Secure Transactions using Wireless Networks

Rajeswari.P M.tech(CS) V.Sreenadha Sharma(Associate Professor)
Audishankara college of engineering and technology.
Raji.0534@gmail.com

Abstract

Internet is the main tool for e-business. E-transaction is made faster by Internet. With the increase of e-transaction internet fraud or e-business fraud is increasing. Credit fraud in the banking sector is a growing concern. Few sort of card (debit/credit) fraud is decreasing by providing detection and prevention system from banks and government. But card-not-present fraud losses are increasing at higher rate because of online transaction as there is no chance to use Chip and PIN as well as card is not used face-to-face. Card-not-present fraud losses are growing in an un-protective and un-detective way. Here we seek to investigate the current debate regarding the credit fraud in the banking sector and vulnerabilities in online banking and to study some possible remedial actions to detect and prevent credit fraud. The research also reveals lots of channels of fraud in online banking which are increasing day by day. These kinds of fraud are the main barriers for the e-businessthE banking sector.

Keywords: Public key Encryption ,Hashing Technique, OTP Configuration, One Way Functions ,Psuedo random output.

Introduction

Now a days most of the people using the internet because internet providing the more services to the customer for e.g., Net Banking, E-Transaction, Online applications etc.., Authentication is more required for internet providing services because there is no authentication at that time unauthorized persons is also easy to access the authorized persons profile for this one authentication is required for internet providing services The internet providing the username ,password options these are unique one. Based on these username and password easy to login and transaction that particular website through our smart cards. In this *process* we are facing one problem that is..,

PREOBLM

An unauthorized person that to who knows our details like username and password also they are having our smart card at that time they can easily login to that website and easy to purchase through that our smart card to over come this problem ,In the proposed one ,we are describing the TWO FACTOR AUTHENTICATION mechanism.[1]

SOLUTION

Two factor authentication gives a protection for E_Transaction process by the name itself it describes that TWO FACTOR AUTHENTICATION that is,for authentication it provides two factors,one is, already the USER KNOWS, another one is, They HAVE TO KNOW.

The first password is getting from the banking system. where we get the second one,that is also provided by the banking system only. how to get the second one is, number of second multiple passwords are coming from the initial sedd [2]to the mobile phone through the sms. the use of the sms systems the user knows password is a static password.

WHY WE NEED MOBILE PHONE

An authentication scheme using the mobile phone as an aurhentication token because in this one, GSM method is used already the people had learned that how to use the GMS method in the mobile phone and also In the proposed solution does not require any extra hardware device installed in the mobile phone at the user side. Parallely, the mobile phone is working as a hardware token device,to the E-transaction process.[3]

LITERATURE SURVEY

The idea of an OTP was first suggested by leslie lamport[4] in the early 1980's. otp means that one time password this is valid for a single login session or transaction.Otp is emphasizes that each time the user tries to log on, the algorithm produces pseudorandom output generator thus improving the security.

PUBLIC KEY ENCRYPTION

Needham and Schroeder[5]described a means for authenticating signatures using public key encryption First A's is a secret key and B's is a public key

Notation: A→B:{{PASSWORD}ASK}BPK.

The sending message is USER A to USER B,which has been doubly encrypted.The receiver B is read the message by applying the A's secret key then decrypting the encrypted text.In a world of permanent and uncompromised keys this technique provides a fool proof authentication mechanism.[7]

HASHING

The OTP generation is more secure. A secret key is used together with the challenge.The secret key is shared between the server and the client. The simple password exponential key exchange protocol is used for exchange the key.To exchange the keys we are using the simple password exponential key exchange protocol this is more securable.[5] this is also used for an hacker that means who is able to read and modify all the messages between the client and server that person cannot learn the shared key and cannot make more than one guess for the password in each interaction with a party that knows it.[6]

The SPEKE required only two messages like

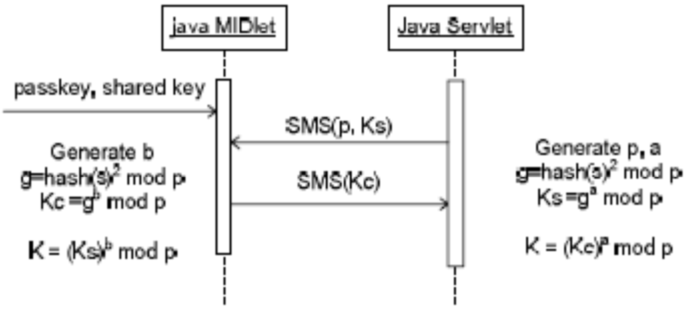

Figure 3. Key exchange

The keyexchange is generating a large and randomlyselected prime p and it computes

In this one 's' is for ,displaying the short OTP in the browser after registration Then the server computes,

g = hash(s)2 mod p
Ks = g a modp

In the above equation 'a' stands for to generate random number It sends servlet to MIDLET is p and ks through the sms after receiving the sms from the servlet server,the MIDLETgeneratesthe

g = hash(s)2 mod p
Kc = gb modp

MIDLET generates the random number it sends to servlet server kc to the AS and computes The secret key is,

K = (Ks)b mod p.

