Available online at http://acfa.apeejay.edu

APEEJAY JOURNAL OF COMPUTER SCIENCE AND APPLICATIONS

ISSN:0974-5742(P)
Vol. 2, January 2014

Susceptibility Analysis of Security Mechanisms Adopted by Indian Banking Sector

[1]Tejinder Pal Singh Brar, [2]Dr. Sawtantar Singh Khurmi, [3]Dr. Dhiraj Sharma
[1]University Institute of computing, Chandigarh University, Mohali,
[2]Bhai Maha Singh College of Engineering, Kotkapura Road, Muktsar,
[3]School of Management Studies, Punjabi University, Patiala

Abstract

Indian financial institutions have witnessed rapid growth in terms of their customer base. On the other hand corporate customers' of these institutions are increasingly worried about security threats while navigating the growing challenge of compliance risk. Financial institutions in India are relying on in-band two factor authentication methods in which user need to prove his identity more than one way. Even if in-band authentication is used as two-factor authentication, it is subject to a number of prevalent attacks. Number of authentication measures such as passwords and challenge questions are now considered weak security mechanisms. Many data breaches are linked to compromised usernames, passwords and OTP's. Infect, no single security solution is enough to defend against today's multifaceted exploits. There are so many different ways to get passwords like phishing, social engineering and keylogging etc. In this scenario, financial institutions need to strengthen their security structure so that enhanced secure environment can be provided.

Keywords: Phishing, Encryption, Authentication, OTP

1. Introduction

Threat landscape has been significantly changed because attackers have developed more complicated methods to compromise authentication mechanisms and gain unauthorized access to customers' information. Phishing attacks or malware can easily steal passwords, and attacker correctly answers the challenge questions on the basis of amount of information about customer that is available online. Challenge questions generally ask things like date of birth. These types of questions are easy to answer because large amount of information is available online about customer. When we talk about social networking websites, a large number of answers to challenge questions can be easily figured out from these online resources.

In the current online banking scenario, the last development that was found to be made by financial institutions is "in-band" two factor authentication in which user need to prove his identity more than one way. The general way that we think about this is depends upon two factors i.e. "something user knows" and "something user have". Customer is required to enter username and password as the first factor and then afterwards OTP is sent to customer's mobile phone through which customer conduct transactions. Beyond that, multifactor authentication can be applied in a lot of different banking contexts like while modifying the customer profile, administrative functions i.e. creating and managing user accounts, high-risk or high-value transactions, managing user transfer limits etc.

In-band authentication is vulnerable to prevalent attacks. OTP or one-time password/passcode can come from token, SMS or any other source. The problem is that customer types it into his web browser and certainly many of the worst attacks are mounted by malware that has infected customer's computer and is watching everything a customer types. As soon as customer types that OTP, the malware simply grabs that code and sends it to a criminal and who logs in pretending to be authorized customer. There's nothing that an in-band token-based approach can do if customer's computer is infected by malware.

Now a day's data breaches are happening all over the world on a regular basis. Many data breaches are linked to compromised usernames, passwords and OTP's. It raises a question: Why do not we make strong security controls and why we rely on simple user names and passwords? Infect, no single security solution is enough to defend against today's versatile attacks. Various attack tools have been developed and programmed into downloadable kits.

Rootkit-based malware secretly installed on a computer system that can monitor a customer's activities that aid theft and misuse of their login credentials. Such type of malware can break strong authentication techniques like multi-factor authentication. In recent years, commercial Internet banking transactions tend to be higher risk, due to higher account balances, commercial type transactions, and larger transaction amounts.

