# A Review of Security System in E-Banking

**Ms. Rachana C. R.**

E-channels today are providing outstanding efficiency for both banks and their customers. In order to build on this efficiency, it becomes obvious that trust, availability and usability of e-channels must definitely be safeguarded. Today, a number of technical and organizational security measures are required to protect the authenticity, integrity and confidentiality of each and every e-banking transaction.

E-banking has become increasingly prevalent, employed by many financial institutions to reduce costs associated with having personnel serve customers physically. This has resulted in increased speed, improved flexibility of business transactions, better service and shortened processing periods for customers.

With all the existing security systems, internet fraud is still on the rise and fraud schemes have become even more sophisticated. Fraudsters use various techniques to gain information from customers who transact using the e-banking facilities. Few requests might draw customers to be part of a survey or inform them that their session has expired and they need to validate/ update/reveal their account to revive it. This could happen when software of files is downloaded from an unknown source or through threats which claim that their online session will be shutdown if reconfirmation of account details is not carried out. In order to minimize the opportunities for fraud, the e-banking services offering institutions need to control authorization and access privileges. They should have appropriate authorization controls and access privileges while ensuring effective aggregation of duties for their e-banking services and their respective supportive processes as well as the underlying infrastructures. Phishing attacks, Trojan horses, Key loggers, Pharming, Malware software's have resulted in banks looking for more sophisticated security solutions to protect their customers online.

The 3 major building blocks of security mechanisms namely encryption, Digital signatures and checksums/ hash algorithms must be imbibed in any e-banking application/service to make E-banking transactions more secure.

**Types of Internet Banking**

There are three types of internet banking employed in the marketplace:

**1. Informational**- This system presents the lowest risk. Typically, the bank has information about product descriptions, exchange rates and contact details on a stand-alone server. These informational systems typically have no path between the server and the bank§ internal network. This level of Internet banking can be provided by the bank or outsourced. While the risk to the bank is relatively low, the server or Web site may be vulnerable to alteration. Appropriate controls must be in place to prevent unauthorized alterations to the bank§ server or Web site.

**2. Communicative-** This allows some interaction between the bank§ systems and the customer. The interaction may be limited to statements, account balances, e-mail, loan applications, or static file updates (name, address, nominee changes). Compared to informational systems, with this configuration, the system has higher risks as these servers may have a path to the bank§ internal networks. Appropriate controls must be in place to prevent and alert the management of any unauthorized attempt to access the bank§ internal networks and computer systems. Virus controls also become much more critical in this environment.

Mrs. Rachana C R, Assistant Professor. Department of Studies in Computer Science, Pooja Bhagavat Memorial Mahajana Post-Graduate Centre,Mysore

**3. Transactional** – This system allows customers to execute transactions. In this set-up, a path typically exists between the server and the bank's or outsourcer's internal network; hence, this is the highest risk architecture and must have the strongest controls. Transactions include accessing accounts, paying bills, transferring funds, etc. It further includes remote subscription of known customers to new services provided by financial institutions.

**Security Attacks**

Attacks or intrusion attempts on banks 'computer and network systems are a major concern. Studies show that systems are more vulnerable to internal attacks than external, because internal system users have knowledge of the system and access. Banks should have sound preventive and detection controls to protect their Internet e-banking systems from exploitation both internally and externally.

Security issues are a major source of concern for everyone both inside and outside the banking industry. E-banking increases security risks, potentially exposing hitherto isolated systems to open and risky environments.

Security breaches essentially fall into three categories; breaches with serious criminal intent (e.g. fraud, theft of commercially sensitive or financial information), breaches by 'casual hackers' (e.g. defacement of web sites or 'denial of service' - causing web sites to crash), and flaws in systems design and/or set up leading to security breaches (e.g. genuine users seeing / being able to transact on other users' accounts). All of these threats have potentially serious financial, legal and reputational implications.

Many banks are finding that their systems are being probed for weaknesses hundreds of times a day but damage/losses arising from security breaches have so far tended to be minor. However some banks could develop more sensitive "burglar alarms", so that they are better aware of the nature and frequency of unsuccessful attempts to break into their system.

