Issues and Challenges in Two Factor Authentication Algorithms

Article *in* International Journal of Latest Trends in Engineering and Technology · January 2016

CITATIONS
7

READS
10,331

2 authors, including:

Asoke Nath
St. Xavier's College, Kolkata
279 PUBLICATIONS **2,303** CITATIONS

SEE PROFILE

Issues and Challenges in Two Factor Authentication Algorithms

Asoke Nath
St. Xavier's College(Autonomous)
Department of Computer Science, Kolkata, India

Tanushree Mondal
St. Xavier's College (Autonomous)
Department of Computer Science, Kolkata, India

Abstract **-Two factor authentications has been introduced in order to enhance security in authentication systems. Different factors have been introduced, which are combined for means of controlling access. The increasing demand for high security applications has led to a growing interest into protect confidential data using password, token, biometrics etc. In the present paper the authors have made comprehensive study on the various issues and challenges in using two factor authentication algorithms. The authors have also discussed how two factor authentication may be standardized for Industrial use.**

Keyword-Password, One time password(OTP), Biometrics, token, salting, verification.

I. INTRODUCTION

Due to massive explorations in Internet technologies the security issues and authentication issues are nowadays are now a very important challenge in all spheres of our life. Especially in Banks, Government offices, healthcare industry, defense organization, educational sectors the authentication of user is now a most vital issue. Government organizations are setting standards, passing laws and forcing organizations and agencies to comply with these standards with non compliance being met with wide-ranging consequences [1]. Both corporate and personal assets are at risk against people trying impersonating users and stealing money and information. So we need security. For providing better security into someone's account the idea of authentication is introduced. Authentication is done to identify whether a person is genuine or not if she/he is genuine then grant the access of the system otherwise denied it. An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. We have three types of authentication techniques.

- Single Factor Authentication(1FA)
- Two Factor Authentication(2FA)
- Multi Factor Authentication (MFA)

a) Single Factor Authentication

In short, single factor authentication is your basic username/ password combination. The single factor in this case is something you know; your password. Most business networks and most internet sites use basic username/password combination to allow access to secured or private resources. Single-factor-authentication methods such as the basic username/password combination are no longer sufficient enough. Today's widespread use of single factor authentication is in the midst of change. Two-factor authentication provides a significant increase in security. No longer will an un-secured password provide enough information to a hacker to allow a breach in security. The password or pin number must be used in conjunction the use of tokens, smart-cards or even biometrics. The combination of the two factors will provide companies make sure of the people accessing secure systems.

b) Two Factor Authentication

Two factor authentication(fig:1) is exactly what it sounds like; you need two factors to prove who you are instead of just one. Two factor authentication provides a significant increase in security over the traditional username/password combination.

Fig:1:Two Factor authentication, Pic source: www.vasco.com

There are three universally recognized factors for authentication exists today:

- Something known: - examples of this include a password, a pin, a secret key, a private key etc.

- Something possessed:- examples of this include a debit card, a credit card, a smart card, a passport, a driver's license ,an identification card etc.

- Something inherent:- examples of this Biometrics such as what you are finger prints, face reorganization etc.

Use two-factor authentication whenever possible, it is one of the strongest ways to protect access to your accounts and information[2].

Example

A common example of two factor authentication is your ATM card. To access your ATM (fig:2) you need to have something (your ATM card) and you need to know something (your PIN). If an attacker steals your ATM card, it does them no good unless they also know your PIN (which is why you never want to write your PIN on the card). By requiring two factors for authentication you are better protected as opposed to just one. Two factor authentication works online in a manner similar to your ATM card and PIN combination. You use your username and password when you want to access your online accounts. However, after you successfully enter the correct password, instead of going directly to your accounts the site requires a second factor of authentication, such as a verification code or your fingerprint. If you do not have the second factor then you are not granted access. This second step protects you. If an attacker has compromised your password, you and your account are still safe, as the attacker cannot complete the second step without having the second factor.