2. Review of literature

Detection of attacks still needs to be enhanced significantly not only in India but also across the globe. The online fraud/attacks that have been reported around the globe over the last 2 years are related to poor or simplistic authentication practices. In spite of innovation in security technologies, fraudsters still manage to breach banks' resistance from time to time. Consider these numbers: every month, around 18,000 phishing attacks take place around the world; 3% of Internet users from the EU27 group of countries lost money to online fraud last year; and there are at least 2,500 varieties of E-banking malware. Nearly 80% of U.S. banks think that malware on their customers' PC is a top security risk. Indeed this seems justified because U.S. consumers lost over US$ 2 billion and 1.3 million PCs to malware in 2010, Dinesh (2011). The top spot of weak authentication is taken by password which is the most prevalent and weak form of authentication because it is very easy to steal. According to Kitten (2014) the average annualized cost of cyber-crime for U.S. financial services institutions in 2013 was $23.6 million i.e. nearly 44 percent increase from 2012. Almost all of these major fraud cases in the last couple of years can be linked to authentication infrastructures.

Schwartz (2014) describes a security lapse related to credit and debit card transactions; he described how Atlanta-based world's largest express carrier and package delivery company UPS store suffered a point-of-sale malware attack that compromised numerous card transactions. About 105,000 credit card and debit card transactions were compromised in this data breach. On the same lines Karimi (2014) reports that Federal Trade Commission reports identity theft accounted for 18 percent of consumer complaints in 2012 alone and about 85 percent of identity theft incidents involved fraudulent use of credit card information. Finkle and Henry (2013) found that Target Corp (TGT.N) which is one of the biggest retailers in U.S. attacked by hackers in November 2013 which lasts for 19 days. This attack compromised up to 40 million credit cards and debit cards also managed to steal encrypted personal identification numbers (PINs) that makes it the second-largest data breach in U.S. retail history.

While analyzing Indian scenario of cyber attacks, Bipindra (2014) in his report highlight the incident when Defense Research and Development Organization's (DRDO) computers were hacked by Chinese hackers and carted away electronic files relating to Cabinet Committee on Security (CCS) which is the country's highest decision-making body on security affairs. This is not the first incident where China has been concerned in security attacks on the Indian government. According to article posted by Information Age (2012), hackers have breached information systems belonging to the Indian Navy, stealing sensitive data and sending it to computers with Chinese IP addresses. It was found that systems at India's Eastern Naval Command were found to be infected with malware in February 2012. The malware collected and transmitted confidential files and documents to Chinese IP addresses. Similarly a report from the University of Toronto in 2010 alleged that Chinese hackers had accessed Indian military systems. Kumar (2014), states that 3,000 internet connections of the Defense Ministry and the Air Force Communication Centre have been compromised and about three hundred thousand modems in Delhi are also vulnerable to Domain Name System (DNS) exploitation attacks, with servers based in foreign countries that can access sensitive information by means of phishing, traffic interception and diversion through a specific route.

While taking note on state-wise scenario, NCRB (2013) reported 4,356 cases were registered under IT Act during the year 2013 as compared to 2,876 cases during 2012, thus showing an increase of 51.5% in 2013 over 2012. Similarly, according to Gurung (2014) there is an increase in the cyber crime by 51%, the cases related to cyber crime that was filled in the year 2013 was 4356 and this year it is increased by 51 percent in comparison to previous year. The increase in the cyber crime has mainly linked three states that are connected to Information Technology (IT) i.e. Andhra Pradesh, Karnataka and Maharashtra. Table 1 shows incidences of registered cases in top 10 states of India during 2013 and their comparison with cases registered in 2012. In yet another kind of security related incident Tripathy (2014) reported that Chinese telecom company Huawei Technologies had hacked into telecom carrier Bharat Sanchar Nigam Ltd (BSNL). Similarly in 2012, a US panel urged American companies to stop doing business with Huawei and ZTE Corporation and warns that China could use firms' equipment to spy on certain communications and threaten vital systems through computerized links. A report from NCRB (2013) as shown in table 1 shows year wise comparison from 2010 to 2013 of various IT related crimes.

