International Journal of Education and Science Research Review

E-ISSN 2348-6457

Volume-3, Issue-1 February- 2016,

P-ISSN 2349-1817

www.ijesrr.org

Email- editor@ijesrr.org

COMPULSION & ARCHITECURE OF TWO WAY AUTHENTICATION SYSTEM

Vikas Jain
Assistant Professor
Dept. of Computer Application
C.C.S. University, Meerut

ABSTRACT

Authentication is a process from which the valid user can access the services from the system. Providing the access to only authenticated persons to use the service is getting tougher now a day because the intruders can collect the information of the person and based on that they are going to break the security of the system. The security to the system can be provided using various methods. The types of the security system are password based systems such as ATM machines, internet banking etc., physical based security system such as RFID, Id cards etc. and biometric based system such as iris recognition, face recognition etc. In password based security system user can get access to service if and only if the password is matched accurately. Commonly the user will set the password based on his/her personal information such as their birth place, favourite person, lucky number etc. In Two Way authentication technique use a best approach for secure web transaction. It uses a TIC code it is called transaction identification code and SMS it is called short message service both provide the higher security level. TIC is a OTP (one time password) technique and issued by bank or other financial institution to the user or person who is access to the web services.

KEYWORDS: Authentication, security

INTRODUCTION

The growing popularity of cloud based services is prompting organizations to consider shifting applications and data onto cloud. However, organizations dealing with highly sensitive information are apprehensive of moving its applications & data to public cloud owing to concern about security of its information. It is hence incumbent on service providers that only legitimate Users will access its services and resources in cloud. Verifying authenticity of remote users is a necessary pre-requisite in a cloud environment before allowing access to secure resources/services/ applications. The simplest & most commonly used user authentication mechanism is password based authentication. However, Users tend to choose easy to remember password, and many a times use same password for multiple accounts, which makes it often the weakest link in security. Furthermore, service providers authenticating Users on the basis of password, stores password verification information in their databases and such authentication schemes with verification table are known to be vulnerable to various attacks.

Two-factor authentication technology overcomes the limitations of password authentication and decreases the probability that the claimant is presenting false evidence of its identity to verifier. If different service providers set up their own two-factor authentication services, Users have to do registration and login process repeatedly. Also, Users accessing multiple cloud services may be required to hold multiple authentication tokens associated with various service providers. Authentication factors such as crypto-tokens and smart cards with cryptographic capabilities have been vastly used as a second authentication factor. However, Users are required to always carry these authentication tokens which make it cumbersome from practical usability perspective. Also its usage involves cost thus restricting its adoption to corporate environments. The authentication process can be made more user-convenient if the authentication factor chosen is such that it is commonly used by all types of Users. Leveraging the use of mobile phone as an authentication factor can help address issue of user convenience at no extra cost while improving the security of authentication schemes.

TWO WAY AUTHENTICATION APPROACH

Introduction:- secure electronic transaction is a one way authentication technique so it increase lots of risk that way use one more approach is called multifactor authentication technique .it is a secure wed transaction it also include the cell phone in this transaction. Multifactor Authentication Technique:- This process use the two authentication techniques a) TIC (Transaction Identification code) & b) SMS.

TIC AUTHENTICATION TECHNIQUE

It is a Transaction Identification Code used to identify both the user which is involve in this transaction. It is identify the transaction has been initiated by the valid user or right person.

- TIC codes are issued by the bank.
- It is combination of numeric or alphanumeric characters.
- It is randomly generated number. It is 8 bit or 16 bit number which is assign to user or customer.
- It is like a one time password which means one TIC code used only one time during transaction
- It is unique code.

In this process we are assuming bank are responsible to store TIC generation logic and they are also responsible the complexity of TIC code .bank are responsible for keep TIC as a secret. Bank also provide the list of TIC code to the customer or user. The Bank or Financial institution will keep a record of issued TIC codes to its customers and match the same code during the online web transaction. A TIC code is cancelled after each successful transaction.

SMS Authentication Bank stores the customer phone number to provide sms confirmation to user during transaction. We assume that user will carry his cell phone or receive sms. After getting sms user also send the response (YES or NO). when user send YES which means he is a valid user and he want to access the information & when user send NO or does not send any response to web server which means it is not a valid user and transaction will be terminated.