The most sensitive computer systems, such as those used for high value payments or those storing highly confidential information, tend to be the most comprehensively secured. One could therefore imply that the greater the potential loss to a bank the less likely it is to occur, and in general this is the case. However, while banks tend to have reasonable perimeter security, there is sometimes insufficient segregation between internal systems and poor internal security. It may be that someone could breach the lighter security around a low value system, e.g. a bank's retail web site, and gain entry to a high value system via the bank's internal network. We are encouraging banks to look at the firewalls between their different systems to ensure adequate damage limitation should an external breach occur. As ever though, the greatest threat so far has been from the enemy within – i.e. employees, contractors and so on.

It is easy to overemphasize the security risks in e-banking. It must be remembered that the Internet could remove some errors introduced by manual processing (by increasing the degree of straight through processing from the customer through banks' systems). This reduces risks to the integrity of transaction data (although the risk of customer's incorrectly inputting data remains). As e-banking advances, focusing general attention on security risks, there could be large security gains.

There are several types of Attacks which specifically target E-banking operations.

Few of them are:

**a. Guessing Passwords**

This software specifically designed to guess passwords tests all possible combinations to gain entry into a network.

**b. Brute Force**

This technique captures encrypted messages and uses a software to break the code and gain access to

messages, user ID ś, and passwords.

**c. Random Dialing**

Here, the attacker tries to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could then be used as a point of attack.

**d. Social Engineering**

An attacker calls the bank ś help desk impersonating an authorized user to gain information about the system including changing passwords.

**e. Trojan Horse**

A programmer can embed code into a system that will allow the programmer himself or another person gain unauthorized entrance into the system or network.

**f. Pharming**

This attack takes place without any conscious action on your part. This involves the installation of malicious code on your computer. In one of its kind, you must open an email, or email attachment; you visit a fake website and without your knowledge, you provide information that compromises your financial identity.

**g. Phishing attacks**

These attacks use fake email messages from an agency or individual pretending to represent your bank or financial institution. The email asks you for your personal/sensitive information like name, password, and account number etc., and provides links to a counterfeit website. If in case you follow the link & provide the requested information, intruders can access your personal account information & finances.

**h. Spear Phishing**

It is very common among corporate e-banking customers. E-mails are sent to employees working in finance and executing high value transactions, who based on the e-mail, can ask the bank to initiate a transfer of funds.

**i. Malware**

It directs to the term for maliciously crafted software code. It is specifically a factor in online financial crime attacks may perform many operations.

**i. Sniffers** (Network monitors) :

Account Information Theft malware is capable of capturing the keystrokes for your login information and can also monitor and capture other data you use to authenticate your identity.

**ii. Fake website substitution:**

Malware software in this case is capable of replacing your bank's legitimate website with a page that can look identical, except that the web address will vary in some way. This is a typical example for the "man-in that middle attack" in terms of network security attacks. When you submit information on the webpage it is sent both the bank and the malicious attacks without your knowledge.

**iii. Account hijacking:**

Without your knowledge, malware can hijack your browser and transfer funds. Basically involves intercepting transmissions, then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat. When you attempt to login at a bank website, the software launches a hidden browser window on your computer, logs into your bank website, reads your current account balance & creates a secret fund transfer to the intruder-owned account.

The following are the approaches financial institutions need to have:

▲ A strategic approach to information security, building best practice security controls into systems and networks as they are developed

▲ A proactive approach to information security, involving active testing of system security controls (e.g. penetration testing), rapid response to new threats and vulnerabilities and regular review of market place developments

▲ Sufficient staff with information security expertise

▲ Active use of system based security management and monitoring tools

▲ Strong business information security controls

**E-Banking Adoptability Factors**

Most banks today offer outstanding online banking systems. These user friendly services save time for both the banking staff and customer. These services help customers check their balance, schedule transfers, pay bills, and even store away important digital documents on the bank's secure server. For people who access the internet via their cell phones, this is especially true. It is more convenient and easy to check the balance on their account before a purchase when they have the option of internet banking. Otherwise, they would find themselves having to check their balance via an ATM or making a call to the bank for the information.

The following figure (1) shows the key factors that are affecting the decision making of a consumer for initiating the use of Internet Banking facilities.