Table 1. Year wise comparison of different crime heads in India

S. no.	Crime heads	Cases Registered				% Variation in 2013 over 2012
		2010	2011	2012	2013	
1.	Hacking i) Damage/loss to computer resource ii) Hacking	346 164	826 157	1440 435	1966 550	36.5 26.4
2.	Failure of compliance of certifying authority	2	6	6	13	116.7
3.	To assist in decrypting the information intercepted by govt. agency	1	3	3	6	100.0
4.	Unauthorized access to protected computer system	3	5	3	27	800.0
5.	Publishing false digital signature certificate	2	3	1	4	300.0
6.	Breach of confidentiality/privacy	15	26	46	93	102.2
7.	Fraud of digital signature certificate	3	12	10	71	610.0

Source: NCRB (2013)

As we can observe from figure 1 that forgery cases in 2013 that have been registered are above 700 whereas criminal breach of trust is above 500. Figure 2 shows that in 2013 hacking cases come around 2500 that have been registered.

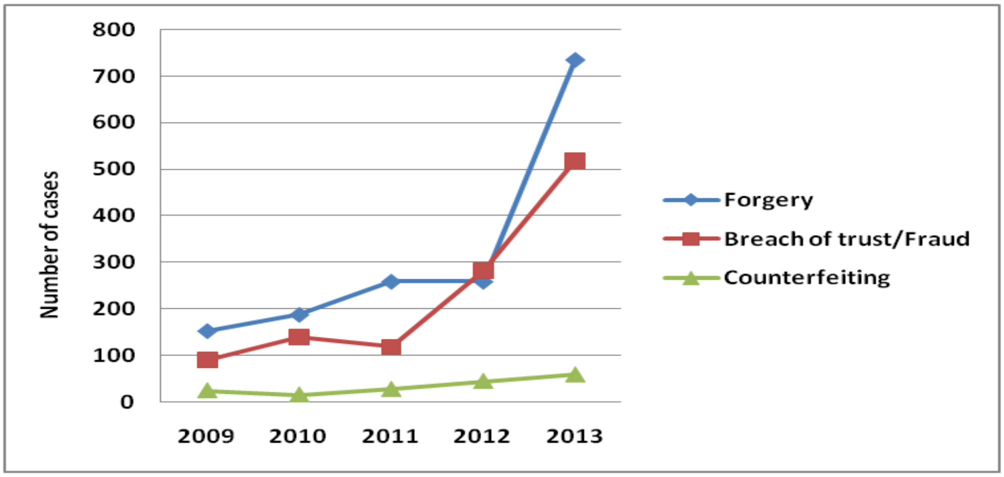

Figure 1. Cyber crimes case registered under IPC (**Source.** NCRB, 2013)

As described in figure 1 cases related to breach of trust/fraud and forgery cases has been highest in 2013. Total 735 forgery cases have been registered under Indian penal code in 2013 which is the highest as compared to last four years. While 518 cases related to breach of trust/fraud have been registered in 2013; it is also highest in last four years.

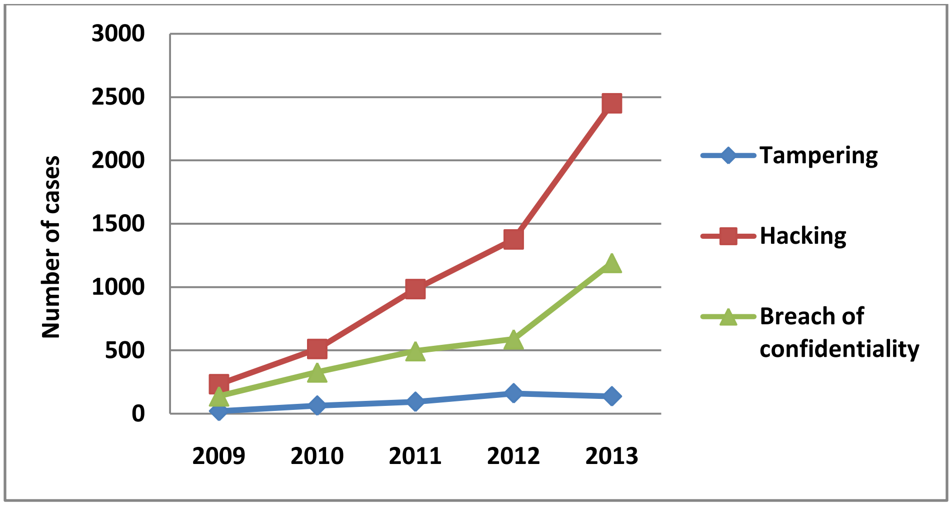

Figure 2. Cyber crimes case registered under IT act (Source. NCRB, 2013)

