IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Special Issue || Dec. 2019 || PP 44-50
International Conference on Management Practices, Innovations & Research 2019

A Survey on Online Transaction Processing Security

Aniket A. Ganvir
Department of Computer Science & Engineering Tulsiramji Gaikwad-Patil College of Engineering & Technology Nagpur, India

Abstract*—Nowadays, online transactions are becoming popular in India since Demonetization occurred. Making online transactions having benefits for users like cashback, reward points, redeem coupons, etc. Besides, online transactions are easy and flexible, at other hand, this technology needs strong security method. This paper targets the security concept among the payments which are carried over the Internet.*

Online transaction processing security is nothing but the protection of online payments from illegal access, modification, usage or damage. Online payments are evolving as extremely helpful to end clients and business parties, however it additionally creates new risks and vulnerabilities, for example, security threats. For making effective and efficient transaction operations over the internet, Information security is essential constraint. In this paper a review of Online Transactions and Online Transaction Security, purpose of online transaction security, various security issues in online payments, and different security framework has being talked about.

Keywords—*Online transaction; OLTP; Keystroke Logging; Secure Electronic Transaction; WebPin*

I. Introduction

With the persistent development and invasion of the Internet in all parts of day-to-day lives nearly everything should be possible on the web, which has prompt to the expansion in online transactions. Online exchange is nothing but the dematerialised trade of data between two entities (individuals or associations) through PC frameworks. It covers an entire scope of operations like trade or exchange of ideas, cash, products, fund transfer, business agreement etc. The current online payment system has been experiencing numerous threats. Security is one of the main worries that restrict clients and associations into engaging with online payment processing. Furthermore, since the payments totally depend on internet for there working, so security of exchanges is one of the main issue nowadays. Security objectives comprises of privacy, integrity, authentication and accessibility. Online Transaction Security is the protection of payment assets from illegal access, usage and modification. Different safety efforts have been taken in this way. Security measures must be applied in a manner that it secure various components (client, network, and server) of online payment systems and ensure privacy, availability and integrity which are basic security objectives.

A. Online Transaction Components

Online transaction components include:

- Client: Client is nothing but the user’s web program. Browser processed the request of user and send through https to the network.
- Network: Internet, intranet, virtual private network etc. are included in Network. Network acts as an interface between server and client and caused them to communicate with each other.
- Server: Basically server deals with the authority, association, and individual. It handles the user's request and produce the proper response. Below fig.1 deals with general structure of Secure Online Transaction.

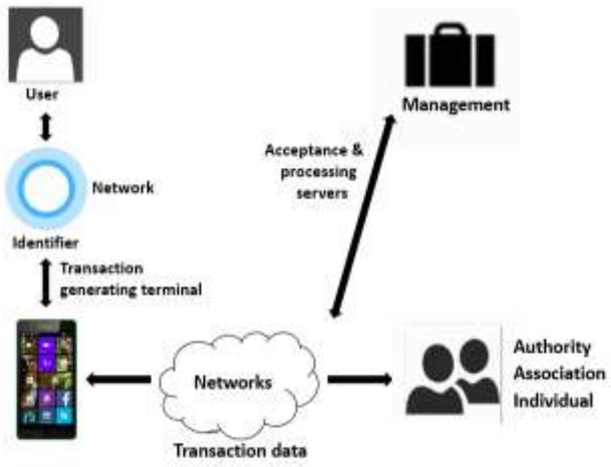

Fig.1: Secure online transactions – general structure.

Online transaction processing system's working is as follows:

- User begins with the transaction at transaction generating terminal. Terminal may be any like mobile, PC, tablet and so forth. Web browser/program at transaction producing terminal process the request of user i.e. change over it into a specific arrangement for sending it over the system.
- After that, Web Browser/Program through network sends the request of transaction to the server.
- After receiving request, first of all server verifies the transaction so that whether it is from legal user or not. If transaction being successfully verified then it will be acknowledged for further processing otherwise the transaction get discarded.

