A Study of Security Schemes and Related Issues inOnline Payment Systems

ChannakeshavaRN
Assistant Professor, Department of Computer Science, Government Science College, Chitradurga,keshavarn@gmail.com.

Abstract: This paper provides a study on existing security schemes in online payments systems and their strengths and weaknesses. Which include security schemes adopted by internet banking, EFTs, Debit/Credit card transactions and wallets etc., As these transactions are carried through transmission medium laid in public access areas, there is always threat of someone intruding into the transmission medium and gets the critical information so that he may utilize the critical data for his benefit. If the transactions carried through online are not secured enough customers or banks always exposed to threat of losing money. For ensuring secured transactions security is enforced in different levels encryption, OTP through phone, security pin etc. all these methods adopted for security willnot deny intruder from reading the content, but makes the information unreadable for a third person.

Keywords: SSL/TLS, Net-Banking, Mobile-Banking, Payment Gateway,Online Payments, OTP, Device Identification, CAPTCHA

.

1. INTRODUCTION:

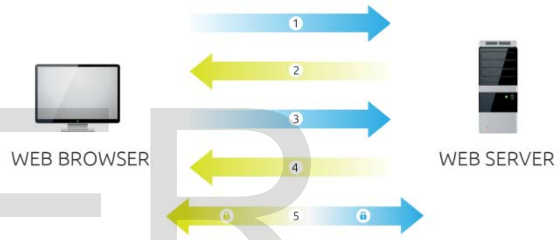
Online payment Systems are getting popular in recent days and after the demonetization online payment systems are becoming popular even in rural sides of the country. EFT, Credit/Debit Cards, Net-banking, Wallets, mobile banking are being the most popular payments, online cheating is always trying to snatch the money from the innocent people. There are innumerable numbers of attacks on accounts of innocent people for snatching money from them. We can recall recently State bank of India confirmed number of debit/credit cards information was theft online. Our study here is to bring a light on security systems adopted by these payment systems to ensure safe and secured transactions.

2. ONLINE PAYMENT SYSTEMS:

Net-banking, credit/Debit card payments, EFT, Wallets offered by payment banks etc are wellknown online payment systems.

Terms in Online Transaction Security Systems:

SSL (Secured Server Login) is a security protocol. The SSL protocol determines variables of the encryption for both the link and the data being transmitted. Transport Layer Security TLS Protocol is the successor of SSLv3. When a web browser attempts to access a website secured with SSL, a “SSL handshake” is executed between the browser and web server. A public key, private key and session keys are used in the SSL. Data encrypted using public key can be decrypted by private key and vice-versa. As encrypting using public key and private key uses lot of computation, they are used only during SSL handshake and for communication after establishing secured connection; session key is used to encrypt/decrypt all the data being communicated.



During the handshake process web server also installs an Extended Validation (EV) SSL Certificate which ensures the end user with assured confidentiality of the website. And this can be verified by the following signs in the browser. SSL uses a 128 bit encryption which means key used for encrypting data to be transmitted maybe one among 2^128 possibilities.

- Green in the address bar (green bar or issuance name, see below)
- Website owner's company name in the address bar
- https:// at the beginning of the domain name
- Padlock in the address bar
- Organization information in the certificate details.

Kerberos: Kerberos is a network authentication tool uses port no 88. Kerberos uses on the basis of tickets to allow nodes communicating over a non-secure network prove their identity to each other in a secure manner. Kerberos is used for only authentications; Whereas SSL is an encryption technique for authentication as well as communication.

One Time Passwords (OTP): to ensure the person trying to login is genuine and authenticated person; most of the web-servers generates a random code and sends it to customer’s phone or e-mail. And login is permitted only after introducing himself with the OTP through the window provided.

CAPTCHA:"Completely Automated Public Turing test to tell Computers and Humans Apart" A randomly generated image which contains text or numbers. This is to be again inputed for authentication through the same page. CAPTCHA avoids automated programs from trying with randomly generated passwords and other security data.

Device Identification: Web servers keeps the tracking details of devices from which each user logging in. if the user is trying to login from a different device than a regular device them more stringent security is enforced. For the regularly logging in devices less security checks are adopted.

Transaction monitoring for fraud detection: practices of user logging in are cross-checked with login failure patterns to block certain devices from logging in. Ex: If a user failed to login from certain device continuously, that particular device is blocked for further logins for that user.

Virtual keyboard: most of the Net-banking websites force the users to input login details from the virtual keyboards provided. This prevents key-loggers from tracking the key pressings while inputting usernames/passwords.

Personalized Messages: Some websites provide way to display personal message before user provides password to login to ensure user is logged into genuine site.

Payment Card Industry Security Standards: These standards are laid down by the payment card industry security standards council. To ensure safe transactions online through cards council has laid standards for: Merchants and processors, for developers and for manufacturers.

Digital Signature: is a digital code generated and authenticated by public key encryption, digital signature is attached to documents transmitted through electronic messages to verify its authenticity.