After receiving the secret key kc MIDLET computes the

K = (Kc)a mod p

OTP generation:

The OTP is generated from a hash of a concatenation of the challenge and the secret key

OTP=hash(challenge||secretkey)

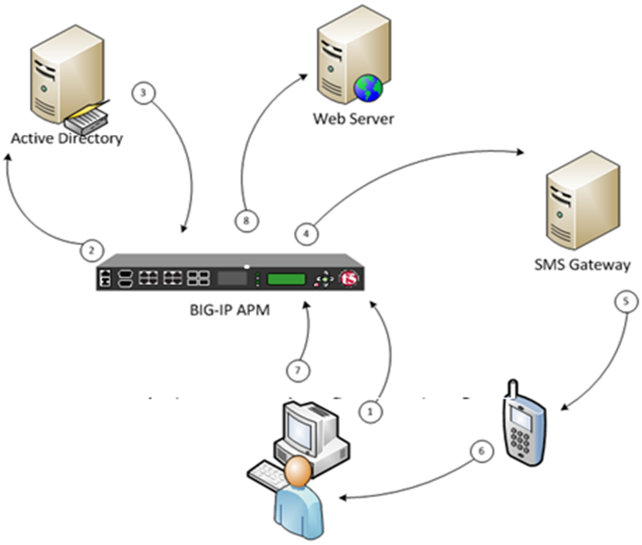

Fig: OTP Process flow

IMPLIMENTATION

For security purpose the proposed system is consists are of three parts
(1)In the client's mobile phone software is installed,
(2)Server software,
(3)The GSM modem is connected to the sever.

OUR APPROCH

Three recognized Authentication factors are existing today:

(i)What you know(e.g.,Password)
(ii)What you have(e.g.,Token)
(iii)Whatyouare(e.g.,biometrics)

In this one,we are extended the Lamport's idea along with some modifications because to produce forwardness and infiniteness. Why we produce these two because to avoiding the use of public key encryption.In this one,we integreate the lamort's idea using two different one way hash functions,h1(.)--this is seed updating and h2(.)--this is for OTP generation

OTP(A,B)=h2^B(h1^A(initial password))

MOBILE REGISTRATION

User wants Two different hash functions h1(.) and h2(.) and initial seed 'sint' these three factors are installed on their mobile phones the service provider is shared this information.Theseed is shared the unique parameters of the host and the uer,because it notifies that whatis the international mobile equipment identity and who is the international mobile subscriber identity and mention the registration date of the mobile phone also username and pin.

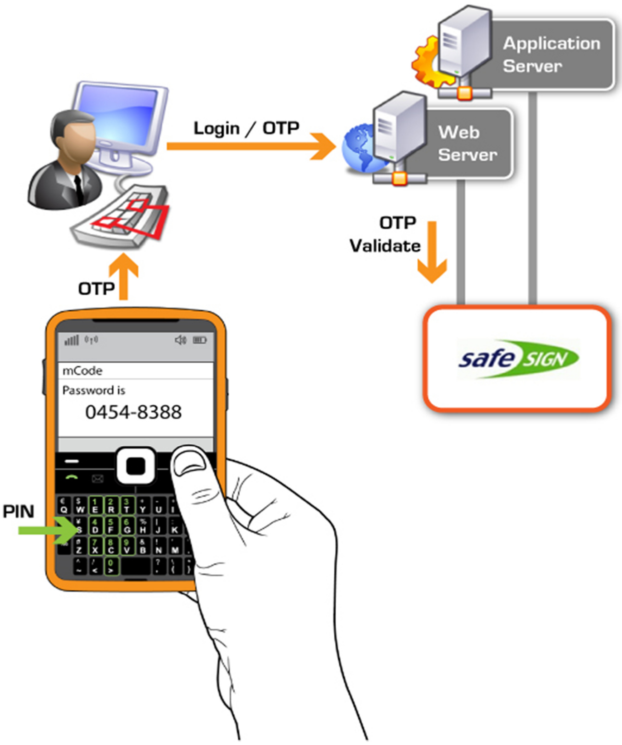

Fig:Mobile Registration

LOGIN REQUEST

When the user enters into the website through the username and the password.After entering the knows password the server compares this password and generates the one time password that will be sent to the user'smobile device .The user then enters the OTPauthentication code fromthemobile devices and a 4 to 8 digit pin onto the webpage that I waiting for user input to comlete the transaction.[8]