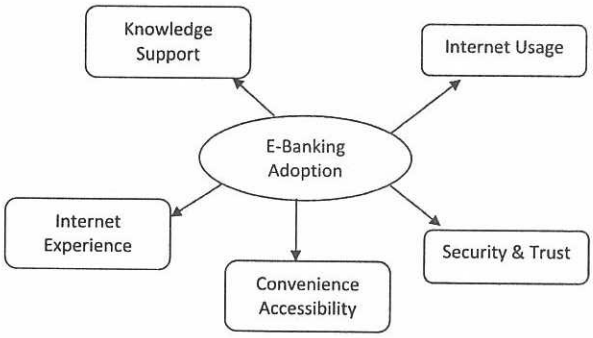


Figure 1: Key factors influencing E-Banking Consumer Adoption

➢ **Internet Usage**: For any customer, it is important to consider the factors that influence him/her to opt for Internet banking. Basic understanding of the use of the Internet is a must for any Internet banking customer.

➢ **Internet Experience**: A Person should never feel that he must have gone to the bank to get his work done instead of visiting the website of the bank. The experience he obtains from the e-banking website must be rich productive.

➢ **Convenience of Accessibility:** The account holder must find it convenient to avail the benefits of the e-banking facility. He must feel comfortable getting the necessary services from the bank website.

➢ **Knowledge & Support**: The bank must be willing to attract its customers to use the bank's website. For this, the bank must be able to provide the necessary assistance to all those who visit the E-banking website. The necessary support should be extended to all those who are its customers. There should be options for obtaining extra information about a facility offered to its customers by the bank.

➢ **Security and Trust**: The most important building block of any transaction is security & trust. The electronic banking facility must take appropriate steps to ensure the security of any transaction.

The following **figure (2)** depicts the search volume index of online banks and banking against news reference volumes.

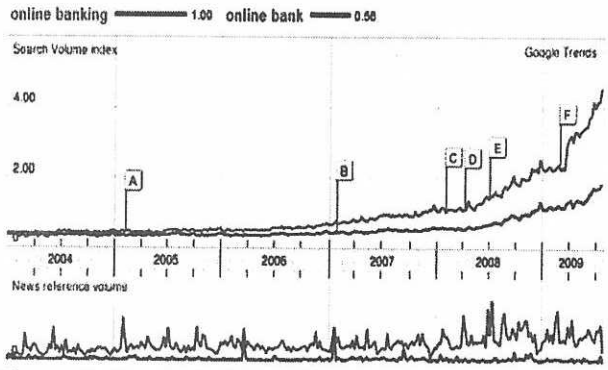


Figure 2: Graph depicting the search volume index of online banks and banking against news reference volumes.

The following report shows the improved feedback from customers who use E-banking facilities for their daily transactions. In 2010, 70 percent of survey respondents reported being satisfied with their primary bank, a marginal decrease versus last year.

| Satisfaction with Primary Financial Institution<br>March 23 – April 9, 2010, n = 2,576<br>Source: comScore Banking Survey | | | |
|---|---|---|---|
| | Percent of Respondents who are "Highly Satisfied" | | |
| **Financial Institution** | **2008** | **2009** | **2010** |
| ***Bank*** | ***72%*** | ***71%*** | ***70%*** |
| Brokerage Firm | 70% | 58% | 64% |
| Credit Card Company | 65% | 62% | 60% |

**Figure 3: Improvement in Customer Satisfaction for Online Brokerages**

**Security Nets**

Banks should ensure that there are appropriate measures to protect the data integrity of e-banking transactions, records and information. All e-banking transactions should generate clear audit trails, which should be archived. It is also vital to generate and protect records of customer instructions in a legally acceptable format.

Banks should strengthen information security controls to preserve the confidentiality and integrity of customer data. Firewalls, ethical hacking tests, physical and logical access controls are some of the methods available.

The following security levels can be implemented on the basis of the communication model.

- Server side security
- User authentication
- Firewalls
- Protection of Documents
- Transmission Security
- Encryption
- Secure Email
- Secure HTTP
- Secure Electronic Transaction
- Client side Security
- Trojan Horses
- External Viewers
- Privacy

According to the latest figures from the UK Card's Association, Online banking fraud losses increased by 14 percent to £59.7 million last year. This represents an increase of £7.2 million in online banking fraud losses compared with 2008 (£52.5 million).

