Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2011, vol. 16, no.2 (http://www.arraydev.com/commerce/jibc/)

E-Banking Security Issues – Is There A Solution in Biometrics?

Amtul Fatima
Scholar, Jawaharlal University of Technological studies, A.P., India
Postal Address: **Tallakunta, Chandrayangutta x-road, Hyderabad -500 005,A.P., India**
Email: ***brackishsea@gmail.com***

ABSTRACT

The providers of Internet banking services must be more responsive towards security requirements. While there is no doubt that Internet banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings. Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. Using biometrics for identification restrict individuals from access to physical spaces and electronic services An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans. In this study, the security threats in Internet banking, its solutions in biometrics and its acceptance in the consumer market are studied using descriptive and exploratory research. The methods of descriptive research are used to obtain information concerning the major security issues in e-Banking. The research had been completed on the basis of secondary data (online databases, scientific journals, surveys, news).

Keywords: Biometrics, e-banking, electronic banking, e-security, secure transactions, security threats, Identity thefts

INTRODUCTION

Banking organisations have been delivering services to consumers and businesses remotely for years. Electronic funds transfer, including small payments and corporate cash management systems, as well as publicly accessible machines for currency withdrawal and retail account management are global fixtures. However, delivering financial services over public networks such as the Internet is bringing about a fundamental shift in the financial services industry.[1] According to Heikki et al. (2002), the transformation from the traditional banking towards e-banking has been a 'leap' change. The increase in information access terminals along with the growing use of information sensitive applications such as e-commerce, e-learning, e-banking and e-healthcare have generated a real requirement of reliable, easy to use, and generally acceptable control methods for confidential and vital information. On the other hand, the necessity for privacy must be balanced with security requirements for the advantage of the general public. Payment systems are undergoing radical changes stirred largely by technical advancement such as distributed network technology, real-time processing and online consumers' inclination to use e-banking interfaces making the study of biometrics even more important in this new E-World.[2] Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services.[3] An accurate automatic personal identification is critical to a wide range of application domains. Traditional personal identification methods (e.g., passwords, PIN) suffer from a number of drawbacks and are unable to satisfy the security requirement of our highly inter-connected information society. Biometrics refers to automatic identification of an individual based on her physiological or behavioral traits. While biometrics is not an identification panacea, it is beginning to provide very powerful tools for the problems requiring positive identification.[4]

e-BANKING – THE PRESENT SCENARIO:

In August of 1995, Citibank had problems with outsiders breaking into their system. A $10 million computer fraud against Citibank was the first successful penetration by a hacker into the system which transferred trillions of dollars a day around the world. Of the $10 million dollars illegally transferred, $400,000 were not found.[5]

In August 2000, British police have arrested three men in connection with an attempt to defraud the Internet bank Egg. The bank was reportedly the target of an effort to obtain money via fraudulent accounts but no money was stolen and Egg stressed that none of its computer systems had been breached. According to the BBC, fraudsters had attempted to obtain thousands of pounds (GBP) via multiple savings accounts and loans. The three men are allegedly part of an organised crime syndicate. [7]

In April 2010, a fire alarm company in Arkansas lost more than $110,000 this month when hackers stole the firm's online banking credentials and drained its payroll account. Over the course of the previous few days, someone had approved two batches of payroll payments — one for $45,000 and another for $67,000. A few days later, Melanie Eakel, chief executive of JE Systems Inc. , was informed by the bank that it was the [Internet] address that was used to process the payments, and the online banking user name and password.[6]

In such a situation, information security is essential to a financial institution's ability to deliver e-banking services, protect the confidentiality and integrity of customer information, and ensure that accountability exists for changes to the information and the processing and communications systems. A major challenge for e-Banking that requires innovative approaches stems from the need to annihilate the effects of rapidly growing cyber-crime. Recent statistics show that the internet usage has gone up dramatically since last decade with Asia's penetration itself being 21.5% and 37.9% population of penetration for the rest of the world [8]. Further statistics report that 35.9% of financial sector is the target of Phishing frauds [9]. According to Javelin 2010 identity theft report, the number of identity theft victims and the amount of fraud increased by 12 and 12.5% respectively, the highest rate ever issued by the company.