Fig 2:An ATM machine, Pic Source: www.instantfundas.com

c) Multi Factor Authentication(MFA)

Multi factor Authentication is especially important when it comes to protecting enterprise data and it uses more than two factors.

II. VARIOUS FACTORS OF TWO FACTORAUTHENTICATION

a. Password

The simplest and oldest method of entity authentication[1] is the password based authentication.
Fixed password and One Time Password(OTP).

FIXED PASSWORD: A fixed password is a password that is used over again for every access. Several schemes have been introduced, one upon the other.

i. *Direct (P)*

In this approach(fig3), the system keeps a table (a file) that is sorted by user identification. To access the system resources, the user sends her user identification and password, in plaintext, to the system. The system uses the identification to find the password in the table. If the password sent by the user matches the password in the table, access is granted; otherwise, it is denied.

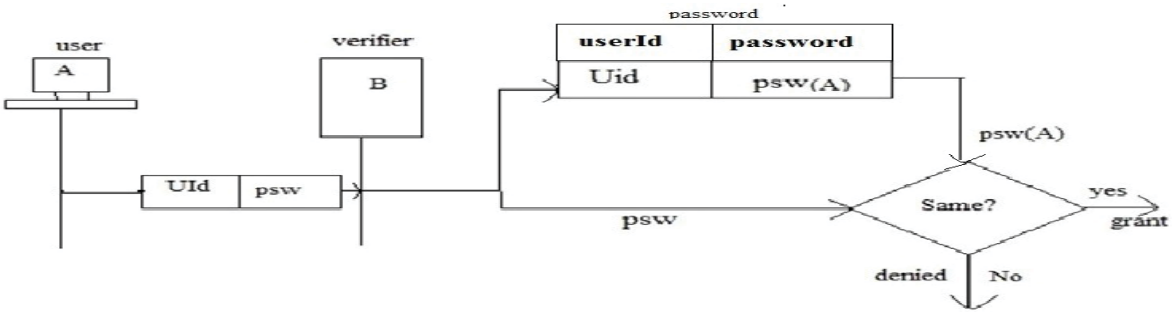


Fig3: By using direct value of the Password

ii. *Hash Function(P)*

A more secure approach is to store the hash(fig:4) of the password (instead of the plaintext password) in the password file. Any user can read the contents of the file, but, because the hash function is a one-way function, it is almost impossible to guess the value of the password. When the password is created, the system hashes it and stores the hash in the password file. When the user sends the ID and the password, the system creates a hash of the password and then compares the hash value with the one stored in the file. If there is a match, the user is granted access; otherwise access is denied. In this case, the file does not need to be read protected.

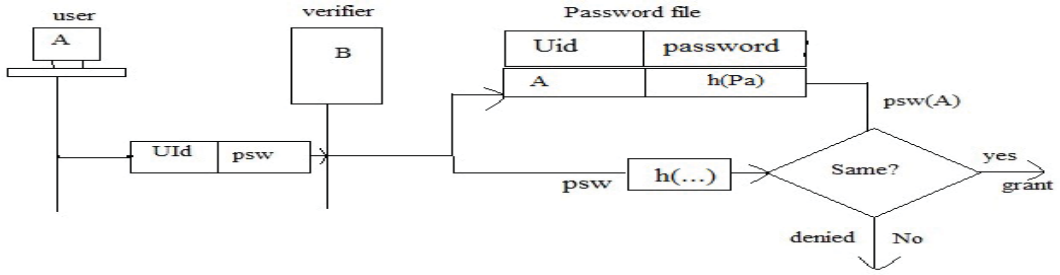


Fig4 :By Applying a Hash Function on a password

iii. *Salting*

The third approach is called salting (fig:5) the password. When the password string is created, a random string is called salt, is concatenated to the password. The salted password is then hashed. The ID, the salt, and the hash are then stored in the file.Now,when a user asks for access, the system extracts the salt, concatenates it with the received password, makes a hash out of the result, and compares it with the hash stored in the file. If there is a match, access is granted; otherwise, it is denied.