Payment Gateways: Payment gateway is a server carries out transaction between Accepting Bank (Account of merchant) and paying bank (customer account). These can also handle transaction status such as successful, Unsuccessful, partial etc.

Online Payment Systems:

Net banking: Traditional Banks through their portal give access to the accounts of individuals through a Secured SSL/TLS connection. Normally these transactions require a username and passwords for authentication. Most of the banks are providing 2 fold authentications which require additional information for authentication, such as OTPs through SMS, or e-Mail. Some banks also offering finger print readers through smart phones.

Cards: Maybe it is Credit card or a debit card it is a payment network which are linked to a bank account in the backend. Cards carries out the payments to any other account holder electronically irrespective of banks and geopolitical areas, however governing rules will apply.

Wallets: Wallets are becoming more popular after RBI issued Payment banks license and even after demonetization. Through the wallets one can hold a limited amount of cash as per the laid guidelines. One can transfer this amount to other person's wallet or pay bills using very simple steps so that very less literate can also transfer money digitally. Ex: Paytm, Airtel Bank, Etc.,.

Mobile Banking: Most of the Commercial banks now offering mobile-banking services through which customer can carryout instant payments through Apps. But in 2014 a security expert Winston Bond demonstrated that the mobile banking app downloaded from a app distributor can be reverse engineered and source code of the app is modified according to our intention and it can again uploaded to the distributors site such as google play store.

3. ADVANTAGES OF ONLINE PAYMENT SYSTEMS:

No Fake currency Notes: Physical form of cash are dubbed and a considerable percentage of cash in physical form is mixed with fake notes. Fake currency always drags national economy. More over these notes are easily caught in the hands of innocent poor and middle class people.

No Black money: One who earns money in illegal forms always hides that income without disclosing and also that amount will not be accounted by Income tax department. But when this money is held in electronic format in a bank can be easily tracked by income tax departments. Collection of taxes causes healthy development of the nation.

No Theft/Burglars: Physical form of money can be snatched by thieves or burglars. But snatching money held in electronic form and protected by passwords and other authentication methods cannot be snatched.

Convenience and Time saving: payment of utility bills standing on a line and withdrawing cash from banks terminals/ATMs are time consuming where as you can pay these bills without any hassles using your electronic devices.

Change problems in retail Shopping: Have a 500/2000 Rs Note and you have to take tea, you may have to spend some more bugs in the tea shop for matching the required change.

4. CHALLENGES IN ONLINE PAYMENT SYSTEMS:

Failed Transactions: Almost all transactions carried out are tightly managed for consistency of the accounts. But if a network connection is unreliable and if it fails in between the transaction carrying out, un expected situation may raise; the amount deducted from the payer may not be get credited to the receivers account or a failed transaction may still deduct amount from customer account. These situations are addressed manually by banks, for assuring no loss occurred to the customer.But it is a time consuming activity and people working with little margins will have to face tough times.

Compromising accounts: As Net banking and Credit/Debit Cards are linked to Bank accounts directly and most of bank account holders hold huge amounts of cash in their accounts, this is one treasure that hackers are always keeping on trying on. For hacking a net banking account hackers may use. There are so many stringent rules laid down for securing the payments communication, it has become impossible for a hacker to hack accounts online, and even all the servers are managed and monitored most of the hackers concentrates less educated end user to get passwords ad other security information. For that many techniques are adopted.

An effort to prove that the card payments are not secured; A research paper has been published in the academic journal IEEE Security and privacy, which demonstrated that a dubbed Distributed guessing attack can reveal the credit card number, its expiration date and CVV. However they have demonstrated the security issue on VISA cards, a similar attack on other cards cannot be ruled out.

Phishing: which is a redirected page from any vulnerable website and looks like a same page as official netbanking page only difference will be the URL.

Trojans: Trojans takes the form of a virus and they works as key-loggers which stores all keypressings into a log file or a RAT RemoteAdministration Tools which can monitor all the activity carried out in the system remotely.

Session Hijacking: while using a weaker encrypted wireless networks or a open wireless connection may be easy to redirect users session to any path as intended by the hacker and can listen to all your communication of critical data such as passwords.

Some frauds in merchant outlets use card swipe machines which keep a copy of encrypted card data and if a 4 digit pin number is cracked it is done completely with hacking. Duplicate card can be created and linked account is completely taken control of.

Requirement of Internet Access, and the transmitted through money is being transmitted through different payment systems and you may be charged for that.

One more major issue for payments is that the payments agents are not governed by Governments. VISA, Maestro, Master card all are international players, through them once the amount is transacted cannot be reversed. Even if the policy changes can be done for reversing the payments, there are many hurdles and issues in this regard as it is required to prove that the payment is a fake. And if it is proved the payment is fake by then the culprit might not keep the balance in his account. A major effort of the Indian government in this regard is being Rupay card.

Public WiFi stations are nowadays becoming fashion for the users of internet where one can gain access to internet service without authentication. Access to any service without authentication means the communication is open access and the data communicated is weakly or not encrypted. Attempts to payments in such connections always expose a payer to lose his secret credentials.

