International Journal of Security and Its Applications
Vol.9, No.9 (2015), pp.265-274
http://dx.doi.org/10.14257/ijsia.2015.9.9.23

Two Way Authentication in MITM Attack to Enhance Security of E-commerce Transactions

[1]Rupali Savita and [2]Unmukh Datta

[1,2]Dept. of CSE
Maharana Pratap College of Technology, Gwalior, India
Dept. of CSE/ IT
savita.rupali19@gmail.com, ummukh62@hotmail.com

Abstract

Serviceable and secure authentication is a research field that approaches dissimilar challenges related to authentication, including security, from a human-computer interaction perspective. The process of identifying an individual usually based on an email id and passwords. In this paper, we focus on client and server authentication. We examine the phishing problem, Man-In-The-Middle Attack, The main challenge in the design of a security system for high security is, how to prevent the attacks against data modification and authentication. Web based delivery is one of the most complicated phishing techniques. Also known as "man-in-the-middle," the hacker is being found on the original website and the phishing system.

Keywords: *MITMA, authentication, phishing, hacker , Security*

1. Introduction

E-commerce: e-commerce is the major success of this era. It is a major achievement of this era. In e-commerce, the transaction phase takes place over the internet. In transaction various phases of an electronic transaction, the more important such as product specification, order details, payment, and delivery information travel methodology of modern business. Through e-commerce we can buy, sell, business of good service over the internet. There are new ways of business over traditional business system. [1]

Type of e-commerce

1) Business to business (B2B)
2) Business to consumer (B2C)
3) Consumer to consumer (C2C)
4) Consumer to business (C2B)
5) Business to government (B2G)
6) Government to Business (G2B)
7) Government to Citizen (G2C)
8) M-commerce (mobile commerce)

In business to business, there is an intermediate between in business, it's like a business organization sell its product to whole seller or business with website through which it connects to customer. Business to consumer, there is no intermediate step; here consumer can directly connect with business which is connected to a website. In consumer to consumer the interaction of consumer on both sides. C2c, where consumer post their advertisement on internet like property, product which they want to sell. On another side a consumer can purchase the product through website. [2] It depends on the website to take for advertisement or not. In consumer to business communicates between

ISSN: 1738-9976 IJSIA

client direct communicate with business site. In business to government vacancy form filled by website is a kind of B2G. In government to business search website that show Auction or tender in government. In government to citizens the policy of government to citizen are provided by such website. It has provided service through wireless technology based on the wireless application protocol (WAP). It includes the sale and purchase of a product, services, bill payment, and information delivery and so on. [3]

Advantage of e-commerce

- Lack of road traffic, man power and page work,
- We can save huge costs,
- E-commerce can increase sales,
- It can make products and services available in remote areas,
- E-commerce provides 24X7 support and service.[4]

2. Principle of Security

In a model world, we make certain the security purpose if each eligible module can get or receive every message intended for it. There are the four rulers of security. There are three more access control, availability and freshness of data.

A. Data Confidentiality:

In confidentiality, unauthorized person should not able to access a sensitive data secret is to use the cryptography technique, data should not seep out, hence pull off the privacy.

B. Data Authentication

The authentication principle helps to verify the identity of a person. The authentication process makes clear in your mind the sender message or document is accurately made out. Authentication of data verifies an identity of the sender and receiver with the help of a few techniques.

C. Data Integrity

The integrity, principle protects data in opposition to of active threats.

D. Data Non-repudiation

This helps to secure communication clients, in sender can prove the receiver can receive the message.

E. Data Access control

Access point enables contact between Host application and field devices, which is controlling the access point.

F. Data Availability

This is helping to provide the necessary needs of customer information.

G. Data Freshness

The principle of freshness means those receivers are receiving the fresh and latest data and make certain that no adversary can replay the not getting any younger data.

H. Scalability

Scalability is not directly connecting with security, but it is an important issue because it has a grand impact on security services. Also scalable security mechanisms to handle large network.

3. Techniques of Authentication

Every field, we must have security as a result security is the one of the most up-to-date topics in nowadays. Authentication is the verification and establishes the identity of the user, which is allowed to user access to the resources. In computer science, authenticated a person's identity is verified often required to secure access to private data or systems.