Organizations such as banks with dedicated Internet connections face greater risk of someone from the Internet gaining unauthorized access to their computer or network than those who use dial-up modem. However, the electronic banking system users still face the security risks with unauthorized access into their banking accounts. Therefore, it is extremely important to build in non-repudiability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.[5]

LEGAL AUTHORITIES REGULATING E-BANKING:

Most legal regulations regarding the protection of consumer interests by ensuring the security of e-Banking platforms are considering:

- Ensuring the security and confidentiality of customer information;
- Protection against any anticipated threats or hazards to the security or integrity of such information;
- Protection against unauthorized access to or use of such information that could result in substantial harms or inconvenience to any customer.

Different formal set of laws that regulate e-commerce and e-banking are enacted in different countries with the common aim of protecting cyber crimes. Few of them are Electronic Commerce Act (Ireland), Electronic Transactions Act (UK, USA, Australia, New Zealand, Singapore), Electronic Transactions Ordinance (Hong Kong, Pakistan), Information Technology Act (India), Information Communication Technology Act Draft (Bangladesh) [11]. In Romania, specific legislation has been created by the development of Law no. 455/2001 on Electronic Signatures, Regulations of National Bank of Romania no. 4 / 2002 concerning transactions by electronic payment instruments and the relationship between participants in these transactions and the Law no. 365/2002 on electronic commerce[10]. The Reserve Bank of India, like peers in Malaysia, Indonesia, the Philippines, and other countries around the world, has created rules for e-money issued by nonbanks to address a previous regulatory vacuum [12]. The Information Technology Bill, 1999 and Electronic Commerce Bill, 1999 in India are intended to be general purpose legislation covering mainly issues like secure electronic records and signatures, acceptance of digital signatures, duties of certification authority, liability of network service providers, computer crime and data protection. Both the bills deal with electronic contracts and they are being promoted by the Government of India primarily to facilitate introduction of Electronic Data Interchange in the commercial sector [13]. A brief examination of data privacy and bank secrecy regulations in developing countries reveals a patchwork of rules issued by a variety of agencies with overlapping jurisdiction and oversight (Lyman, Pickens, and Porteous 2008). As an example of differences among countries, bank secrecy rules do not explicitly apply to agents in India, whereas they do in Brazil, Peru, Colombia, and Mexico. (In India, however, providers are liable for the acts of omission and commission of their agents in all respects, including bank secrecy.) While Peru and India have data privacy regulation, Brazil has none. [12] In India, Enactment of the IT Act 2000 and IT (Amendment) Act 2008, Anti Money Laundering Act 2002, establishment of Adjudication Officers and Cyber Appellate Tribunal, Financial Intelligence unit – India, have facilitated in providing requisite legal framework to carry out the transaction in the internet media. In a nutshell the Act has provided the requisite legal recognition to the electronic records for the purpose of conducting e-commerce activities. Several offenses concerned with cyber media have been identified and requisite penalties in the form of imprisonment and/or with fine have been formulated to curb the cyber crime. The IT Act 2000, u/s 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. The IT (Amendment) Act 2008 has made a mention of electronic authentication technique, the details of which however are not mentioned in the Schedule II of the Act. The digital signature technology identified in the Act needs to be compatible with the technology adopted by the banks.

Reserve Bank of India vide its guidelines dated June 14, 2001, has made it mandatory for the banks to adopt digital signature as authentication tool/technique for the purpose of authentication and non-repudiation.

SECURITY THREATS IN E-BANKING:

Since Electronic Banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The number of malicious applications targeting online banking transactions has increased dramatically in recent years.

The disclosure of important information that should remain confidential, by unauthorized persons or that exceed their authority can cause significant losses for financial institutions. Alteration of information by entering, modifying or overwriting data into the system without authorization or by exceeding one's authority is a type of attack that could potentially harm greatly the banks and their customers.[10]