Protecting the customers through single password authentication is not secure enough for personal online banking applications since internet frauds have drastically raised. Hackers gaining access to vulnerable home PCs and intercepting the password shows that encryption alone does not prove to be the most apt security measure.

The use of Transaction number (TANs) is a second layer of security imposed by many online banking services. TANs are essentially single use passwords. Only valid for a limited period; the password is unique & cannot be reused one time passwords are the latest tool used by banking service providers. With OTPs customers need not memorize their passwords. Whenever a consumer wants to perform transactions using the online banking interface, the request is received and the password is sent to the customer's phone via SMS. This password expires once it has been used. With this, the bank is able to identify the user when he request access to the e-banking application.

Two factor authentication customers are provided with security token devices capable of generating single use passwords unique to the customer's token.

The use of digital certificates avoids certain authentication risks. The transactions are digitally signed or authenticated by linking to a physical device (eg. Computer, Cell Phone etc.)

Biometric devices are an advanced form of authentication for secure e-banking. These devices may make use of a retina scan, finger or thumb print scan, facial scan, or voice print scan. Use of biometrics is not yet considered mainstream, but may be used by some banks for authentication. It becomes important

to evaluate biometric activities based on management's understanding of risks, internal or external reviews, and the overall performance of these devices.

Few important checkpoints which the customers should follow for secure E-banking are:

· The bank's information about its online privacy policies and practices must be reviewed thoroughly.

· Before setting up any online bill payment, the privacy policy of the company or service you will be sending payment to must be checked.

· Choose an online personal identification number (PIN) that is unique & hard to guess.

· Anti-virus, firewall and antispyware programs installed on your computer must be kept up to date.

· Check your online account balance for unauthorized activity every now and then.

**Conclusion**

Online banking continues to present challenges for financial security and personal privacy. Online banking involves certain risks. It is important to educate everyone about these risks, how unauthorized access to financial information occurs, and the steps that can be taken to protect financial information.

Many in the banking industry expect significant growth in the use of the Internet for the purchase of goods and services and electronic data interchange. The banking industry also recognizes that the Internet must be secure to achieve a high level of confidence with both consumers and businesses.

Sound management of banking products and services, especially those provided over the Internet, is fundamental to maintaining a high level of public confidence not only in the individual bank and its brand name but also in the banking system as a whole.

In order to enhance the customer experience, banks should conduct usability tests and monitor user feedback; provide smooth navigation aids; incorporate easy-to-access contextual help; and minimize data entry problems with appropriate user interface elements, such as calendar widgets.

For several of these enhancements, the back office has to get involved. Specifically, banks are seeking to maintain a consistent look and feel across applications used by multiple lines of business; incorporate third-party offerings into the Internet banking channel; and create links between online applications. The optimal development strategy for e-banks is likely to be the cultivation of the demand side along the paths of least resistance, in particular in regard to consumer perceptions of transaction security, transaction accuracy, user friendliness, and network speed.

Young, male and highly educated individuals are typically first to adopt new technologies. The profile of the average online banker is still biased towards the characteristics of the early core group of mostly young, male and well-educated individuals.

***References***

*1. Internet Banking Comptroller's Handbook, October 1999.*

*2. Liao, Z. and Cheung, M.T. Internet-based e-banking and consumer attitudes: An empirical study. Information and Management 39. 4 (2002), 283–295.*

*3. Banking Securely Online, Produced 2006 by US-CERT, a government organization. Updated 2008.*

***4.aaron.taylor in Business, The Future of Online Banking, http://bizcovering.com/business/the-future-of-online-banking/***

***5.Anh Nguyen and Computerworlduk, Computerworld, UK, Online banking fraud losses rise to nearly £60 million.***

*a. http://www.networkworld.com/news/2010/031110-online-banking-fraud-losses-rise.html*

*6. Customer Experience Takes Center Stage in Online Banking, comScore Releases 2010 U.S. State of Online Banking Report.*

*a. http://www.comscore.com/Press_Events/Press_Releases/2010/5/comScore_Releases_2010_U.S._State_of_Online_Banking_Report.*

***7.E banking: risks and responses, Speech by Carol Sergeant, Director, Banks & Buildings Societies Financial Services Authority.***

***8.Online Banking: The Young and Well Educated extend their lead until 2010, Deutsche Bank Research, MAY 2008.***