TWO WAY AUTHENTICATION SYSTEMS

It is a system for two way authentication it describes the five major components:-

- User : user is a valid account holding customer of the bank
- Customer Agent (CA): it is software which is installed into user mobile device.
- Merchant Agent (MA): it is a online service provider so that user can perform online transaction and purchasing through merchant agent.
- Customer bank : this is the bank at which the user has a valid account

Merchant bank: this is the bank at which merchant has valid account

SMS GATEWAY SERVICE PROVIDER

SMS has shown significant resilience in market that is bombarded with media that all add to the clutter of daily Communications. SMS is a form of highly personal, immediate communication with high reach capability, low cost and high retention levels. With communications media converging, SMS is now accessible in many ways as a business tool. SmsCountry is an SMS Gateway provider, which provides an interface between an existing systems and the SMS Messaging Gateway.

It is a lower level connectivity option, but offers the very good functionality and flexibility for the end user. With the API SmsCountry can set up alert-based SMS delivery from SmsCountry's server. Depending on the messaging requirements, SmsCountry may find one or more of SmsCountry's products to suit SmsCountry needs, out of which they have opted HTTP API which gives us the easy ways in order to connect to the SmsCountry API for sending SMS.

HTTP/HTTPS API is one of the easiest server-based ways of communicating SmsCountry's gateway. We can use it either in the form of a HTTP-POST or as a URL that uses GET method for sending SMS. It is recommended to POST for larger data transfer, due to the size limitations of GET. Communication to the API can be done either via HTTPS on port 443 or HTTP on port 80. All calls we made to the API must be URL-encoded. The parameter names used here are case-sensitive. Batch messaging done in a variety of ways. For using SmsCountry’s API, we need to register at: www.SmsCountry.com and sign-up there and buy the SMS credits, so that we can send SMS.

ARCHITECTURE OF TWO WAY AUTHENTICATION

Two way Authentication System Architecture is as below. In Two way Authentication System user submit their credentials and that credentials goes to server which is checked that credentials after that if credentials is valid its goes to next step that is generate a code and send it to registered mobile number after and system waiting for that code to be entered.

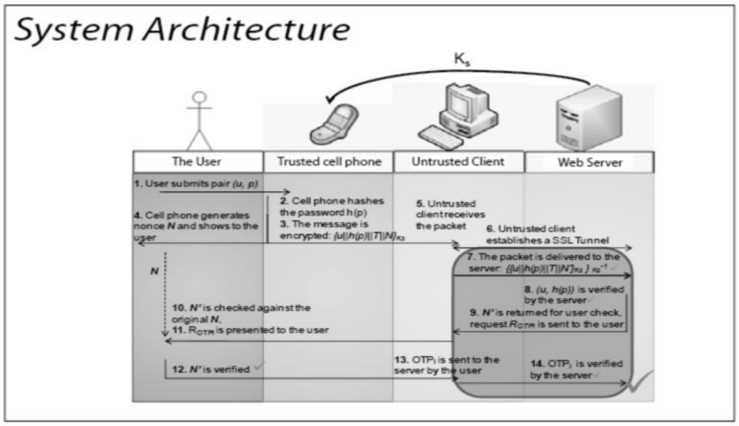

System Architecture
K_s
The User
Trusted cell phone
Untrusted Client
Web Server
1. User submits pair (u, p)
2. Cell phone hashes the password h(p)
3. The message is encrypted: {u||h(p)||T||N}$_{Ks}$
4. Cell phone generates nonce N and shows to the user
5. Untrusted client receives the packet
6. Untrusted client establishes a SSL Tunnel
7. The packet is delivered to the server: {{u||h(p)||T||N'}$_{Ks}$}$_{Ks}^{-1}$
8. (u, h(p)) is verified by the server
9. N' is returned for user check, request R_{OTR} is sent to the user
N
10. N' is checked against the original N,
11. R_{OTR} is presented to the user
12. N' is verified
13. OTP_i is sent to the server by the user
14. OTP_i is verified by the server

Fig-1: System Architecture of 2WAS

After receiving code user submit this code to system and system verified that it’s the right code or not if the code is right then user get welcome page else system goes on login page. With the help of two way authentication we can easily able to secure our id and password from unauthorised access. Authentication scenario is as demonstrate in below diagram