Figure 2 represents cases related to tampering, hacking and breach of confidentiality. 2450 hacking cases have been registered under IT act in 2013; it is highest figure while comparing with cases that has been recorded in the last four years. Breach of confidentiality related cases that have been registered in 2013 are 1192 which is also highest as compared to previous four years.

3. Authentication measures provided by Indian banks

In order to prevent online banking fraud, authentication of both customers and transactions is vital. Let's look at the current state of online banking authentication techniques used by various bank groups in India. At present, authentication of corporate customers' is performed by using combination of the methods (refer figure3).

SSL encryption (web) protocol is the de-facto Internet security standard. It provides authentication, confidentiality, integrity and no repudiation of messages transmitted over Internet between the customer's web browser and the bank web server. But it doesn't provide way to surety whether a user is a legitimate or not. SSL doesn't guarantee the safety and security of transaction over the Internet. However, user name/Id and password is the most popular and common method that requires users' to enter their credentials. As additional security, users may be required to ensure that their passwords are strong, change them routinely after a fixed number of days, or may be assigned a different one for transaction authorization.

On the other hand challenge questions are used use as a backup in the occurrence where primary logon authentication technique becomes inoperable. Challenge questions can be used to re-authenticate the customer or verify a specific transaction subsequent to the initial logon. User is presented with one or more simple questions from a list that was first presented to the customer when they originally enrolled with E-banking system. After positive verification of customer by verifying username /password and shared secret, OTP verifies users' identity that is based on something a user has. For example, customer might have a token (physical or virtual), he must enter a random number generated by the token to authenticate himself each time he conduct a transaction – like a payment. Alternatively, the bank might send a One Time Password (OTP) to the customers' registered mobile device each time they initiate that transaction. Customer need to send write the code on the specified field and send back to the bank through web link. Secured link between customer and bank branch is provided by 128-bit SSL encryption. Further factor-1 authentication is provided by user id/username password and shared secret / secret question. In factor-2 authentication, another layer of security is provided by OTP/Token that uses in-band authentication.

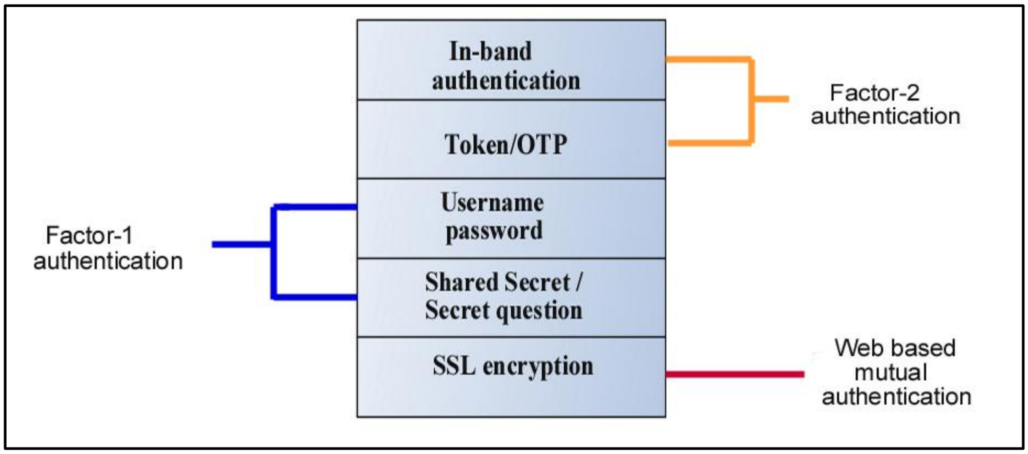

Figure 3. Different security layers in current E-banking environment (**Source.** Developed by researcher)