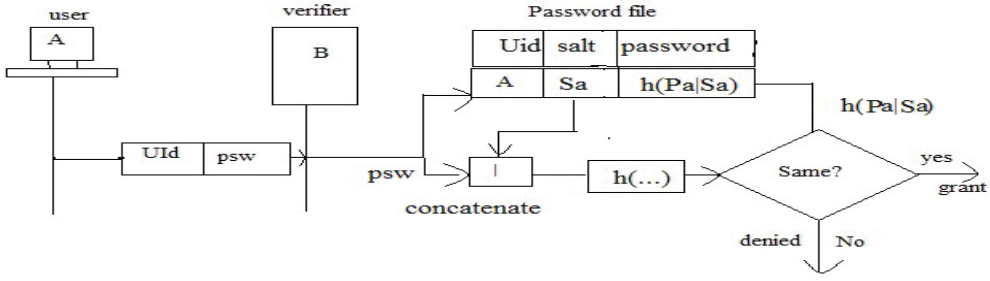


Fig5:Salting a Password

In this approach ,two identification techniques are combined. A good example of this type of authentication is the use of an ATM card with a PIN(Personal Identification Number) .The card belongs to the category 'something known'. The PIN is a password that enhances the security of the card.

➢ *PASSWORD STRENGTH*

In general the longer a password is the stronger it is, it relates directly to mathematics. Passwords can be associated with a cryptographic value which is dependent upon a number of variables. Using additional variables such as upper case, lower case and numbers can generate even stronger passwords.
Long passwords are good, but consider the following:
User 1 password = redcheese6
User 2 password = dflihkpo
User 1 password is made up of 2 words and one number, assuming 20,000 easy to remember common words in the English language, strength is 20K * 20K * 10 = 4 billion or in terms of cryptographic strength, a 32 bit key.
User 2 password is 8 characters randomly generated therefore strength is 26 to the power of 8 = 208 billion combinations or in terms or cryptography strength, a 38 bit key.
The User 2 password is stronger and surpasses the strength of user 1. However, to gain this sort of strength usually requires the user to have a photographic memory or to write this password down.

ONE TIME PASSWORD

A one time password is a password that is used only once.This kind of password makes eavesdropping and salting useless.This three approaches are:

i. In the first approach, the user and the system agree upon a list of passwords. Each password on the list can be used only once. There are some drawbacks in this approach. First, the system and the user must keep a long list of passwords.Second,if the user does not use the passwords in sequence , the system needs to perform a log search to find the match. This scheme makes eavesdropping and reuse of the password useless. The password is valid only once and cannot be used again.

ii. In the second approach, the user and the system agree to sequentially update the password. The user and the system agree on the original password, P1, which is valid only for the first access. During the first access, the user generates a new password, P2, and encrypts this password with P1 as the key.P2 is the password for the second access. During the second access, the user generates new password,P3, and encrypts it with P2; P3 is used for the third access. In other words, Pi is used to create Pi+1.If third parties guess the first password (P1), she can find all of the subsequent ones.

iii. In the third approach, the user and the system create a sequentially updated password using a hash function. In this approach,elegantly devised by Leslie Lamport, the user and the system agree upto a original password, Po ,and a counter, n. The system calculates $h^n(P_0)$,where h^n means applying a hash function n times.In other words,
$h^n(x)=h(h^{n-1}(x))h^{n-1}(x) = h(h^{n-2}(x))\ldots h^2(x)=h(h(x))h^1(x)=h(x)$