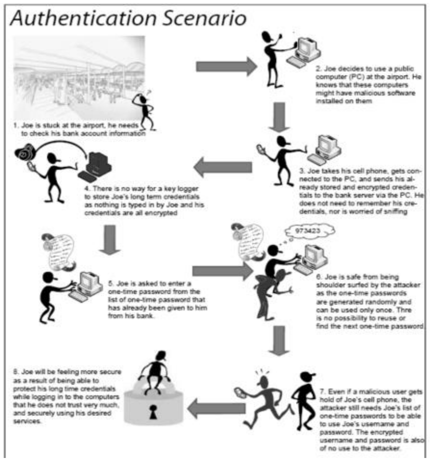
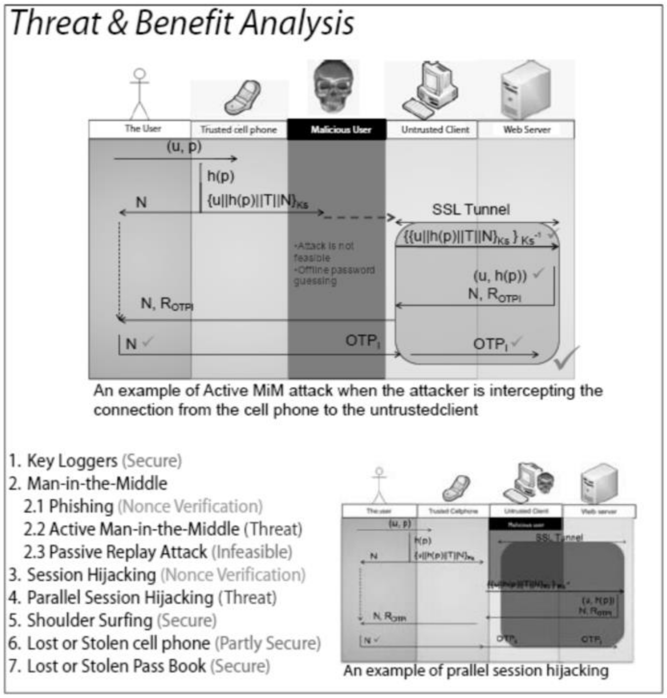

Authentication Scenario
1. Joe is stuck at the airport, he needs to check his bank account information
2. Joe decides to use a public computer (PC) at the airport. He knows that these computers might have malicious software installed on them
3. Joe takes his cell phone, gets connected to the PC, and sends his already stored and encrypted credentials to the bank server via the PC. He does not need to remember his credentials, nor is worried of sniffing
4. There is no way for a key logger to store Joe's long term credentials as nothing is typed in by Joe and his credentials are all encrypted
5. Joe is asked to enter a one-time password from the list of one-time password that has already been given to him from his bank.
973423
6. Joe is safe from being shoulder surfed by the attacker as the one-time passwords are generated randomly and can be used only once. Thre is no possibility to reuse or find the next one-time password
7. Even if a malicious user gets hold of Joe's cell phone, the attacker still needs Joe's list of one-time passwords to be able to use Joe's username and password. The encrypted username and password is also of no use to the attacker.
8. Joe will be feeling more secure as a result of being able to protect his long time credentials while logging in to the computers that he does not trust very much, and securely using his desired services.

Fig 2: Authentication Scenario of 2WAS

THREAT & BENEFIT ANALYSIS

We can do detail analysis and found that with the help of two way authentication system we can do make secure our system with the following



Threat & Benefit Analysis

An example of Active MiM attack when the attacker is intercepting the connection from the cell phone to the untrustedclient

1. Key Loggers (Secure)
2. Man-in-the-Middle
   2.1 Phishing (Nonce Verification)
   2.2 Active Man-in-the-Middle (Threat)
   2.3 Passive Replay Attack (Infeasible)
3. Session Hijacking (Nonce Verification)
4. Parallel Session Hijacking (Threat)
5. Shoulder Surfing (Secure)
6. Lost or Stolen cell phone (Partly Secure)
7. Lost or Stolen Pass Book (Secure)

An example of prallel session hijacking

Fig 3: Threat & Benefit Analysis of 2WAS

After a detailed analysis we found that we can do secure our system from Key Loggers, Phishing, active man in middle, passive reply attack, Session hijacking, parallel session hijacking, and shoulder surfing. So Two ways authentication system is make us more secure than ordinary authentication system.