1) *One factor authentication:* in this authentication mechanism, this is included only one factor such as knowing anything.
2) *Multi factor authentication:* MFA is, truth be told a layer term that describes an authentication format that uses two or more self-sufficient sources to establish, verify the identity.[5] Three aspects of MFA (multi factor authentication):
   a. Something you have
   b. Something you know
   c. Something you are

Something you have, which is can be stolen. Such as key, card, etc. Something, you know, which is can be guessed, united, and stolen. Such as password. And next is something you are which is can be costly and copy for somebody. Such as biometric authentication. Now a day's mostly we combined the two Aspect of authentication like an ATM machine, we all know about the process of ATM machine: ATM card and PIN, ATM card is a 'something you have' and another is 'something you know'.

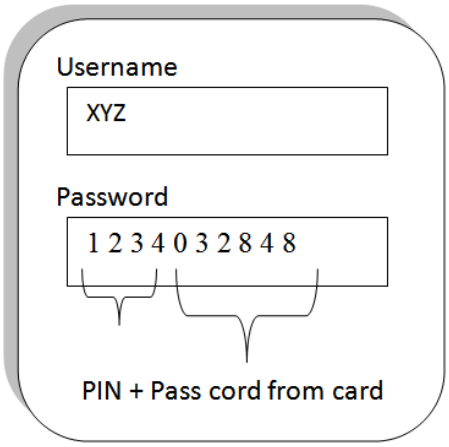

Figure 1. MFA Authentication, ATM Machine

Which is also known as multi factor authentication, a usual example of multifactor authentication would be an ATM machine, in this figure show as which is required, something you have (card, key) with something you know (password) to verify a person.

1) Biometric authentication

Biometric accurately means "measuring existence" and refers to the use of known a recorded objective behavior of a person to authenticate their individuality, common schemes include:

1. Voice identification
2. Fingerprint
3. Face scans

4. Eye prints for instance retina and iris scans.

As we know that word “bio” with the meaning of life and “metric” with the purpose of mean dimension (measurement). We learn of automatic detection, make use of objective or behavioral quality is called biometrics.

2) Transaction Authentication

In the transaction authentication, simply, we authenticated looks for reasonable flaws when compare with data about user details of the current position of the transaction. In authentication transactions many factors are required .

Id address where the user is coming from, identification of user location real world geographic location of user, hardware using a user, time and day, previous user performance of pattern, etc. All factors are key in judging the authentication of identifying activity on trust, verifying digital identity present to the scheme is really who are.

3) Tokens

The token is that small part of a set hardware, which is used in 2 factor authentication for more secure e-commerce transactions or systems. In the form of a card system, dongle, or RFID, chip and provide a one time password (OTP). They can input the code and normal username/password to access a network.
We use a token because it makes it harder for a hacker to access account information easily.

4) Out-of-band authentication

In OOB concept as a whole take a partial channel like a mobile device, which is authenticated a person for transaction originated from a computer. We know that every day transaction cross an entrance like a large cash transfer would trigger a phone call, text message, or notification on a dedicated application (mobile app) that additional authorization is necessary for a transaction to go throughout. This is difficult to hacker hack account information for stealing money.

4. Protocols

In window server 2003 provide some different client/server authentication type verify the identity of person, including:

(1) Kerberos authentication protocol
(2) NT LAN Manager (NTLM) authentication protocol
(3) SSL/TLS: Transport layer security / secure socket layer and SET. [6]
(4) Digest authentication
(5) Smart cards
(6) Virtual Private network and remote access services (RAS)

5. Security Challengers

1) Since the types of threats, attacks and exploits have evolved; various terms have been coined to describe the individuals involved, some of the most common terms being: White hat, Hacker, Black hat, Cracker, Phisher, Spammer.
2) Authentication issues based on node deployment:

First Static Deployment: In this issues operation the nodes are inactive and certainly not shift such nodes are weak to attacks such as replay, node concession as the nodes are without complexity visible. Authentication protocols have to work against in these issues.

Second Dynamic Deployment: A quantity of the issues in this type are re-confirmation of an affecting node, un-traceability a node's progress should be undetectable, communication reliability, secrecy, node confine and finding the middle ground.