Using a Rooted smart-phone for payments will again pose serious security issue, as the phone itself is not safe for keeping secrets.

5. THREE LEVEL SECURITY IMPLEMENTATION.

Online payment servers are not only secured for attacks but there are also systems for detecting possible breaches; Failure attempt to same account from different devices within a stipulated time period, Failure attempt to different accounts from same device, etc are identified as attempts for breaching security levels. And such devices or accounts are locked for certain cooling period. After knowing all the security issues to be online for transacting we may think twice to go for.By the same we cannot deny the valuable advantages that the online transactions are giving. People has found many solutions for not to lose money in online payments; some people use additional accounts with lesser balance and that is linked to debit card. Use of wallets provided by payment banks are also safer bets.

Now a day's some banks offering mobile banking apps in the touch of fingerprint. All these facilities are evolving as people of cashless world don't want to keep their usernames and passwords in memory. And also the usernames and passwords are not the ultimate security keys.

We can increase security using two or three fold authentications. But at each authentication levels the encryption algorithms take much time out of processor. And also traffic for authentication hence using proposed three level authentications requires a lot of time and computational resources.

Our plan is to classify the transactions in 3 categories,and imposing different levels of security over them along with the current security schemes.

Level 1	Accounts with less balance (below 10000)
Level 2	Accounts with moderate balance (Below 2 Lakhs)
Level 3	Accounts with heavy balance (more than 5 Lakh)

Level 1: Accounts with less balance may be imposed with a one fold Authentication: From a secured Desktop site with password protected. Or through a mobile app with a finger print sensor or with a simple 4 digit pin. These accounts may be generally used for utility payments or cashless transactions during retail shopping.

Level 2: Accounts with moderate balances may require extra authentication such as OTP, along with Username and password. Login may be with one fold authentication if the device IP is identified as regularly used one. Of course transaction of amount again may require additional authentication in the form of OTP, or a digital signature. If the device is different than regular use additional information about users personal detail and a CAPTCHA for proving himself as a human may be imposed.

Level 3: These heavy balance accounts need to login with two fold authentications such as username/Password combinations and a digital signature key, a CAPTCHA for proving himself as a human may be imposed. For transactions an OTP as a combination of SMS and e-mail are a must for transactions. Identified devices may omit entering CAPTCHA.

Problem again with these increased security levels is that, all these can be breached with just taking control of smart-phone, if the user is using the same phone for getting SMS OTP e-Mail OTP and banking transaction. There are many apps that are smart enough to read the SMS in the phone. And take snapshot of the user with the front camera of phone without the notice of the user. There is no surprise that an app can read e-mails in the inbox of the user to get OTP sent from the bank for authentication. The increased security in the level 3 transactions also mandates that the devices accessing the e-mail OTP, and SMS OTP and logging in device all three should be different, which will reduce the possibility of the security breaches.

The above mentioned security levels may be deployed on to the Net banking and payments through Wallets but Imposing Digital signature key and CAPTCHA for card payments through online may use the above security levels. Enforcing a digital signature key in the card swiping machines requires a massive up gradation of card swiping machines. But one thing can be changed is entering PIN in the swiping machines; which should be changed to OTP, which reduces the possibility of tracking PIN in the outlets.

6. CONCLUSION:

As long as we discuss security issues we can propose more and more stringent policies so that we may minimize the breaking of security schemes. As the technology makes hard rules for security so sophisticated the hackers are and they learn to breach the security levels. So this strengthening of payment systems will always need to upgrade and update with next technologies.

One problem raised as issue of online payment systems and not addressed is; Failure transaction. If a transaction is failed due to any technical issue, an automated recovery should be carried out to bring back the account to a consistent status. And also a manual service such as A USSD Service or a message service for customer to initiate a recovery into his account to bring back the account to consistency.

The communications between two devices are encrypted and this always ensures that the information can never be theft and accounts could not be compromised. But at two ends of the communication lies in two devices; user terminals and servers which can be exploited. In case of servers which are closely monitored and even a breach in security are detected. And also PCI DSS (Payment Card Industry Data Security Standard)are the standards laid for securing user data in Servers responsible for online payments.

Rest lies on the end users who are less educated and all the attacks are targeted towards him. Only a proper education and care taken by him almost saves him from the breach of security in his account.

A policy to blacklist IPs which are responsible for attempting a security breach is needed.

7. REFERENCES:

1. The study of e-commerce security issues and solutions-niranjanamurthy m, dr. Dharmendra chahar.
2. Improving the security of the internet banking system using three-level security implementation-emekareginaldnwogu.
3. The security of electronic banking-yi-jen yang.
4. Does the online card payment landscape unwittingly facilitate fraud?-ali ma, arief b, emms m, van moorsel a. *IEEE security & privacy* 2017.
5. Payment card industry security standards-standards guide.
6. http://www.makeuseof.com/tag/online-banking-secure-5-recent-breaches-will-worry/
7. security and privacy issues in e-banking: an empirical study of customers' perception- dr. tejinderpalsingh
8. Mobile Banking Security: Challenges, Solutions-Cognizant 20-20 insights.