International Journal of Research in Advent Technology, Vol. 3, No.6, June 2015
E-ISSN: 2321-9637

A Survey on Online Transaction Security

Tanvi Dhingra[1], Gurleen Kaur[2]
Department of Computer Science and Engineering [1, 2], PEC University of Technology ,Chandigarh 160012,India[1, 2]
Email: tani26august@gmail.com [1] , gurleen29jeet@gmail.com [2]

Abstract- Online Transaction Security is basically the protection of online transaction assets from unauthorized access, use, alteration, or destruction i.e to ensure CIA (Confidentiality, Integrity, Availability) triad of information security. Online Transactions are emerging as very useful to end users and business parties, but it also creates a set of new risks and vulnerabilities such as security threats. Information security, therefore, is an essential requirement for efficient and effective transaction activities over the internet. In this paper an overview of Online Transactions and Online Transaction Security, purpose of security in online transactions, different security issues in online transactions, and various security mechanisms of online transaction system has being discussed.

Index Terms- Online transaction, Keystroke logging; Biometrics, Secure Electronic Transaction, WebPin Technology

1. INTRODUCTION

With the continuous growth and pervasion of the Internet in all aspects of daily lives almost everything can be done online, which has lead to the increase in online transactions. Online transaction is basically the dematerialised exchange of information between two entities (individuals or organizations) via computer systems. It encompasses a whole range of activities like exchange or trade of ideas, money, goods etc, transfer of funds into, out of or from an account, a deal or business agreement etc. The existing online transaction system has been suffering from many threats. Security is one of the principal concerns that restrict customers and organizations into engaging with online transactions. Moreover, since the transactions completely rely on internet (which is highly unsafe from security point of view) for there working, so security of transactions is one of the major issue these days. Security goals consists of confidentiality, integrity, non-repudiation, authenticity and availability. Online Transaction Security is the protection of transaction assets from unauthorized access, use and alteration. Various security measures have been taken in this direction. Security measures should be applied
in such a way that it protect different components (client, network, server) of online transactions systems and ensure various basic security goals like confidentiality, availability and integrity.

1.1. Elements of online transactions

Elements of online transactions include:

- Client: Client is basically the user's web browser. User requset is processed by the browser and send via https to the network.
- Network: Network includes internet, intranet, virtual private network etc. It basically acts as an interface between client and server and helps them to communicate.
- Server: Server basically includes authority, company, individual. It process the user's request and generate the appropriate response.Fig.1 represents the general framework of Secure Online transaction.

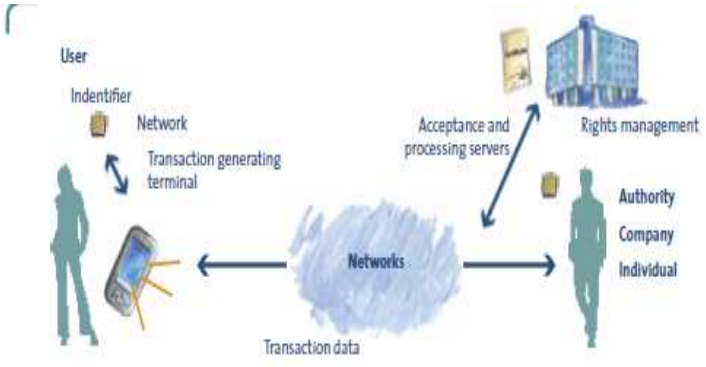


Fig.1: General Diagram of Secure Online transactions[2]

Working of online transaction system is as follows:

- User starts the transaction at transaction generating terminal. Terminal can be any like mobile, PC etc. Web browser at transaction generating terminal process the user request i.e convert it into a particular format for sending it over the network.
- Web Browser via network sends the transaction request to the server.
- Server first verifies the transaction i.e whether it is from valid user or not. If transaction is verified then it will be accepted for further processing otherwise the transaction is discarded.