6. MITM (Man in the Middle Attack)

Suppose that user has attempted a connection to a web site SP' which impersonates SP. SP' is a man in the middle, i.e., SP' connects to SP as well as user since the SP' connects to SP the information appended to the signature request contains the identity information of SP (e.g., URL information). This information is displayed to U who is expected to check whether it is as same as the connected party – SP' - and if not decides not SP is warned which breaks the connection with SP', thus preventing the MITM attack without any user involvement.

For a better understanding of the key difference between the two protocols, we provide the following example: Suppose Raj receives a phishing email that pretends to be her bank *pbank.com* but contains a link to the bogus Site *ppbank.com*.

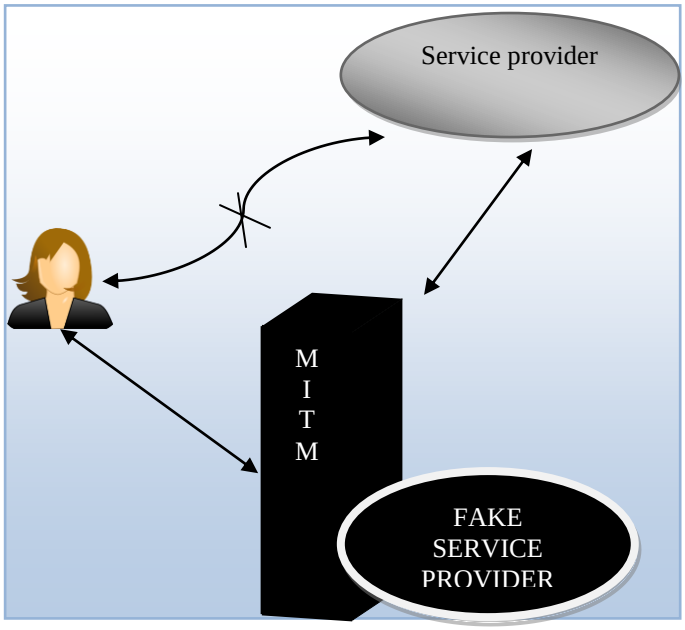

Figure 2. MITM Attack

For a better understanding of the key difference between the two protocols, we provide the following example: Suppose Raj receives a phishing email that pretends to be her bank *pbank.com* but contains a link to the bogus Site *ppbank.com*. With her mobile device, she clicks on the link and opens *ppank.com* while thinking she is visiting *pbank.com*. The bogus site immediately opens a session on the real bank website *pbank.com* to impersonate Alice And commit a fraud. Since Alice chooses to use Mobile-ID, the bogus site has no choice but to mimic it on the real site. Then, the real bank web site establishes a secure connection to MIS to authenticate Alice. [7] MIS obtains a signed Message from Raj machine which contains the information that Raj is connected to *ppank.com*. MIS could easily see the mismatch between the real and bogus web sites and informs *pbank.com* for this incident. As a result, a real-time phishing attack is prevented.[8]

7. Literature View

a. Kanupriya Sharma (2014), In this paper, Discussed on the subject of e-commerce and m-commerce in this paper mutually are extremely opposed to each one previous as well as to resemble in a quantity of intellect. However, nowadays m-commerce suitable towards its further enhance characteristics is replace and attractive position of e-commerce. Thus, in support of the principle of security we have discussed at this time on the subject of unlike biometric technique and moreover, they make use of designed for the purpose of safety measures in m-commerce area everywhere customer execute dissimilar communication. While we need safety and also need a lot of dissimilar technique which are used in support of verification to categorize the justifiable customer [9].
b. Raghav Gautam (2014), E-commerce safety is a component of the in sequence Security structure and is particularly practical to the mechanism that have an effect on e-commerce that take in workstation Security, information security and other wider realms of the in sequence protection structure. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet [10].
c. Praveen Kumar Mishra (2013), types of MITM attacks, their consequences, technique and solution underneath dissimilar conditions giving users options to select single from a choice of solutions. MITM assault is one of the primary techniques in workstation based hack To determine how this category of assault works, in this paper describes a technique of MITM attack based on ARP spoof, and process of preventing such attacks. A recent technique is projected this paper to protect the exchange of open keys in SSP. By adopting the projected method, the substitute of public key becomes new protected and consequently, the procedure of SSP will be protected, steadfast and make available security against MITM attacks [11].
d. K. SHANMUGAM (2014), In this paper focuses on a highly developed mobile safety measures structure to make available fast and extremely protected human being friendly M-commerce transaction. M-commerce transaction works in multistep procedure Protocol WAP gateway. TLS/SSL protocol is used to transmit information and produce between the WAP gateway and server. Seller verification is done by a third party. WTLS and TLS/SSL protocols make use of a message authentication code (MAC) method to make available the information honesty [12].