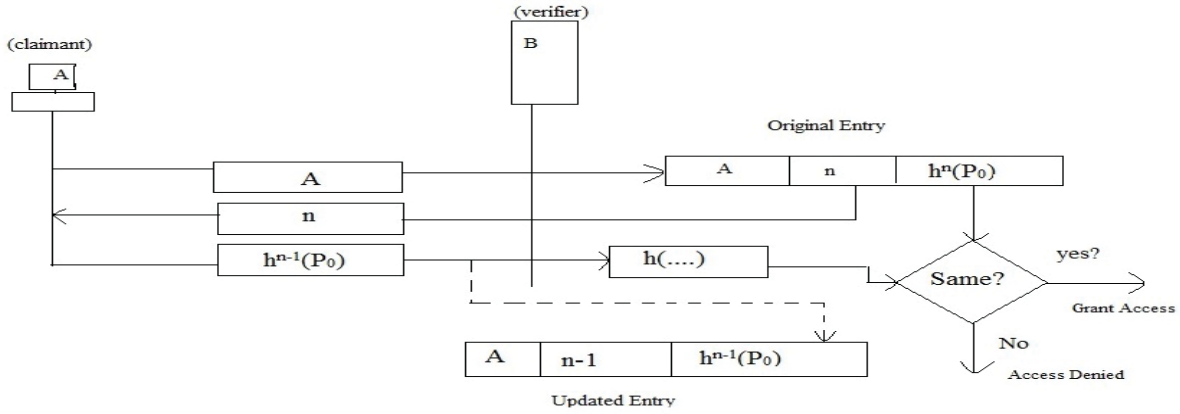


Fig:6:Lamport one time password using hash function

The system stores the identity of A, the value of n, and the value of $h^n(P_0)$.Above fig. shows how the user accesses the system the first time. When the system receives the response of the user in the third message, it

applies the hash function to the value received to see if it matches the value stored in the entry. If there is a match access is granted; otherwise, it is denied. The system then decrements the value
Of n in the entry and replaces the old value of the password $h^n(P_0)$. with the new value $h^{n-1}(P_0)$. When the user tries to access the system for the second time, the value of the counter it receives is n-1. The third message from the user is now $h^{n-2}(P_0)$.When the system receives this message, it applies to hash function to get $h^{n-1}(P_0)$,which can be compared to the updated entry. The value of n in the entry is decremented each time there is an access. When the value becomes 0, the users can no longer access to the system; everything must be set up again. For this reason, the value of n is normally chosen as a large number such as 1000.

- *ATTACKS ON OTP*

i. All OTP authentication system needs to protect from a man-in middle attack.
ii. But it is secure from replay attack.

b. Token:

Fig:7 Cryptographic tokens, Pic source: wordtothewise.com

Tokens (fig:7) display a set of numbers on a small screen. Usually, the set of numbers changes every minute. This number then is joined with the user's password, or pin number to create a passcode. A correct passcode then authenticates the user to access the secure resources. Banks and companies are using tokens as a mean of two factor authentication. A security token is a physical device that an authorized user of computer services is given to aid in authentication. It is also referred to as an authentication token or a cryptographic token.

Tokens come in two formats: hardware and software.

Hardware tokens are small devices which are small and can be conveniently carried. Some of these tokens store cryptographic keys or biometric data, while others display a PIN that changes with time. At any particular time when a user wishes to log-in, i.e. authenticate, he uses the PIN displayed on the token in addition to his normal account password.

Software tokens are programs that run on computers and provide a PIN that changes with time. Such programs implement a One Time Password (OTP) algorithm. OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in the sequence. The sequence should be random to the maximum possible extent, unpredictable, and irreversible. Factors that can be used in OTP generation include names, time, seed, etc.
Several commercial two factor authentication systems exist today such as BestBuy's BesToken, RSA's SecurID, and Secure Computing's Safeword. BesToken applies two-factor authentication through a smart card chip integrated USB token. It has a great deal of functionality by being able to both generate and store users' information such as passwords, certificates and keys. One application is to use it to log into laptops. In this case, the user has to enter a password while the USB token is plugged to the laptop at the time of the login. A hacker must compromise both the USB and the user account password to log into the laptop. SecurID from RSA uses a token (which could be hardware or software) whose internal clock is synchronized with the main server. Each token has a *unique seed* which is used to generate a pseudo-random number. This seed is loaded into the server upon purchase of the token and used to identify the user. An OTP is generated using the token every 60 seconds. The same process occurs at the server side. A user uses the OTP along with a PIN which only he knows to authenticate and is validated at the server side. If the OTP and PIN match, the user is authenticated. In services such as ecommerce, a great deal of time and money is put into countering possible threats and it has been pointed out that the client and the server as well as the channel of communication between them is imperative. In 2005 the National Bank of Abu Dhabi (NBAD) became the first bank in the Middle East to implement two