II. Related Work

Security is one of the ongoing concerns that limits customers and organizations engaging with online transaction. Web applications progressively integrate third-party services. The integration brings new security issues due to the complexity for an application to manage its internal states with those of the component services and the web client through the Internet. [2]

Viruses are a dangerous threat in the Internet. Viruses disrupt online operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs are the most serious threat to Internet. Trojan horse programs allow data integrity and fraud attacks and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the online payment server wouldn‘t know the order was fake or real. Password protection, encoded client-server communication, public private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encoded. [3]

Due to the rise in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the raised up awareness of online customers about the threats of performing transactions online. Many customers refuse to perform online transactions cause of lack of trust or fear for their personal information. [4]

Data security has taken on intensified importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the masquerade of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers. [5]

The effect of security, protection and trust towards consumers plays a crucial role in online transaction implementation however, if well carry out, instantaneous flow of goods and services internally and externally. Besides, vital information could also be concurrently processed to match with data flowing from external online transactions which could allow for efficient and effective integration into organizational processes. [7]

III. Security Cracks on Online Transaction

A. Man-in-the-browser attack

Man-in-the-browser attack happens at client side (i.e. on user's web program/browser). It leads to violation of security objective i.e. integrity. In this attack a malicious code (like Trojan) settles down into the program/browser and rests snoozing. At the point when the user begins its transaction than this malware awakens itself and control the program/browser to show a fake login page that design like the login page of the official site with only a couple changes like extra fields which requests for filling of confirmation code, card security and PIN and so forth. When anybody unknowingly enter those points of interest, then intruder takes the benefit of that to break the security. This illustrates in Fig.2 which shows the Man-in-browser attack.

B. Man-in-the-middle attack

Man-in-the-middle attack happens on network. This is an attack on highly-sensitive information of online transactions. To execute this attack, attacker utilizes an approach namely as pharming which includes the usage of malicious system infrastructures, for example, malicious access points which redirect users from official website to a malicious fraudulent site that get the user credentials and acting as genuine user to execute malicious activities.

C. Keystroke logging

In logging, the client inputs its ID, PIN and secret key to the site for personal authentication and authorization through the keyboard. At the point when the user presses the keyboard, the input strokes are transmitted via port connected to the keyboard, various different devices, and the keyboard driver to achieve the program. Here program act as web browser. In Keystroke logging, the key strucked by the client is recorded in an incognito way and the user is totally unconscious of it. The recorded structure is later on utilized against the user to break client's security. The essential steps are as follows:

- Port Polling Attack: Port polling attack happens at the port, when port gets input signal. In this attack, external device status i.e. keyboard is inspected by the hacker. Hacker makes a record of this sampled input information.
- Fake driver Insertion: After making the record of sampled data, hacker attach the fake driver. A driver is a program that controls the gadget. Hence, attachment of fake driver helps the attacker for handling and controlling the device in its own particular manner.
- Message hooking: Here, after attaching on port and driver, attacker gone to perform message hooking. Generally, in message hooking an application can install a subroutine to make monitor the message traffic in the system. Fig.2 shows a point by point description of Keystroke Logging attack.

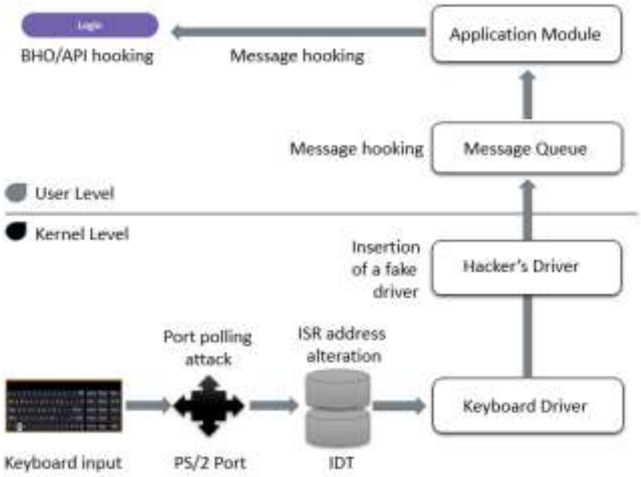

Fig.2: An overview of Keystroke logging.

D. Phishing

Nowadays, phishing become common threat to online transactions. Phishing is nothing but the criminally fraudulent activity in which highly sensitive information like username, PIN and other personal information are try to attempting by taking on the appearance of a genuine entity in an electronic interface. Communication claiming to be from well-known social sites, auction websites, online payment processors or IT managers are ordinarily used to track the clueless public. Phishing is typically completed by email or texting (instant message), and it often trap users to enter log credentials at a fake log-in window whose design is similar and looks like official one.

