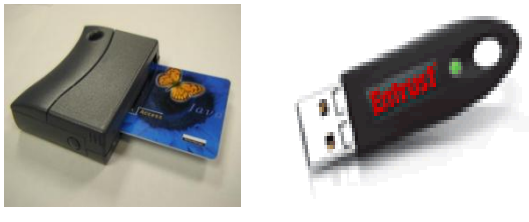

Fig.1. Smart Cards

Principle of the USB tokens:

The USB token device is a small portable device. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is detected [3] by the system, it prompts the user to enter his or her password (the second authenticating factor) so as to gain access to the system as shown in Fig 1.

A USB token also known as dongle, is a security token that works with the USB interface on a computer. It is a type of hardware authenticator used for two-factor authentication used along with password. USB tokens are hard to be duplicated. Therefore, they act as a secure medium for storing and transmitting confidential data. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment [2].
No doubt, the two factor authentication provides stronger security against the normal password authentication. But still, there are chances of failure if both the authentication factors are compromised by a hacker (e.g., an attacker has successfully obtained the password and the data in the smart-card). In these circumstances, a third authentication factor can solve the problem and improve the system's security.

3) **Three- Factor Authentication:** Another authentication mechanism is the third factor authentication through biometric authentication where users are identified by physiological or behavioural characteristics [5].

Examples of biometric features include hand or finger impressions, facial gestures, iris recognition etc. Biometrics acts as a reliable authentication factor since they cannot be easily lost or forgotten.

IV. Motivation of work: Fingerprint Recognition:

Fingerprint recognition techniques analyze human finger print pattern, along with minute unique marks known as minutiae. These are the ridge endings and bifurcations in the fingerprint ridges. No two thumb impressions or biometrics are unique in the world. Therefore, the data obtained from fingerprints of the user are dense in nature and the density justifies why fingerprints act as a reliable means of identification.

Fingerprint recognition systems stored the data related to the exact fingerprint minutiae [9] of the authentic user, whereas images of actual fingerprints are not retained by the system as shown in Fig 2. Hence, fingerprint scanners may be used as input devices or pointing

devices (mice), or they may be even used as stand-alone scanning devices which can be attached to a computer.

Fingerprints are unique and complex enough to provide a robust template for authentication as shown in the figure. Instead of using single finger biometric features, multiple fingerprints from the same individual results in a greater extent of accuracy. Fingerprint identification technologies provide accurate results when compared to other available biometric methods [7].

End users may face some problems using a fingerprint-scanning device. A special hardware and software capable of identifying these features must be either installed on the user's computer or inbuilt in to the system[8].

Implementing Fingerprint recognition may differ from system to system based on the level of significance. This technology is not portable since a scanning device needs to be installed and attached to each participating user's system. However, fingerprint recognition is easy to install and use than other technologies like iris scanning.

Fig2. Fingerprint and minutiae

V. Our Work and Experiment

The Motivation of our work is the issues related to three factor authentication. Every user is in possession of at least one of the authentication factors. If the user is unable to use the above said factors then how the user does gain access control is the rationale here.

A. Security Issues:

Error tolerance has not been considered properly in the existing three factor mechanism. Most existing 3-factor authentication schemes have security problems and privacy issues like User Adoption, high rate of error, impersonation of an individual.

The goal is to provide Privacy to the user's biometric features and protection against remote opponents.

B. Failure of Three Factor Authentication:

In this paper we are experimenting on a special biometric feature "fingerprint". If the three factor authentication fails due to any disaster to the finger (ex, .any injury to the finger), there should be an alternative for the user to gain access to the system.

C. Diffie-Hellman Key Exchange Algorithm:

Diffie-Hellman Key Exchange is a well known secret key exchange algorithm. It is used for exchange of authentication signatures It allows two communicating parties to exchange a 'key' over an insecure medium such as the internet [4]. Though there is an equal chance of interception by the hacker, he will not be able to break the key by applying any mathematical calculations apart from employing the usual brute force method.

The Key Exchange Algorithm:

Consider two people wishing to communicate named Ben and Nen. Their communication should be away from Eve (eavesdropper). Eve should not be able to intercept their message. Ben and Nen agree upon and generate two public keys g and p, where p is a prime number and g is a primitive root of p [10].

The implementation for Diffie Hellman key exchange algorithm can be shown as follows:

Step 1 : Let BEN and NEN select any large prime number 'q'. Then calculate the primitive root of q denoted by 'a' such that a<q

Step 2 : Key generation by BEN: Select a random number X_A as the private key where $X_A < q$. Now Calculate the public key Y_A such that $Y_A = a^{X_A} \bmod q$

Step 3 : Key generation by NEN: Select a random number X_B as the private key where $X_B < q$ and calculate the public key Y_B where $Y_B = a^{X_B} \bmod q$

Step 4 : Now, NEN and BEN exchange the public key values

Step 5 : Actual key generation by BEN as $K = Y_B^{X_A} \bmod q$

Step 6 : Actual key generation by NEN as

$K = Y_A^{X_B} \bmod q$

If the intruder tries to calculate the value of k, then he should definitely need values either ^{X_A} or ^{X_B} [11]. Otherwise, he would need a Discrete Logarithm Problem to find the value of the secret key. There is no known algorithm to accomplish this in a reasonable amount of time.