factor authentication using tokens. It employed the RSA SecurID solution and issued its 19000 customers small hardware tokens [7, 14]. The National Bank of Dubai (NBD) made it compulsory for commercial customers to obtain tokens; as for personal customers the bank offered them the option to obtain the tokens. In 2005, Bank of America also began providing two factor authentication for its 14 million customers by offering hardware tokens. Many international banks also opted to provide their users with tokens for additional security, such as Bank of Queensland, the Commonwealth Bank of Australia and the Bank of Ireland. Using tokens involves several steps including registration of users, token production and distribution, user and token authentication, and user and token revocation among others.While tokens provide a much safer environment for users, it can be very costly for organizations. For example, a bank with a million customers will have to purchase, install, and maintain a million tokens. Furthermore, the bank has to provide continuous support for training customers on how to use the tokens. The banks have to also be ready to provide replacements if a token breaks or gets stolen. Replacing a token is a lot more expensive than replacing an ATM card or resetting a password. From the customer's prospective, having an account with more than one bank means the need to carry and maintain several tokens which constitute a big inconvenience and can lead to tokens being lost, stolen, or broken. In many cases, the customers are charged for each token. We propose a mobile-based software token that will save the organizations the cost of purchasing and maintaining the hardware tokens. Furthermore, will allow customers to install multiple software tokens on their mobile phones. Hence, they will only worry about their mobile phones instead of worrying about several hardware tokens.

c. Biometrics

Biometrics used as the Second Factor. The use of tokens, smart cards and key fobs are the primary second factor in two-factor authentication. However, as technology advances, biometrics are taking and increasing role to insure the identity of individuals trying to access resources. An alternative to key fobs, tokens or smart cards, using biometrics as a part of two-part authentication is a fairly old concept. While advances in technology make biometrics more conceivable cost wise, adopting this concept still is the most expensive alternative for resource security. Biometrics is the measurement of physiological or behavioral features that identify a person (authentication by something inherent).Biometrics measures features that can not be guessed, stolen, or shared.

➢ *COMPONENTS*

Several components are needed for biometrics, including capturing devices, processors, and storage devices. Capturing devices such as readers(or sensors) measure biometric features. Processors change the measured features to the type of data appropriate for saving. Storage devices save the result of processing for authentication.

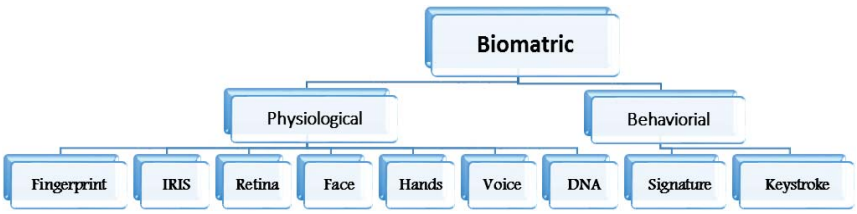
➢ *AUTHENTICATION*

Authentication is done by verification or identification.

- *Verification*: In verification, a person's feature is matched against a single record in the database (one-to-one matching) to find if she is who she is claiming to be. This is useful, for example, when a bank needs to verify a customer's signature on a check.

- *Identification* :In identification, a person's feature is matched against a single record in the database (one-to-many matching) to find if she has a record in the database. This is useful, for example, when a company needs to allow access to the building only to employees.