E. SQL Injection

SQL injection attack happens at the server side. Basically, this is an attack on integrity, confidentiality, accessibility of the online payment information. At present, SQL injection is common and popular strategy for hacking. By using this strategy an illegal person can access the database of the site and also can access the all details from the particular database. In SQL Injection, an attacker can easily bypass log-ins, accesses sensitive information, change contents of site, and shutting-down the server.

IV. Online Payment Services

Online payment services and systems for accepting payments on the Web allows user to making online transactions over the Internet. Popular online payment services are as follows:

A. PayPal

PayPal is the world's most widely used payment service, processing over $4 billion in payments in 2011. PayPal payments are made using a user's existing account or with a CC/DC (Credit Card/Debit Card). Money can be sent directly to an email address, thus allow the users to register for a new PayPal account. Additionally to taking payments, PayPal also allows its users to send money through the service, which is a feature that only a few payment solutions provide. PayPal takes 2.9% + $0.30 per transaction as a pricing and has no setup or monthly fees.

B. Google Checkout

Google Checkout is another online payment service which compete with PayPal. Google Checkout allows users to pay for goods and services via an account connected to their Google profile. Google Checkout payments quite easy because many users already having google account. Google Checkout fees start at 2.9% + $0.30 per transaction for sales less than $3,000.

C. Authorize.Net

Authorize.Net is the Internet's most widely used payment gateway. With a user base of over 300,000 merchants, Authorize.Net has been the go-to method for online payment sites that need a gateway to accepting payments. Widely used e-commerce platforms such as Volusion, X-Cart and Magento are designed to accept payments using Authorize.Net easier.

Authorize.Net has a $99 setup fee, costs $20 per month and takes a $0.10 per-transaction fee.

D. Amazon Payments

Amazon Payments allows its authorized users to receive money using its API (and to send money out via ACH). Amazon Payments are used by popular crowdfunding site Kickstarter. Amazon Payments fees start at 2.9% + $0.30 per transaction for payments over $10 (the percentage they take is less for larger transactions). For payments under $10, the fee is 5.0% + $0.05 per transaction. [12]

V. Online Banking Payment Authorization Methods

Nowadays, with the rise of smartphones and other various applications, additional options for online transactions has arrived. Overview of Internet Banking payment authorization methods are as follows:

A. TAN (Transaction Authentication Number) list

TAN is one of the beginning system for authorization that came on the Banking industry. When customer wish to make online transactions, he/she asked to enter a TAN from a list that the bank sent to legitimate customer.

Generally, the TAN list typically contains 100 numbers that can use to validate payments. Besides, it is very convenient to use, with the exception that the list is limited, so it is not that much secure.

B. TAN with Captcha

To deal with the man-in-the-middle issue, TANs with captchas were generated. This is mainly used in Germany. In this authorization method, a code is associated with each TAN on the list which is called BEN (Confirmation Number). When user make a transaction, user must confirm it with the TAN, but ensure that the captcha returned from the bank which needs to be identical to the one displayed on your list.

The purpose is that, hackers don't have access to the captcha so that they cannot return the accurate code to the customer on the verification page.

C. Mobile TAN

This method differs from TAN lists where mTAN sends transaction numbers to the customer's mobile phone when requested. The message additionally displays transaction information such as the amount of the transaction with merchant name.

Basically, the TAN is generated by the bank when a user initiates a transaction, and then forwarded towards the legitimate user. The mTAN method offers several benefits over basic TAN systems. There is no list in mTAN which can fall into the hands of hackers. While customer's phone may be stolen, he/she have better options to secure it, like encrypting it fully so that attackers cannot get access.

mTAN method may be more secure than basic TANs, but it is still at risk to attacks. For example, malware can be installed on device to grab the information in real-time.

D. PhotoTAN

Basically, the photoTAN method needs an app or standalone device. It works by analyzing colorized QR codes using the app or device. Transaction details are sent to the bank in encoded format where they are processed. The photoTAN system is secure against man-in-the-middle attacks as a separate gadget is being used in the process.

E. FinTS (formerly named as HBCI)

The finTS system is referred as German online banking standard where it uses Electronic signatures (chip card), and also PIN and TAN. It is as secure as it can get, but needs set up which may be too technical for some customers. As a result, TAN systems like basic TAN, TAN with captcha are not strongly secure rather than system that is offering better security.