8. Proposed Algorithm

While we come across that man in the middle attack is a huge difficulty in e-commerce. The MITM attack on the part of a phishing attack, which is create a fake web service provider. However, it can be resolved if we confirm server first, for example. If we are tiresome to open www.flipkart.com then there should be a process by which customer should get some information from the server, which is mainly stored at the time of registration or generated with the facilitate of user performance.

1) In first step user send its own information like user id to the server.
2) In second step server will check the user information to an existing database and ask a question to user to authenticate itself user will answer this question.
3) Now users will ask a question to the server.
4) Server will check the answer and send it to users mail id, in this way severs will authenticate itself.
5) In step user will enter its password to complete its authentication.

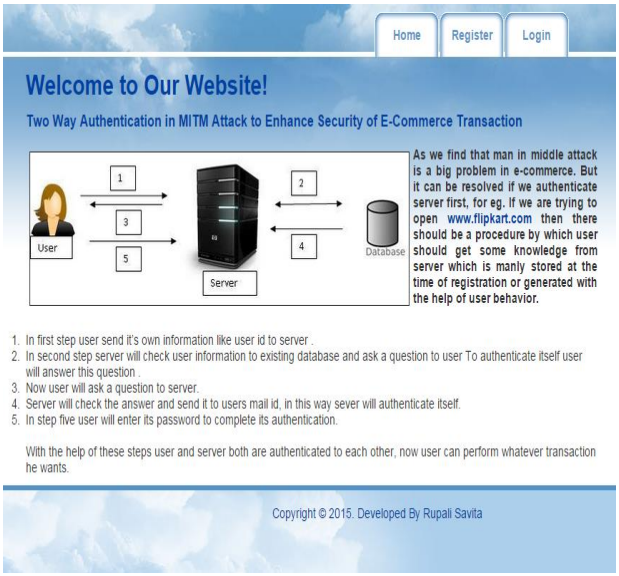

Figure 3. Home Page

Figure 3 which is home page screenshot, and users can interact with this front page. And Description of this website in home page.

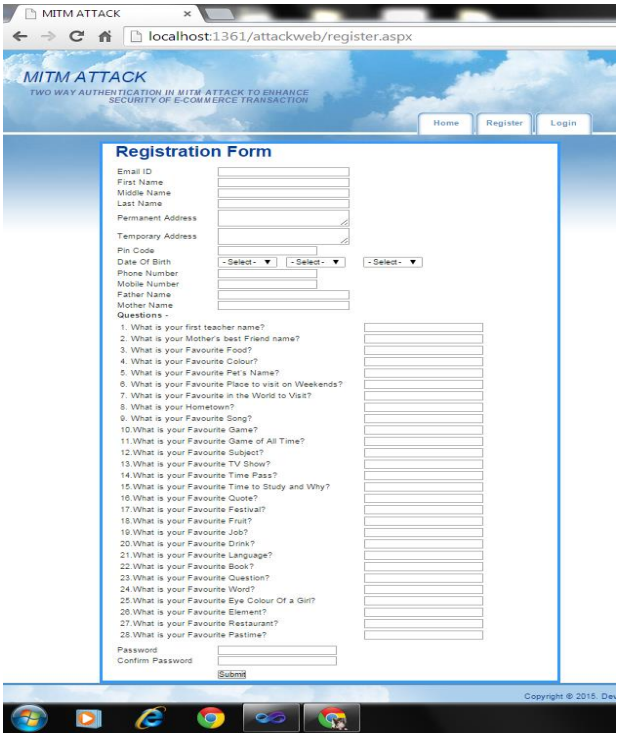

Figure 4. Registration Form

Figure 4 Registration Form, in this screenshot user registration form, some basic information about the user can enter and also 28 questions are complesarry.