➢ *TECHNIQUES*: Biometric techniques can be divided into two broad categories:



PHYSICOLOGICAL TECHNIQUES

Physiological Techniques measure the physical traits of the human body for verification and identification.

i. *Fingerprint*

Although there are several methods for measuring characteristics associated with fingerprints (fig 8 and fig 9), two most common are minutiae based and image based. In the minutiae based technique, the system creates a graph based on where individual ridges start/stop or branch. In the image based technique the system creates an image of the fingertip and finds similarities to the image in the database. It supports both identification and verification. However, fingerprints can be altered by aging, injury, or diseases.

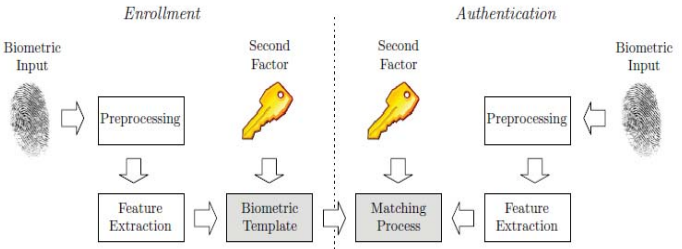


Fig:8 , The basic operation mode of a two factor authentication System. During enrollment and authentication additional factors are presented to the system[3]. Pic source: paper on 2FA Christian Rathgeb and Andreas Uhl University of Salzburg,Salzburg, Austria.

Fig9, Fingerprint,Pic source: forums.oneplus.net

ii. *Iris*

This techniques measure the pattern within the iris(fig:10) that is unique for each person. It normally requires a lasar beam (infrared).

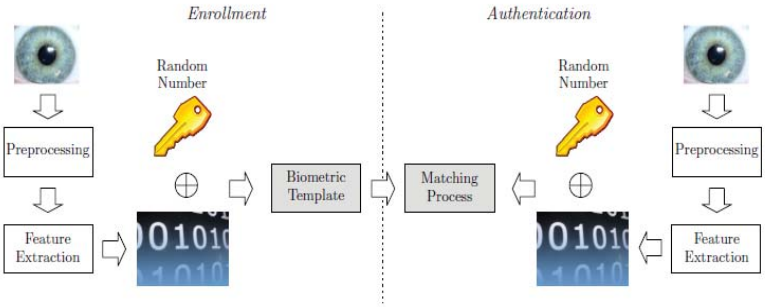


Fig 10, Random numbers are introduced with which iris codes are sequentially XORed during enrollment. At authentication the biometric template is XORed with another random number and the result is matched against an extracted iris code. Pic source: paper on 2FA Christian Rathgeb and Andreas Uhl University of Salzburg, Austria.

iii. *Retina*

The devices for this purpose examine the blood vessels in the back of the eyes. However these devices are expensive and not common yet.

iv. *Face*

This technique analyzes the geometry of the face based on the distance between facial features such as the nose, mouth, and eyes. Some technologies combine geometric features with skin texture.

v. *Hand*

This techniques measure the dimension of hands, including the shape and length of the fingers. This techniques can be used in indoors and outdoors.

There are two more physiological techniques DNA and voice. But these are not used very frequently in real life.

BEHAVIORAL TECHNIQUES

Behavioral techniques measure some human behavior traits[4].

i. Signature

In the past signature were used in the bank industry to verify the identity of the check writer. There are still many human experts today who can determine whether a signature on a check or a document is the same as a signature on file.

ii. *Keystroke*

The keystrokes (typing rhythm) techniques measure the behavior of a person related to working with a keyboard. It can measure the duration of key depression, the time between keystrokes, number and frequency of errors, the pressure on the keys, and so on.

- *ACCURACY*

Accuracy of biometric techniques is measured using two parameters:
False Rejection Rate=False Rejection/Total Rejection.
False Acceptance Rare=False Acceptance/Total attempts.