A common mistake made by end users is believing that their online banking session is perfectly safe when they use an SSL connection. Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window. But SSL is designed as a secure tunnel from the end user computer to the bank mainframe and does not protect the end points such as the end user's computer. [14] The attacker installs a Trojan, such as key logger program, on a user's computer. This happens when users visited certain websites and downloaded programs. As they are doing this, key logger program is also installed on their computer without their knowledge. When users log into their bank's website, the information keyed in during that session will be captured and sent to the attacker [15]. Minor disruptions on the part of third party service providers can expose banking organisations to potential financial loss and substantial legal and reputation risk. Complexity is also added by multiple vendor/service provider relationships that often support e-banking operations. Major security breaches in a bank or a non-bank competitor's web site could undermine overall consumer or market confidence in banks' ability to appropriately manage Internet-based transactions. [1]

Man-In-The-Middle attack is the type of attack where attackers intrude into an existing connection to intercept the exchanged data and inject false information. It involves eavesdropping on a connection, intruding into a connection, intercepting messages, and selectively modifying data. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. Pharming is a type of fraud that involves diverting the client Internet connection to a counterfeit website, so that even when he enters the correct address into his browser, he ends up on the forged site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. In recent years both pharming and phishing have been used for online identity theft information. The most prevalent threats include viruses, Worms, Trojan Horses, drive-by downloads, spoofing-attacks.[10] As was first reported early in March on Internet Banking Wire, for instance, a "server worm" known as the SQLSlammer Worm attacked Microsoft's SQL Server 2000 and Desktop Engine 2000 software, slowing online traffic and even temporarily cutting off cash at some ATMs at Bank of America and Canadian Imperial Bank of Commerce.

The worm caused so much congestion on the bank's internal network that "when an ATM went to communicate or dispense cash," it was unable to do so, explained a Bank of America spokesperson. Security vendor Symantec, Cupertino, Calif., tracks activity on the internet as part of its offerings and issues a Security Response Report regularly. They noted that in recent months "Klez," "Bugbear," and "OPA serve" constituted 80% of the malicious code gathered from monitoring systems deployed at client locations. [16] An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution’s Internet-based products and services. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution’s overall strategy for Internet banking and electronic commerce customer services. The level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application. [3]

Security threats can affect a financial institution through numerous vulnerabilities. No single control or security device can adequately protect a system connected to a public network. Many problems concerning the security of transactions are the result of unprotected data being sent between clients and servers. E-Banking platforms offer several methods to ensure a high level of security: (a) identification and authentication, (b) encryption, and (3) firewalls mechanism. The identification of an online bank takes the form of a known Internet address or Uniform Resource Locator (URL), while the customer is identified by his login ID and password to ensure only authorized users can access their accounts. On the other hand, messages between customers and online banks are all encrypted so that another person cannot view the contents of messages. The common encryption standard adopted by most browsers is called Secure Socket Layer (SSL). Firewall is a set of devices configured to permit, deny, encrypt or decrypt all computer traffic between different security domains based upon a set of rules. A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification can ensure that customer account information is protected from unauthorized access. [10] At minimum, a two-factor authentication should be implemented in order to verify the authenticity of the information pertaining to Internet banking services. The first authentication factor can be the use of passwords and the second authentication factor can be the use of tokens such as a smartcard. However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric. This ascertains who one is, biologically.[15]

BIOMETRICS IN E-BANKING:

Electronic commerce and electronic banking are two of the most important and emerging application areas of biometrics due to the rapid progress in electronic transactions. Currently, there are several large biometric security projects in these areas under development, including credit card security (MasterCard) and smart card security (IBM and American Express). Information system/computer network security such as user authentication and access to databases via remote login is another important potential application area for biometrics.[4]

Since traditional paper-based and in-person identity authentication methods reduce the speed and efficiency of electronic transactions, there are a variety of alternative technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of “tokens”, transaction profile scripts, biometric identification, and others. [3]

Biometrics can be defined as a measurable physiological and behavioural characteristic that can be captured and subsequently compared with another instance at the time of verification.[19]

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. A verification system authenticates a person's identity by comparing the captured biometric characteristic with her own biometric template(s) pre-stored in the system. In a verification (authentication) system, an individual desired to be identified submits a claim to an identity to the system usually via a magnetic stripe card, login name, smart card, etc:, and the system either rejects or accepts the submitted claim of identity. [4] Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic. Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. Moskovitch et al. (2009) propose the use of behavioral biometrics, i.e., keystroke and mouse dynamics to authenticate to devices and websites (Moskovitch et al., 2009). A basic biometric authentication system consists of five main components (Anil et al., 2008). These are: sensor, feature extractor, fingerprint/template database, and matcher and decision module.[17]