OTP ALGORITHM

To protecting the our smart cards, we are requested the server to generating the OTP.how its generates it should be hard for hacking and hard to guess and retrieve for unauthorized persons. To satisfy these factors the server generates the OTP.[9]

IMEI NUMBER

IMEI stands for International Mobile Equipment This is accessible for mobile phone and it will stored in the server's database for each client
Identity this is unique for every individual customer.

IMSI NUMBER

IMSI stands for International Mobile Subscriber Identity this is single unique number associated With all GSM and universal mobile telecommunications system network mobile phone users.

USERNAME

The username is not needed because in the IMEI NUMBER it gives all the details of the cutosmer but why we are specifying that is the username is integrated with the pin this Is used for to protect the details of the customer from unauthorized persons when the authorized mobile is lost.

PIN

The data of the username and password are together so, there is no problem once the mobile phone is lost because the OTP cannot be generated correctly without knowing the user's the PIN.

MINUTE

The OTP for each every minute it must be unique this is valid for only one minute time.

FUNCTIONALITIES

CONFIGURATION OF OTP: Configure the OTP characteristics through the policy editor and attributes of this are,

- Restricted time
- Outgoing message template
- Delivery channel
- Number of tries are restricted
- Format of the OTP(e.g..,name,number,numeric,alpha)
- Length of the OTP

CONCLUSION

Now-a-days single factor authentication e.g..,password are easy to guess and easy to hacking for hackers because password are like names,age are easily discovered by automated password collecting programs for this one, recently introduced the TWO FACTOR AUTHENTICATION based on OTP. This is for to meet the demand of organizations for providing stronger authentication options to its user.In The TWO FACTOR AUTHENTICATION for each and every account of the customer they want hardware token. are carry their mobiles at all the times so,in the mobile phone we can install all wanted tokens like software and hardware. This is helpful for both client and organization.

This paper mainly focuses on discovering of TWO FACTOR AUTHENTICATION method using mobile phones. This is somewhat easy solution because there is no need to take extra hardware to the mobile phones. In this one, does not require any extra burden on the customer and organization also. This solution is mainly used for internet providing services like E-Transactions, online applications, net banking ,Infranet etc..,

The customers are more attracted for this TWO FACTOR AUTHENTICATION solution because this is more securable. The OTP algorithm provides some factorsbecause to secure the user profile.

In the proosed system we are implementing TWO options these two are using a free and fast access i.e..,Connection-Less Authentication system and SMS-BASED Authentication System in this one, Connection-Less Authentication system are more expensive based on SMS-Based Authentication system because in the Connection-Less Authentication system there is no connection between client and the server.The server generates the OTP and it sends to the user's mobile phone, but SMS-Based Authentication System is somewhat less cost solution.

In the future developments includes another factor other than the factors i.e.., Somebody You know, that is based on the notation vouching.

REFERENCES

[1] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram khan "OTP-Based Two-Factor Authentication Using Mobile Phones" In international conference on information technology"2011.

[2] S.HAllsteinsen, I.Jorsta, D-v.,Thanh,"Using The mobilebphone as a security token for unified authentication", Sysyems and Networks Communication In:internationalconference on Systems and Networks Communications,2007,p.68-74

[3] S.M.Siddique, M.Amir,"GMSecurity Issues and Challenges SoftwareEngineering",Artificialintelligence,Networking and Parallel/Ditributed Computing,2006. SNPD 2006. 7th ACIS International Conference on digital Object Identifier,pp.413-418.

[4] L.Lamport, "password Authentication With Insecure Communication", In:comm.:ACM,vol.24,no.11,1981,pp.770-772.

[5] Jablon, D., Strong Password-only Authnticated Key Exchange.Computer Communication Review, ACM SIGCOMM, 1996.vol.26 (no.5).

[6] Recorla,e., RFC 2631 Diffie-Hellman Key Agreement method.1999.

[7] Authntication ofignatures using public keybencryption Kellogg S.Booth university of water 100,Canada.

[8] AcceessMatrix TM UAS Future Proof Universal Authntication Server.

[9] Fadi Aloul,SyedZahidi Wassim El-Hajj "Two-Factor Authentication Using Mobile phones".