- *APPLICATION*

Several applications of biometrics are already in use. In commercial environments, these include access to facilities, access to information systems, transaction at point of sales, and employee timekeeping. In the law enforcement system they include investigations (using fingerprint or DNA) and forensic analysis. Border Control and immigration control also use some biometric techniques.

d. Smart Card

Smart Cards are used in combination with a Smart Card reader. The user will insert the card and the card sends an encrypted message to the website or, the reader displays a unique code that the user will enter.

III. PHONE BASED AUTHENTICATION

In general two approaches are taken by manufacturers:

- *Software installed on a phone that creates a one time passcode:*

The main issue with software installed on a phone is how to start the application. The current diverse range of user interfaces on different mobile phone types leads to a significant challenge for support staff. They would need to be fully trained in all supported phone types to help guide the end users[6] through the relevant menus and sub menus needed to navigate to the "Java" section on the phone and then start the relevant authentication program. In addition some phones require a connected PC to install additional software and other types can use the phones browser to download software. Both methods require the end user to understand how to install the software. It is generally accepted that any approach to support more than one operation system will lead to significant technical challenges. An approach that requires software to be installed on a mobile phone should only be considered for a deployment that supports one or a very limited number of mobile phone model types. Finally is should be remembered that users that do not have a company issued mobile phone should be encouraged to use their own private phone. Adding software to a private phone is not only Unsupportable but invasive to the user's property. In comparison, sending a one time SMS message to them is no more invasive that any other person communicating with them especially if you can demonstrate that their phone number is kept secret and will only ever be used for SMS authentication messages.

- *Authentication information sent via SMS in real time:*

By utilizing SMS (texting) all GSM mobiles can be supported without the need to add or support additional software on the phone. However sending authentication information to a users' phone in near real time is a flawed approach. Expecting this text to arrive after the user has entered their user name and pin is inconsistent as SMS text messages suffer from delivery delays at peak times. In addition, if the user authenticating is located in an area that can not receive a mobile signal especially buildings with large stone walls, the incoming SMS message can not be received.

IV. PROS AND CONS OF TWO FACTOR AUTHENTICATION OR ATTACKS ON 2FA

While two-factor authentication[5] may seem like the perfect cure-all for securing networks and resources, there are many security holes that this type of authentication will not protect against. Fake websites provide would-be hackers a way of getting personal information from individuals. The 'store-front' looks authentic, and the user ends up entering information like credit card numbers, social security numbers and bank account information directly into the hands of an identify thief. Two-factor authentication can not protect someone against this type of man-in-the-middle attack. Another type of security breech is if the would-be hacker already has access the computer itself. Then when the user accesses either company or internet resources, the attacker then attempts to piggyback on the transmission and either perform fraudulent transactions, or access secure resources. Trojan horse attacks like this one also cannot be prevented with two-factor authentication.

V. COST

One last factor that may inhibit the introduction of two-factor authentication is the cost. In a two-factor authentication scheme where the second factor is the use of key fobs, or tokens, the costs of those devices alone can be anywhere between $75 and $100 per token. For a company that employ's hundreds of personnel, this initial cost can be quite high. For a company that has thousands of customers online, the cost of the tokens alone could reach into the millions of dollars. Then there is the cost of the infrastructure needed to support the system. Servers, licensing, Administrators and support personnel have to be compensated, server hardware must be kept up-to-date, and support costs and product licensing must be paid. At first thought, only companies with deep pockets might be able to afford the ability to use this functionality. However, as Franklin Curtis of Network Computing states, "Every authentication system carries costs, even if you're using the authentication capabilities included in your network operating system or enterprise application and even with the simplest authentication schemes, developing a user database, assigning privileges, training and supporting users, and maintenance costs must be factored in.