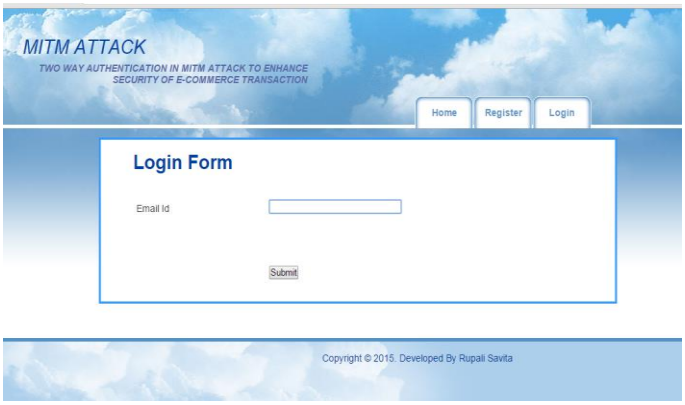

Figure 5. Login Form

Figure 5 Login Form, after registration, the user can enter a valid email_id submit.

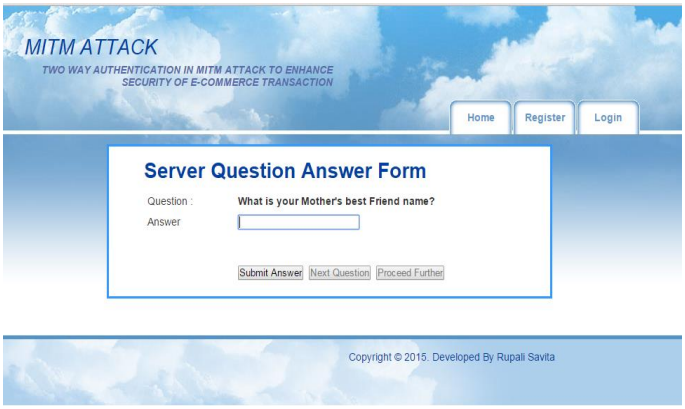

Figure 6. Server Question Answer Form

Figure 6 Server Question Answer Form, now server asks a one question to the user.

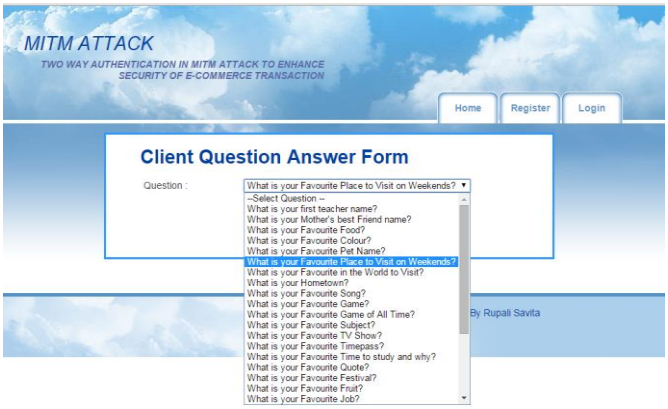

Figure 7. Client question answer form

Figure 7 Client Question Answer Form, in accord to proposed algorithm user can ask any one query to server. And server should be able to send answer user email_id.

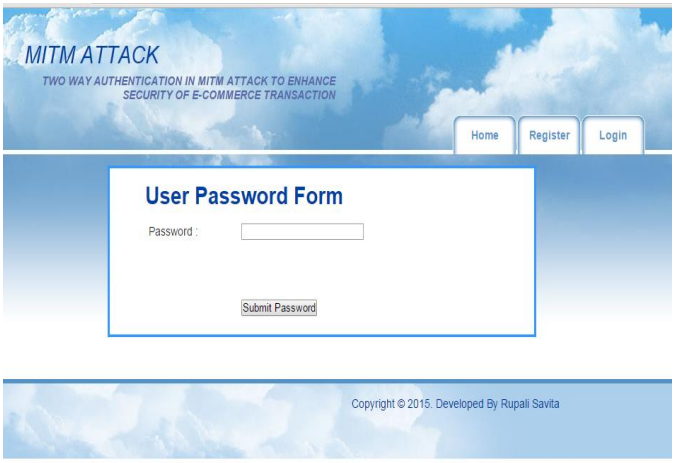

Figure 8. User Password Form

Figure 8 User Password Form, at last step user enters a password and submit this password.