The general purpose of all biometric technologies is to capture and store information at an enrollment stage to compare at a later verification stage. The process of introducing people into a biometrics-based system is called “enrollment.” In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis. Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access. [3]

Basically there are two factors in measuring the accuracy of an efficient biometric system:

1. False reject rate (FRR): FRR is the rate, usually in percentage at which a true authentic person is rejected during the process of authentication as unidentified or unverified by a biometric system.
2. False accept rate (FAR): FAR is the opposite of FRR. FAR is also measured in percentage. This is the rate at which an un-enrolled or an imposter person is accepted as a true authentic by a biometric system. [17]

An important issue in designing a practical biometric system is to determine how an individual should be identified. Depending on the application context, a biometric system may be either a verification (authentication) system or an identification system [5]. The time required by a biometric system to make an identification decision is critical to many applications. For a typical access control application, the system needs to make an authentication decision in real-time. In an ATM application, for instance, it is desirable to accomplish the authentication within about one second. [4]

BENEFITS OF BIOMETRICS:

Biometric technology is one area that no segment of the IT industry can afford to ignore. Biometrics provide security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users. All these industry sectors must evaluate the costs and benefits of implementing such security measures. Different technologies may be appropriate for different applications, depending on perceived user profiles, the need to interface with other systems or databases, environmental conditions, and a host of other application-specific parameters. Its benefits can be summarized in the following points:

- Greater security—biometrics link a person to an action.
- Convenience—clients have no identification number or password to remember.
- Local verification—clients hold their identity information (e.g., on a Smart Card), so there is no need to verify identity via a central repository or server.
- Verification is swift and does not require staff.
- User identity is stored safely and is tamper-free.

The goal of any access control system is to let authorized people into specific places.

Only with the use of a biometric device can this goal be achieved. A card-based access system can control the access of authorized pieces of plastic, but not who is in possession of the card. Systems using PINs (personal identification numbers) require that an individual only know a specific number to gain entry. Who actually enters the code cannot be determined. Biometric devices verify who a person is by what they are, whether it be their hand, eye, fingerprint or voice.

Biometrics also can eliminate the need for cards. While dramatic price reductions have lowered the initial cost of the cards in recent years, the true benefit of eliminating them is realized through a reduced administrative effort. A lost card must be replaced and reissued by someone. There is a cost associated with the time spent to complete the task. Eyes and hands are seldom lost, stolen or forgotten. They also don’t wear out and need to be replaced.

CONCLUSION:

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services.

Biometrics refers to automatic identification of a person based on her physiological or behavioural characteristics. It provides a better solution for the increased security requirements of our information society. As biometric sensors continue to become less expensive (and miniaturized), the negative perception of biometrics as encroachment on individual privacy continue to decline, and as the public realizes that biometrics is actually an effective strategy for protection of privacy/fraud, this technology is likely to be used in almost every transaction needing authentication of personal identities.[4]

The market for biometric devices is not the only part of the industry that is growing. The number of technologies and manufacturers is also expanding. Some of the new technologies look at new unique attributes while others improve on ways to look at characteristics currently being used by today’s biometric systems. Some new approaches are; the thermal pattern created by the blood vessel structure of a person’s face, the pattern of veins and arteries on the back side of your hand, palm print. There is also work being done on an electronic nose. [21]

All other factors remaining identical, the widespread use of biometrics will be stimulated by its adoption in the consumer market. The single most important factor affecting the adoption of biometrics is the cost of the biometrics systems; this includes the cost of the sensors and the related infrastructure. Additionally, biometric technologies requiring very little cooperation/participation from users (e.g., face and thermograms), may be perceived as more convenient to users. A related issue is public acceptance. There may be a generally prevalent perception that biometrics are a threat to the privacy of an individual. The upcoming legislations (e.g., Health Information Portability Act (HIPA) may have a favourable impact on the biometrics industry. [4]

Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. The one thing that can be said with certainty about the future of the biometrics industry is that it is growing! Biometrics are finding their way into all kinds of applications beyond access control. It is expected that more and more information systems/computer networks will be secured with biometrics with the rapid expansion of Internet and Intranet.