Mobile TAN is most likely that system, as it is suitable and fairly secure at the same time, provided that user protect his/her own phone by encoding its data or at least locking it in sleep/inactive mode. [6]

VI. Security Mechanisms

Security is the most important worry of online transaction processing systems. Security objectives like integrity, authentication, data-confidentiality, accessibility and non-repudiation must be fulfilled for the effective working of these systems. To secure the existing system, different components at every stage of payment have been introduced to acquire these objectives.

A. Biometrics

Basically, a biometric system is pattern-recognition system that works by gaining biometric information like fingerprints, palm or hand geometry, retina, iris, and facial character, from a person. Biometric information cannot be obtained, stolen and duplicating is not practically possible. As a result, lots of work has been going ahead to make more and more use of biometrics verification in online transaction processing security systems. Biometric authentication is used in online transactions. In biometric verification, for giving authorizations to legitimate user any one biometric information like fingerprints, facial character etc. are taken at run time for verification reason. The biometric data (e.g. facial qualities) layout would be caught by the client PC and get compared against a default stored template on a DB server. At the point when the user begins the transaction its biometric information (here facial qualities) is taken for log-in purpose.

This data template is encoded by RSA algorithm while going from the network and sent to the host server [9]. RSA calculation is used in light of the fact that it is strongly secure from security perspective since it includes large computations which are hard to brute force. After that server performs authentication and if confirmed then just user will be permitted to get resources. For giving the upgraded security biometrics has been used with the encryption technology so at the remote transmission nobody can hack the biometric information template. Below fig shows working of biometrics.

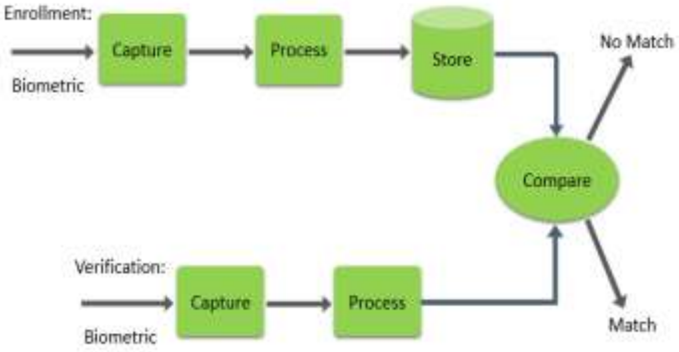

Fig.4: Biometrics working.

B. Secure Electronic Transactions Protocol

It is a communication protocol standard who's used to securing the web transactions. Cryptography is used by secure electronic transaction to provide security to the online transactions. The ordinary techniques for encryption in secure electronic transaction can just keep up the data security. The private data of customer could be accessed by the unauthorized person for further malicious purposes.

Accordingly, it is important to apply effective encryption strategies to improve data security and also data communication authentication.

Multiple Encryption Technique in SET: This technique is used to produce more secured and advanced digital signature. This advanced digital signature is very complicated to crack by hacker or unauthorized party. In this strategy information is encoded multiple times so that strongly secured digital signature is produced. Steps in multiple encryption technique are as follows:

- Input to algorithm is considered as plaintext message.
- Next stage is to apply hash algorithm towards plaintext. Generated output by hash algorithm is message digest.
- Now, encode message digest multiple times with various encryption keys to produce more updated and complex-digital signature.
- Finally, entire information with digital signature is sent to the server. [8]

C. Anti Key Logging Technology

This technology is used to detect key logger threats. It analyzes each and every file in the PC against a database of keyloggers searching signal of presence of a hidden keylogger. As appeared in the given figure, anti-keylogger is executed at both the user-level and kernel-level. At kernel-level anti-keylogger software is executed when the information goes from port to IDT and to keyboard driver. Software block the service of port polling attack and fake drivers. At user-level anti-keylogging software identifies hooking at each level and block it. Detailed description of anti-keylogging technology are shows in fig.5.