Following points describes funds transfer process in current E-banking environment
1. Customer access bank's homepage by writing its URL.
2. Homepage request received by web server and sends it further to customer portal.
3. Customer portal receive the request and reverts with login page. Now login page is displayed to customer.
4. Customer provides his username and password and shared secret (factor-1 authentication), web server after receiving the verification request, sends it the authentication server. Authentication server sends this request to the secure directory where credentials of customers are stored.
5. Secure directory retrieves the customer details and sends it to the authentication server.
6. Authentication server verifies the credentials
7. If credentials are correct then authentication server sends the control to the customer's internet banking profile homepage. If credentials are wrong then authentication server sends the message to customer regarding wrong username or password.
8. Internet banking menu is displayed on homepage.
9. Number of options is displayed on customer homepage.
10. Customer selects the funds transfer option along with destination account number and amount to be transferred.
11. Funds transfer option is received by web server and web server in turn forward request through authentication server and integration layer to core banking system.
12. CBS (Core banking system) generates OTP that is send to customer mobile phone via web server.
13. Customer responds with OTP through web link on the customer portal (factor-2 authentication).
14. OTP authentication is done by authentication server which redirects the control (if OTP correct) to CBS.
15. Transfer of funds is complete and confirmation message is sent to web server.
16. Web server forwards the funds transfer successful message to customer.

4. Conclusion

From the funds transfer and view account details processes we can observe that in funds transfer process uses two-factor authentication mechanism but in case of view account details process only single factor of authentication is utilized. In principle, any activity that carries with it risk on customer's system is a candidate for strong authentication. The interesting concept emerging from this current E-banking scenario is the need for layered security. Strong authentication is required at three different levels of conducting transaction via electronic means. First of all, strong authentication is critical at customer login. Secondly, protecting actual transactions is critical, and it is vital to include transaction details to protect against malware that modifies transactions. And third, it's important to start looking into other account related activities like view account details, bill payment or creating and managing administrative users in the corporate firm. Banks need to realign their authentication infrastructures to include a mix of multi factor authentication measures. It is important to not only to evaluate online banking applications and identify existing vulnerabilities but also there is a need to evaluate layered security approaches and the areas where these additional layers of authentication should be added. For online, as well as other financial transactions strong authentication measures should be built into the multifactor approach. A new or additional layer of authentication is required not only authenticating corporate customers' while log-in process, but also other related activities when customer logged on. The concept of layered security is critical from corporate customers' view point because the rate and amount of these business transactions are usually higher than that of retail consumer transactions. For this purpose banks should implement layered security. Additionally, banks need to offer multifactor authentication to their business customers.

5. Recommendations

Financial institutions in India show upward trend in terms of adoption and usage of electronic banking by corporate sector. But due to fear of financial loss customers' are losing their trust on E-banking security mechanisms. However, banks are trying their best to provide secure environment in which customers' can transact with confidence. Security measures that are currently adopted by Indian banks uses two factor authentication measures. As the study evaluates, due to ongoing cyber attacks and vulnerabilities in current security measures, there is a need to further strengthen the level of security. Following are the recommendations for both corporate customers' as well as for financial institutions.