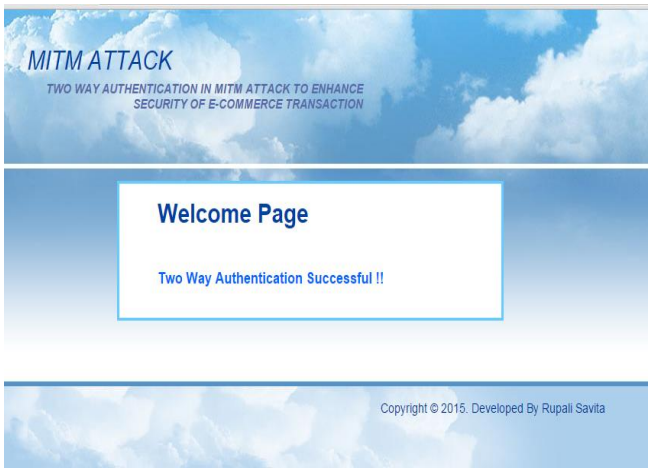

Figure 9. Both Side Authentication

Figure 9 Both Sides Successful Authentication. With the help of these steps user and server both authenticate to each other, now user can perform whatever transaction he/she wants.

9. Conclusion

In this paper, we presented a security authentication technique to overcome the problem of man in the middle attack in e-commerce. We have also examined of Phishing problem and the main challenges in the design of a security system, we also discussed about the different authentication technique in our work we try to solve a very big problem in transaction security of MIMA with the help of our technique first we authenticate a server to a user then we authenticates user for the same server.

References

[1] H. Grewal and Shivani, "A study of ethical and social issues in e-commerce, International Journal of Advanced Research in Computer Science and Software Engineering", vol. 2, no. 7, (**2012**), July.

[2] V. J. Deshmukh, S. S. Kaushik and A. M. Tayade, "Payment Processing Systems and Security for E-Commerce: A Literature Review", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359, vol. 2, no. 5.
[3] K. Sharma**,** "Review of Study of Comparative Analysis of Biometric Authentication Security for M-commerce", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 1, (**2014**) January.
[4] S. Yasin, K. Haseeb and R. J. Qureshi, "Cryptography Based E-Commerce Security: A Review", IJCSI International Journal of Computer Science Issues, vol. 9, no. 2, no. 1, (**2012**) March.
[5] D. Panse and P. Haritha, "Multi-factor Authentication in Cloud Computing for Data Storage Security", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 8, (**2014**) August.
[6] N. Kawatra and V. Kumar, "Analysis of E-Commerce Security Protocols SSL and SET", National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (RTMC) (**2011**).
[7] K. Bicakcia, D. Unalb, N. Ascioglucc and O. Adalierc, "Mobile Authentication Secure Against Man-In-The-Middle Attacks", The 11th International Conference on Mobile Systems and Pervasive Computing, (MobiSPC-2014).
[8] C. K. Kumar, G. Jai Arul Jose, C. Sajeev and C. Suyambulingom, "SAFETY MEASURES AGAINST MAN-IN-THE-MIDDLE ATTACK IN KEY EXCHANGE", vol. 7, no. 2, (**2012**) February.
[9] K. Sharma**,** "Review of Study of Comparative Analysis of Biometric Authentication Security for M-commerce", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 1, (**2014**) January.
[10] R. Gautam, "Network Security Issues in e-Commerce, International Journal of Advanced Research in Computer Science and Software Engineering", vol. 4, no. 3, (**2014**), March.
[11] P. K. Mishra, "ANALYSIS OF MITM ATTACK IN SECURE SIMPLE PAIRING", Journal of Global Research in Computer Science, vol. 4, no. 2, (**2013),** February.
[12] P. K. Mishra, "ANALYSIS OF MITM ATTACK IN SECURE SIMPLE PAIRING", Journal of Global Research in Computer Science, vol. 4, no. 2, (**2013**) February.