Fig.2:Man-in-the-browser attack[1]

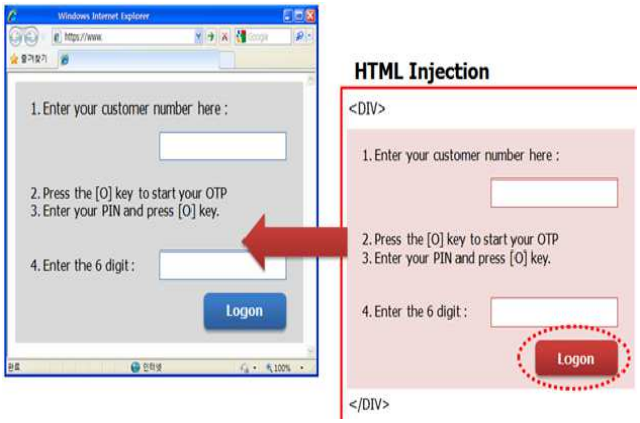
2. RELATED WORK

Large numbers of outstanding achievements has been registered in the research of various cryptography algorithms like DES, triple DES,AES etc for online transaction security and various other security technologies like Secure Socket Layer (SSL) technology, one time password generation, single encryption technique etc have been proposed but security issue is still the biggest problem to online transactions. In a core banking system, there is a chance of encountering forged signature for transaction. And in the net banking system, the password of customer may be hacked and misused. Thus security is still a challenge in these applications. Therefore, it is necessary
to make repeated research and assessment on the mode and security of online payment aiming at eliminating unsafe factors and promoting the development of online transactions[4].

3. SECURITY BREACHES ON ONLINE TRANSACTIONS

3.1. *Man in the browser attack*

Man in the browser attack takes place at client side (i.e on user's web browser). It violates the basic security goal i.e integrity. In this attack a malicious code(e.g Trojan) settles down into the browser and rests asleep. When the user starts its transaction than this malware wakes up itself and manipulate the browser to show a fake login page that looks exactly similar to the login page of the original website with just a few changes like additional fields which asks for filling of verification code, card security and PIN etc. Once anyone unknowingly enter those details, then intruder takes the advantage of that to breach the security.Fig.2 illustrates the Man-in-the-browser attack.



3.2. *Man-in-the-middle attack*

Man-in-the-middle attack takes place on network. This is an attack on confidentiality of online transactions. To execute this attack, attacker uses an approach called pharming which involves the usage of malicious network infrastructures, such as malicious wireless access points to redirect users from the legitimate site they are trying to access to a malicious fraudulent web site that accesses the user credentials and acts on behalf of the user to perform malicious activities.

3.3. *Keystroke logging*

In logging, the user inputs its ID,PIN and password etc. to the website for personal identity authentication through the keyboard. When the user presses the keyboard, the input signals are transmitted through the port connected to the keyboard, a number of other devices, and the keyboard driver to reach the program. Program here is web browser. In Keystroke logging, the key strucked by the user is recorded in a covert manner and the user is completely unaware of it. The recorded structure is later on used against the user to breach user's security. The main steps are as follows:

- Port Polling Attack: This attack takes place at the port, when port receives input signal. In this attack the status of an external device i.e keyboard is sampled by the hacker. Hacker creates a record of this sampled input data.
- Fake driver Insertion: After creating the record of sampled data, hacker inserts the fake driver. A driver is a program that controls the device. So, insertion of fake driver helps the attacker to control the device in its own way.
- Message hooking: After attacking on port and driver, attacker performs message hooking. In message hooking an application can install a subroutine to monitor the message traffic in the system and process certain types of message before they reach the target window procedure.A detailed description of Keystroke Logging attack is shown in Fig.3.

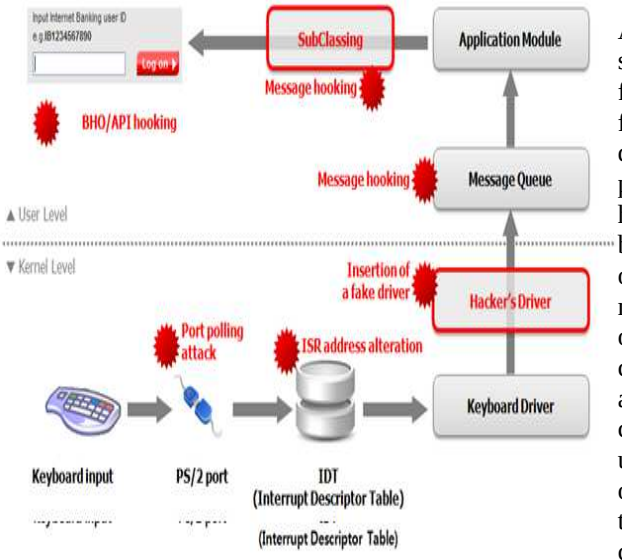


Fig.3:Keystroke logging[1]