VI. TWO-FACTOR AUTHENTICATION IN INDUSTRY

Even though two factor authentication has been around for decades, its adoption into the business world has been slow. However E-Trade[7] Financial and Bank of America have recently adopted this technology to protect their online customer base. E-trade Financial adopted two-factor security with a pilot that began in December of 2004. After an initial pilot of 240 users, E-trade is going to offer free authentication tokens for a select group on individuals. Security traders with more than $50,000 in combined assets, or individuals who regularly trade more than five trades a month will receive these tokens. E-Trade has partnered with Digital Security ID to help implement these improved security standards. Opponents of implementing token based authentication say that keeping up with the token will be an inconvenience. E-Trade President, Lou Klobuchar states, "If they care about this, and they want this additional level of security, we're providing them with a solution. If there was no inconvenience whatsoever to using it, it wouldn't be much of a solution. Bank of America also has implemented a different form of two-factor security. A cyber criminal from Latvia used a key-logging program to get account information from the business owner, and used that information to get $90,000 wired to his personal account. Instead of using a token and randomly generated numbers to authenticate to the banking network, customers will enroll into the system by picking an image they will remember, writing a phrase, and then selecting three challenge questions. On future visits, the customer will enter their user name and then the image they selected will be displayed on the screen, along with the phrase they input upon registration. The image and phrase will then confirm to the user that they are on an authentic B of A website, and not a counterfeit site.

VII. CONCLUSION AND FUTURE CHALLENGES

Two Factor authentications is the future of security measures. It is now the best type of authentication method. In case of on-line money transaction in Banking service or any other Institution the 2-way authentication may be very much useful. Few years before in banking sector only password was used for any kind of money

transaction but nowadays in almost all Banks they introduced password and additional One Time password(OTP) which is valid for only for 5 minutes. Microsoft has even begun implementing various types of two factor authentication into various parts of their business. Further providing that the technology works PayPal made use of this technology recently and has incorporated it into their web services. If you are able to look at like all other technologies, that it's an imperfect yet growing technology, and that many businesses have found great success with it, it's not hard to understand why it is the best type of security we currently have. Two factor authentication becoming an industry standard in a short amount of time. Things like biometrics and Authentication 2.0 further on the future of this security. With so many businesses adopting 2FA, its only a matter of time before other businesses follow suit. Two factor authentication systems is a user friendly package and require little prior knowledge of software. The system is highly flexible and is well efficient to make easy interactions with the database. However, there are many scope to improvise this concept to make the entire authentication system totally unbreakable.

REFERENCES

[1] Roger Elrod,East Carolina University,Summer 2005,DTEC 6870,Semester Project,Due: July 17,05.

[2] White Paper: Options for Two Factor Authentication, Authors: Andrew Kemshall, Phil Underwood, Date: July 2007

[3] Two-Factor Authentication or How to Potentially Counterfeit Experimental Results in Biometric Systems_ Christian Rathgeb and Andreas Uhl, University of Salzburg, Department of Computer Sciences, A-5020 Salzburg, Austria, crathgeb, uhl@cosy.sbg.ac.at.

[4] Cryptography and network security,Behrouz A Forouzan,Debdeep Mukherjee, 2nd Ed.

[5] A Comparative Usability Study of Two-Factor Authentication Emiliano De Cristofaroy University College London e.decristofaro@ucl. ac.uk,Honglu Du PARC, honglu.du@parc.com ,Julien Freudiger PARC julien.freudiger@parc.com Greg Norciey Indiana University, gnorcie@indiana.edu.

[6] On the (In)Security of Mobile Two-Factor Authentication Alexandra Dmitrienko2, Christopher Liebchen1, Christian Rossow3, and Ahmad-Reza Sadeghi1,1 CASED/Technische University at Darmstadt, Germany,2 CASED/Fraunhofer SIT Darmstadt, Germany,3 Vrije University Amsterdam, The Netherlands.

[7] Evaluting the performance of 2FA solution in the BANKING SECTOR ,Olufemi Sunday Adeoye, Department of Computer Science, University of Uyo, Nigeria.