TABLE 2. CATEGORY OF ACTIONS AND RECOMMENDATIONS

Category	Action to be taken	Recommendations
1	Assessing existing authentication infrastructures	From bankers' perspective, they first of all need to assess their existing authentication infrastructures and then need to evaluate their strategy for multifactor authentication.
2	Additional layers of user authentication in the case of high value or exceptional transactions	Financial institutions need to adopt other measures such as limiting the number of online banking operations that a customer can perform each day or applying additional layers of user authentication in the case of high value or exceptional transactions.
3	Should not rely on one form authentication measure	It is strongly recommend that banks should not rely on one form of customer authentication because one dimensional customer authentication is not robust to provide the level of security that customers expect and that protects banks from financial and reputation risk.
4	Periodic risk assessment for banks	Banks should perform periodic risk assessments prior to implementing new electronic financial services or at least every twelve months and adjust their authentication controls for corporate customers' in reply to new threats to their online accounts..
5	Periodic risk assessment for customers	Corporate customers' should also periodically assess their risks and controls regarding online banking access and user authority like monitoring accounts frequently and reviewing electronic transfers; securing all IDs and passwords and educating employees.
6	Additional verification	Even after providing layered security to customer's account, still in case if online banking access has been locked or a suspicious transaction has been identified then additional verification may be performed. In these cases "enhanced device identification" method can be used to strengthen the identity confirming process.
7	Day-to-day situational awareness	Banking institutions need to develop "day-to-day situational awareness" of the latest threats. Situational awareness requires understanding threats and risks in real time to help minimize the impact.

(Source. Developed by researcher)

References:

[1] Bipindra, N. C. (2013). *Chinese 'hack' DRDO computers. Retrieved online at* http://www.newindianexpress.com/nation/article1500336.ece, July 2014.

[2] Gupta Deepak, Kewal Krishan Nailwal, and Sameer Sharma. "Minimizing Hiring Cost For Three Stage Flowshop Scheduling For A Fixed Sequence Of Jobs.", Apeejay Journal of Computer Science and Applications", Vol. 1, 2013, pp. 33-38.

[3] Dinesh, T. C.(2011). *What the future of online banking authentication could be.* Retrieved from www.infosys.com/finacle, July 2014.

[4] Finkle, J. And Henry D. (2013). *Target hackers stole encrypted bank PINs.* Retrieved online at http://www.reuters.com/article/2013/12/24/us-target-databreach-idUSBRE9BN0L220131224, August 2014.

[5] Gurung, V. (2014). *Latest Cyber Crime Reports of India*. Retrieved online at http://www.cyberkendra.com/2014/07/latest-cyber-crime-reports-of india.html#.U_aF_8WSySo, July 2014.

[6] Information age (2012).Chinese hackers' access Indian navy systems. Retrieved online at http://www.information-age.com/technology/security/2110843/%22chinese%22-hackers-access-indian-navy-systems, June 2014.

[7] Karimi, S. (2014). *6 Things You Must Do After Hackers Steal Your Credit Card Data.* Retrieved online at http://money.usnews.com/money/blogs/my-money/2014/02/19/6-things-you-must-do-after-hackers-steal-your-credit-card-data, August 2014.

[8] Kitten (2014). *How to Improve Threat Detection.* Retrieved from http://www.bankinfosecurity.com/interviews/banks-how-to-improve-threat-detection-i-2328, August 2014.

[9] Kumar, V. (2014). *Cyber snoops hack India's secrets: Report reveals how internet spies may have 'compromised' the nation's securit*y. Retrieved online at http://www.dailymail.co.uk/indiahome/indianews/article-2586442/Cyber-snoops-hack-Indias-secrets-Report-reveals-internet-spies-compromised-nations-security.html#ixzz3B5sPlTfV, June 2014.

[10] NCRB (2013). Cyber crimes. Retrieved from http://ncrb.gov.in/CD-CII2013/Home.asp, May 2014.

[11] Schwartz, M.J. (2014). *UPS Reveals Data Breach.* Retrieved online at www.bankinfosecurity.com/ups-reveals-data-breach-a-7217, August 2014.

[12] Tripathy, D. (2014). India-probes-media-report-of-Huawei-hacking-BSNL. Retrieved online at http://www.livemint.com/Industry/rAWayE115erqLzGZOXxVDO/India-probes-media-report-of-Huawei-hacking-BSNL.html, July 2014