3.4. *Phishing*

Phishing is the most common threat to online transactions these days. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames,passwords and other personal details by mas-querading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

3.5. *SQL Injection*

This attack takes place at the server side. This is an attack on confidentiality, integrity, availability of the online transaction data. SQL injection is Common and famous method of hacking at present. Using this method an unauthorized person can access the database of the website and can get all details from the database. With SQL Injections an attacker can bypass logins, access secret data, modify contents of website, shut down the server.

4. SECURITY MECHANISMS

Security is the major concern of online transaction Systems. Security goals like data confidentiality, authenticity, integrity, availability and non-repudiation have to be satisfied for the efficient working of these systems. Various security mechanisms at every stage of transaction have been introduced to achieve these goals and make the existing system secure.

4.1. *Biometrics*

A biometric system is basically a pattern recognition system that operates by acquiring biometric data like fingerprints, hand or palm geometry, retina, iris, and facial characteris-tics, from an individual. Biometric data can not be borrowed, stolen and forging is practically impossible. For this reason a lot of work has been going on to make more and more use of biometrics in online transaction security systems. In online transactions biometric authentication mechanism is used. In biometric authentication, any one biometric data like fingerprints, facial characteristics etc. of user are taken at runtime for authentication purpose. The biometric data(e.g facial characteristics) template would be captured by the user computer and compared against a stored template on a database server. When the user starts the transaction its biometric data(here facial characteristics) is taken during login. This data template is encrypted using RSA algorithm while passing from the network and sent to the host server[2].RSA algorithm is used because it is highly secure from security point of view since it involves a large number of computations which are difficult to brute force. After that server performs verification and if verified then only user will be allowed to access resources. For providing the enhanced security biometrics has been used with the encryption technique so at the wireless transmission no one can hack the biometric data template. Working of biometrics is shown in fig.4 below.

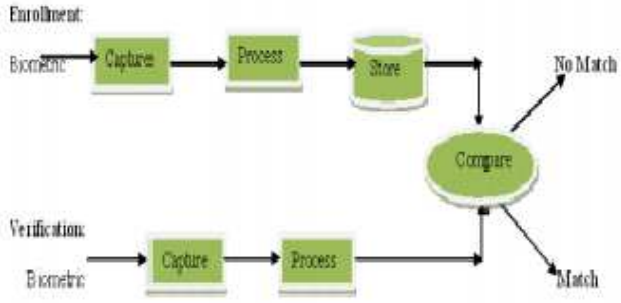


Fig.4:Working of biometrics[4]

4.2. *Secure Electronic Transactions Protocol*

It is a communication protocol standard for securing online transactions. Secure electronic transactions uses cryptography to provide security to the transactions. The most important inovation of SET is multiple encryption technique. The conventional methods of encryption in secure electronic transaction can only maintain the data security. The confidential information of customer could be accessed by the unauthorized user for malicious purpose.
Therefore, it is necessary to apply effective encryption methods to enhance data security as well as authentication of data communication.

1) Multiple Encryption Technique in SET: Multiple encryption techniques is used to generate more secured and advanced digital signature, which is very complicated to crack by any intruder or unauthorized party. In this technique data is encrypted multiple times so that the highly secure digital signature is generated. Steps in multiple encryption technique are:

- Input to the algorithm is plaintext message.
- Next step is to apply hash algorithm to plaintext. Output generated by hash algorithm is message digest.
- Encrypt message digest multiple times with different encryption keys to generate more advance and complex digital signature.
- Whole data with digital signature is sent to the server.[7]

4.3. *Anti Key Logging Technology*

Anti key logging technology is used to detect key logger threats. It compares all the files in the computer against a database of keyloggers looking for similarities which might signal the presence of a hidden keylogger. As shown in the given figure, anti keylogger is implemented at both the user level and kernel level. At kernel level the antikey logger software is implemented when the data goes from port to IDT and to keyboard driver. The software block the port polling attack and fake drivers. At user level antikey logging software detects hooking at each level and block it.