CONCLUSION

This paper goal was to study and implement the two way authentication method and its advantages over the one way authentication system. This paper was followed with the study of the limitations of the two way mobile authentication systems. Once the above were completed, the focus was shifted to the implementation of the two way authentication method. The algorithm selected is SHA-1 Algorithm, and then the implementation of the design for the password generation was carried out in PHP. This was followed by an application development of a Bank application and testing our implementation of the two way authentication system with such an application. The One Time Password (OTP) was sent to the GSM user through SmsCountry, a SMS gateway provider. During the testing of the implementation, it was found that the system was working fine and that our implementation of the two way authentication system was working and had better security compared to the conventional one way authentication system. Our thesis goal to study and implement a two way authentication method was successful and the functionality implemented by us was working satisfactorily.

REFERENCES

1. A. Wierman and T. Osogami "A Unified Framework for Modeling TCP-Vegas, TCP-SACK, and TCP Reno", Technical Report CMU-CS-02.133, School of Computer Science Carnegie Mellon University Pittsburgh, May 2003.
2. A. Zahary, A. Ayesh, "Analytical Study to Detect Threshold Number of Efficient Routes in Multipath AODV Extensions", proceedings of International Conference of Computer Engineering and Systems, ICCES, 2007.
3. D. Ayesh, "Analytical study to detect threshold number of efficient routes in multipath AODV extensions", proceedings of International Conference of Computer Engineering & Systems, ICCES, 2007, pp. 95 – 100 .
4. G. R. Rao, "Mobility and Energy –Based Analysis of Temporally Ordered Routing Algorithm for Ad Hoc Networks, IETE Technical Review, Vol. 25, Issue 14, 2017.
5. Maheshwari Anita : Two Way Authentication Protocol For Mobile Payment System, Vol. 2, Issue4, July-August 2015, pp.2003-2007
6. N.B.Salem, L. Buttyan, J-P. Hubaux, and M.Jakobsson, "Node Cooperation in Hybrid Adhoc Networks," IEEE Transactions

on Mobile Computing, 2018.

7. Philipp Becker “QoS Routing Protocols for Mobile Ad-hoc Networks – A Survey” August 2017
8. Routing and Multicasting Strategies in Wireless Mobile Ad hoc Networks by Sung –Ju Lee University of California, Los Angeles 2000.
9. S. Thorulp, “Mobile Ad Hoc Networks and Routing Protocols”, Implementing and Evaluating the DYMO Routing Protocol, Master’s Thesis at the University of AARHUS, pp. 7- 20, 2007
10. S. William, cryptography and network security(2nd ed): principles and practice: Prentice-Hall,Inc., 1999
11. S.Capkun, L.Buttyan and J.-P. Hubaux, “ Self-organised Public- Key Management for Mobile Ad-Hoc network”, IEEE transactions on Mobile Computing , Vol.2 , pp. 52- 64,2003.
12. Singh Avnessh, ""A dissertation of Enhancing Cloud Computing Security with two way Mobile Security System,", 2012, pp. 65-72
13. Stajmenovic Ivan, “Handbook of Wireless Networks and Mobile Computing”, Wiley Publications, India, 2002.
14. V. Talooki and K. Ziarati, “Performance Comparison of Routing Protocols For Mobile Ad Hoc Networks” Asia-Pacific Conference on Communications, APCC, 2017.
15. V.D.Gligor, “A Key Management Scheme for Distributed Sensor Networks,” proc. 9th ACM Conf. on Computer and Communication Security (ACM CCS’02), 2016.
16. Y. Kim, IL. Moon and S. Cho: A Comparison of Improved AODV Routing Protocol Based IEEE802.11 and IEEE802.11.4”, Journal of Engineering Science and Technology Vol. 4, No. 2, 2016, pp. 132 – 141
17. Z. J. Haas, J.Deng, B. Liang, P.Papadimitratos and S. Sajama, “Wireless Ad-Hoc Networks” in Encyclopedia Of Telecommunications. John Willey, 2014.
18. Z.Lidong and H. Zygmunt “ Secuting Ad- Hoc Networks” Cornell University,1999.