REFERENCES:

1. Electronic Banking Risk Management Issues for Bank Supervisors; Electronic Banking Group White Paper; Oct 2000; Retrieved from http://www.bis.org/publ/bcbs76.pdf (Accessed on Dec 2010)
2. Sharma, K.; Singh, AJ, Biometric Security in the E World**.** *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering*. Nemati, 2010; pp 289-337.
3. Authentication in an Internet Banking Environment; *Federal Financial Institutions Examination Council (FFIEC)*; Retrieved from http://www.ffiec.gov/ffiecinfobase/resources/retail/ffi-authentication_guidance.pdf (Accessed on Dec 2010)
4. Jain A, Hong L, Pankanti S; Biometrics: Promising frontiers for emerging identification market; Feb 2000; Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=?doi=10.1.1.10.5497 (Accessed on Dec 2010)
5. Yang Y.J.; The Security of Electronic Banking. *Proc. Nat. I International Systems Security Conference.* National Computer Security Center. 1997; pp. 41-52.
6. Fire Alarm Company Burned by e-Banking Fraud; Retrieved from http://krebsonsecurity.com/2010/04/fire-alarm-company-burned-by-e-banking-fraud/ (Accessed on Dec 2010)
7. Arrests made over Internet banking fraud; Internet Business News, Aug 2000; Retrieved from http://www.allbusiness.com/finance/615165-1.html (Accessed on Dec 2010)
8. Internet World Stats - Usage and Population Statistics; Retrieved from http://www.internetworldstats.com/stats3.htm (Accessed on Dec 2010)
9. APWG ; Retrieved from http://www.antiphishing.org/ (Accessed on Dec 2010)
10. Vrancianu M.; Popa LA; Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests; *The Amfiteatru Economic Journal.* Jun 2010; 12(28): pp388-403
11. Jamil ZU; Cyberlaw towards a new philosophy of Regulation; Retrieved from http://jamilandjamil.com/wp-content/uploads/2010/11/cyberlaw_supreme_court_v10edit.pdf (accessed on Dec 2010)
12. Dias D, McKee K; Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options; *CGAP Focus Notes*; Sep 2010 Retrieved from http://www.cgap.org/gm/document-1.9.47443/FN_64_Rev.pdf Accessed on Dec 2010
13. Legal Framework for Electronic Banking; Retrieved from http://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=28 (Accessed on Dec 2010)
14. Candid Wüeest; Threats to Online Banking; *White Paper: Symantec Security Response*; Retrieved from http://www.symantec.com/avcenter/reference/threats.to.online.banking.pdf (Accessed on Dec 2010)

15. Zin ANM, Yunos Z; How To Make Online Banking Secure; *The Star InTech*; April 2005. Retrieved from http://www.crime-research.org/analytics/online_banking/ (accessed on Jan 2011)
16. Bielski L.; Striving to Create a Safe Haven Online: ID Theft, Worms, Bugs, and Virtual Eavesdropping Banks Cope with Escalating Threat; *ABA Banking Journal*, May 2003; 95
17. Khan B.; Khan MK.; Alghathbar KS, Biometrics and identity management for homeland security applications in Saudi Arabia; *African Journal of Business Management,* Nov 2010, Vol. 4(15): pp. 3296-3306.
18. Whelan S.; Biometrics Technology; *CGAP IT Innovation Series*; Retrieved from http://www.ruralfinance.org/cds_upload/1126265263594_Biometrics_technology.pdf (Accessed on Dec 2010)
19. Ratha NK, Chikkerur S, Connell JH, Bolle RM; Generating Cancelable Fingerprint Templates, *IEEE Transaction on Pattern, Analysis and Machine Intelligence*, Apr 2007; 29(4), pp. 561-572.
20. Liu S.; Silverman M.; A practical guide to biometric security technology, *IT Professional*, Jan/Feb 2001; 3(1), pp 27 – 32
21. Spence B.; Biometrics In Physical Access Control Issues, Status and Trends; Retrieved from http://www.edsales.com.au/pdfs/biom_PhysicalAccess%20Control.pdf (Accessed on Jan 2010)
22. Alter S.; The work system method for understanding information systems and information system research *Communications of the Association for Information Systems* (Volume 9, 2002) 90-104