Fig.5 shows the detailed description of Anti key logging Technology.

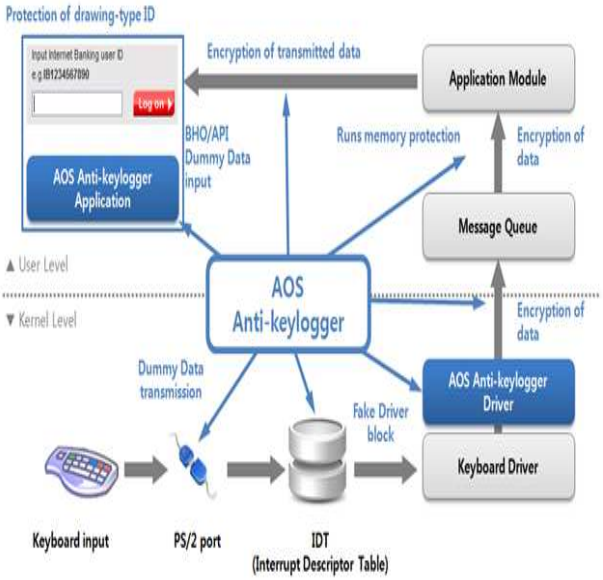


Fig.5:Anti key logging Technology[1]

4.4. WebPin Technology

SSL encryption does not provide end to end security of data i.e when data arrives at the web server it is automatically converted back to its unprotected form rendering it open to
various attacks like man in the middle attack. WebPin technology provides an Internet with end to end security envelope thus solving the problem. WebPin comprises of two main elements:

- A set of java classes,employed at client side,which are used to provide cryptographic functionality to client web browser.
- A hardware security module,employed at server side which provides cryptographic interface between internet environment and server.

1) Working of WebPin Technology:

- When the user via web browser open an internet session to the web server then WebPin enabled applet is downloaded to browser for login screen.
- User then enters the login data and the applet forms the PIN block,encrypt it and MAC's the packet of data to go back to the web server.
- Packet created by the applet is passed to WebPin server machine where MAC is checked , the PIN decrypted and re-encrypted for transfer to host system.
- Webpin Server Machine passes the reencrypted PIN block and calculates a new MAC over the data to be passed to the host.
- The host passes the data to host server machine for the verification of MAC and PIN. Host server machine sends the verification output to the server.[5]

5. CONCLUSION

Online Transaction Security is the protection of online transaction assets from unauthorized access and alteration. There are various security attacks on online transaction system which make the user's terified to use it. Conventional security measures like SSL encryption, authentication does not provide satisfactory security.

Therefore there is a need for satisfactory security system. In this paper various security mechanisms like biometrics, WebPin Technology, Anti key logging Technology, Secure Electronic transaction Protocols for enhanced security of online transactions systems has been discussed. Further improvements in these security technologies have been taking place to provide a more secure system in the near future.

REFERENCES

[1] Online Banking:Threats and Counter measures,http://www.v3webehard.com

[2] Secure Electronic Transactions,http://www.pole-tes.com
[3] Niranjanamurthy M 1, DR. Dharmendra Chahar 2 The study of E-Commerce Security Issues and Solutions; July 2013.
[4] Mangala Belkhede, Veena Gulhane, Dr.Preeti Bajaj Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach;February 2012
[5] Yi Yi Thaw ,Ahmad Kamil Mahmoodl, P.Dhanapal Durai Dominic A Study on the Factors That Inuence the Consumers Trust on E-commerce AdoptionVol. 4, No. 1 2, 2009
[6] Dhirendra Pandey, Dr. A.Rastogi A Critical Research on threats and security technology related to Payment System on E-commerce Network;October 2010
[7] Himanshu Gupta,Vinod Kumar Sharma Role of multiple encryption in secure electronic transaction;November 2011bibitemhSecuring Internet Home Banking,http://www.bluestarindia.com