D. Model Development:

We are proposing an alternative solution to the failure of the third factor by using Diffie-Hellman Key Exchange Algorithm. We involve a third party who certifies the validity of the user, for the failure case of three factor authentication.

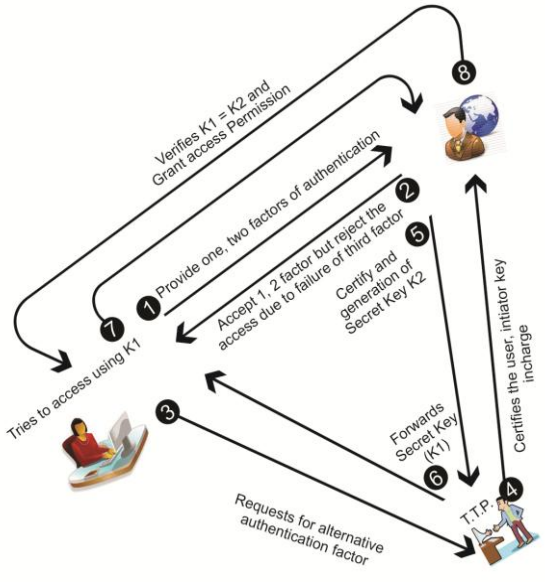

Fig3: Framework of AAP Model

Implementation of our AAP Algorithm: The following table gives an over view of the steps performed in AAP Algorithm.

When the valid user fails to access the system due to the failure of third factor authentication with finger injuries, there should be an alternative authentication factor. In this paper, we propose a solution where we take the help of a trusted third party who acts as an interface between the user and the organization. The third party certifies and authenticates the user in case of failure of biometrics.

The third party and organization will generate a secret key which acts as OTP using Diffie-Hellman key exchange algorithm. Since the key which has been generated at both organization and Trusted Third Party is same, the third party sends the secret key to user. By using that secret key user can get access to the system. Table 1 depicts the communication between the User, Organization and Trusted Third Party.

VI. Conclusion:

As there is a chance of problem to the finger or the biometrics, there should be an alternative for the user to get access to the account. In this paper we developed an alternative model for authentication with the help of a trusted third party.

There are many advantages and disadvantages for different mechanisms of authentication; however it still lies in the users' and administrators' hands to solve these problems. A user may not provide perfect and genuine identification all the time, but keeping the increasing technology in mind and the increase in identity impersonation, users must be cautious of their own security styles and patterns.

User	Organization	Trusted Third Party
Register at third party for Emergency Authentication		Stores the details of the user for future purpose (Emergency)
Normal Login with Ui and PW		
	Ui, PW	
	if (PW=matched)	
	Checks for the PW and then asks for Ti	
Submits Ti.		
	Ti	
	if(Ti= matched)	
	Login success.	
	If(Ti=not matched)	
	Login failed.	
User requests third party for emergency authentication		
		Checks for the authentication details and certifies the user.
	This generated certificate will be sent to the organisation.	
		Organisation generates an OTP (key) along with TTP
	Generate a secret key K	
		TTP forwards the key to User(OTP)
now user logins with the sent OTP/Key		
	Compares and provides access	

Table1. Skeleton of AAP

References:

[1]. Xinyi Huang, Yang Ashley Chonka, Jianying Zhou, and Robert H. Deng "A Generic Framework for Three-Factor Authentication Preserving Security and Privacy in Distributed Systems," IEEE Transactions, 2011
[2]. Jiri Sobotka, Radek Dolezel, "Multifactor authentication systems", Electro revue ISSN.Vol. 1, NO. 4, December 2010
[3]. Stephen S. Hamilton, Martin C. Carlisle, and John A. Hamilton," A Global Look at Authentication", proceedings of the IEEE 2007.
[4]. Keith Palmgren "Diffie-Hellman Key Exchange: A Non-Mathematicians Explanation", ISSA Journal.9, October 2006
[5]. A.K. Jain, R. Bolle, and S. Pankanti, Eds., "Biometrics: Personal Identification in Networked Society," Norwell, MA: Kluwer,1999.
[6]. Identification and authentication, NIST Computer Security Handbook. Special publication 800-12
[7]. Andrew Ackerman, Professor Rafail Ostrovsky "Fingerprint Recognition"
[8]. T. Charles Clancy, Negar Kiyavash, Dennis J. Lin, Electrical and Computer Engineering, "Secure Smartcard Based Fingerprint Authentication". 2003
[9]. Zdeněk Říha Václav Matyáš, "Biometric Authentication Systems" 2000
[10]. Himanshu Arora, "Introduction to Diffie Hellman Key Exchange Algorithm". January 31st, 2013
[11]. Chris Christensen, "Diffie Hellman Key Exchange". Springer, 2010