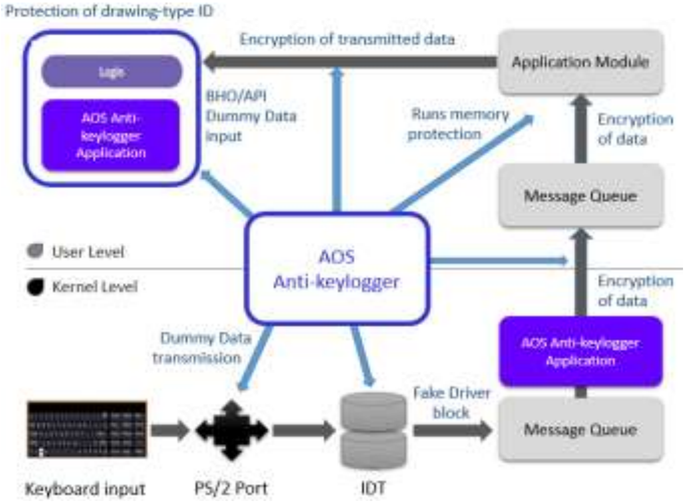

Fig.5: An overview of Anti Keylogging Technology.

D. WebPin Technology

End to end security of data does not provided by SSL encryption i.e. when data comes to the web server it is consequently converted back to its unprotected form. Rendering it open to different attacks like man-in-center attack. However, WebPin strategy provides an Internet with end-to-end security envelope in this way taking care of the issue. WebPin contains two principle components:

- An arrangement of java classes, employed at client side, which are used to give cryptographic functions to client web program/browser.
- A hardware security module, employed at server side which gives cryptographic interface between web environment and server.

WebPin Technology working:

- At the point when the user via web program/browser open a web session to the web server then WebPin empowered applet is downloaded to program/browser for login screen.
- User then enters the log-in information and the applet generates the PIN block, encode it and MAC's the bundle of information to go back to the web server.

- Packet made by the applet is passed to WebPin server machine where MAC is checked, the PIN decoded and re-encoded for transfer to host system.
- WebPin Server Machine passes the re-encoded PIN block and calculates another MAC over the information to be passed to the host.
- The host passes the information to host server machine for the checking of MAC and PIN. Host server machine sends the verification acknowledgement to the server. [1]

VII. Conclusion

Hence, Online Transaction Processing Security is the protection of online transaction assets from illegal access and modification. There are different security attacks on online transaction processing system which make the user afraid to use it. Ordinary security measures like SSL encryption, authentication does not give appropriate security.

As a result, there is a requirement for satisfactory security system. In this paper, different security mechanisms such as biometrics, WebPin Technology, Anti Keylogging Technology, Secure Electronic Transaction protocols for upgraded security technologies have been occurring to give a more secure system soon.

Acknowledgment

First of all, I’m thankful to Prof. R. B. Talmale mam, HoD (CSE), TGPCET, Nagpur. for continuous support and encouragement for completing this paper and also thanks to our CSE Department management staff. I thank Mr. Rajesh Babu sir, Assistant Professor, CSE Department, TGPCET, Nagpur. for his constant support and motivation.

References

[1]. 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

[2]. Asaf Shabtai,Yuval Fledel, Uri Kanonov, Yuval Elovici, Shlomi Dolev (2010), “Google Android: A Comprehensive Security Assessment.” IEEE security and Privacy.

[3]. Dilip Kumar, Yeonseung Ryu, “A Brief Introduction of Biometrics and fingerprint Payment Technology”, Published by the IEEE Computer Society,2008.

[4]. Dr Suresh Sankaranarayanan, “Biometric Security Mechanism in mobile Payment ”, Published by the IEEE Computer Society, 2010.

[5].]B Y Hiew, Andrew BJ Teoh and David CL Ngo, (2006) “Preprocessing of Fingerprint Images Captured with a Digital Camera”, IEEE, ICARVC.

[6]. Martin Brinkmann on May 8, 2014 in Security - How secure are different Online Banking payment authorization methods? http://ghacks.net/deals

[7]. Anil K. Jain, Arun Ross and Salil Prabhakar: “An Introduction to Biometric Recognition” IEEE Transactionson Circuits and Systems for Video Technology, Special Issueon Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[8]. Himanshu Gupta,Vinod Kumar Sharma Role of multiple encryption in secure electronic transaction;November 2011bibitemhSecuring Internet Home Banking, http://www.bluestarindia.com

[9]. Secure Electronic Transactions, http://www.pole-tes.com

[10]. Jake Rocheleau, in E-Commerce, Consumer Guide to Secure Online Transactions, http://www.hongkiat.com/blog/social-commerce/

[11]. Alex Kidman, June 8 2009, Online transaction security: Tips for staying safe, https://www.cnet.com/uk/news/online-transaction-security-tips-for-staying-safe/

[12]. Rosston Meyer, Online Payment Systems, http://sixrevisions.com/ online-payment-systems.html