E-BANKING – INNOVATIVE BANKING PRACTICES

Dr.R.Vasudevan [1] , Akash S [2]
[1]Associate Professor, Management Studies
Easwari Engineering College, Bharathi Salai, Ramapuram, Chennai---600 089
[2]MBA Second Year
Easwari Engineering College, Bharathi Salai, Ramapuram, Chennai---600 089.
E-mail Id: vasu_devan_mba@yahoo.com[1], akashkannah7@gmail.com[2]

ABSTRACT: Security has been widely recognized as one of the main obstacles to the adoption of Internet banking and it is considered an important aspect in the debate over challenges facing internet banking. The performance evaluation of e-banking websites requires a model that enables us to analyze the various imperative factors and criteria related to the quality and performance of e-banking websites. E-banking site evaluation is a complex and dynamic problem involving many factors, and because of the subjective considerations and the ambiguities involved in the assessment, Fuzzy logic (FI) model can be an effective tool in assessing and evaluating of e-banking security performance and quality. In this paper, we propose an intelligent performance assessment model for evaluating e-banking security websites. The proposed model is based on FI operators and produces four measures of security risk attack dimensions: direct internal attack, communication tampering attack, code programming attack and denial of service attack with a hierarchical ring layer structure. Our experimental results show that direct internal attack risk has a large impact on e-banking security performance. The results also confirm that the risk of direct internal attack for e-banking dynamic websites is doubled that of all other attacks

Key Words: Security, Internet Banking Imperative Factors Intelligent Performance

DEFINITION OF E-BANKING:

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. While the risks and controls are similar for the various e-banking access channels, this booklet focuses specifically on Internet-based services due to the Internet's widely accessible public network.

Common E-Banking Services:

Retail Services	Wholesale Services
Account management	Account management
Bill payment and presentment	Cash management
New account opening	Small business loan applications, approvals, or advances
Consumer wire transfers	
Investment/Brokerage services	Commercial wire transfers
Loan application and approval	Business-to-business payments
Account aggregation	Employee benefits/pension administration

E-banking services should consider the following issues:

- ❖ Security controls for safeguarding customer information;
- ❖ Authentication processes necessary to initially verify the identity of new customers and authenticate existing customers who access e-banking services;
- ❖ Liability for unauthorized transactions;
- ❖ Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or credit on-line;
- ❖ Possible violations of laws or regulations pertaining to consumer privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required consumer disclosures; and
- ❖ Negative public perception, customer dissatisfaction, and potential liability resulting from failure to process third-party payments as directed or within specified time frames, lack of availability of on-line services, or unauthorized access to confidential customer information during transmission or storage.

E-BANKING COMPONENTS:
E-banking systems can vary significantly in their configuration depending on a number of factors. Financial institutions should choose their e-banking system configuration, including outsourcing relationships, based on four factors:

- ❖ Strategic objectives for e-banking;
- ❖ Scope, scale, and complexity of equipment, systems, and activities;
- ❖ Technology expertise; and
- ❖ Security and internal control requirements.

Financial institutions may choose to support their e-banking services internally. Alternatively, financial institutions can outsource any aspect of their e-banking systems to third parties. The following entities could provide or host (i.e., allow applications to reside on their servers) e-banking-related services for financial institutions:

- ❖ Another financial institution,
- ❖ Internet service provider,
- ❖ Internet banking software vendor or processor,
- ❖ Core banking vendor or processor,
- ❖ Managed security service provider,
- ❖ Bill payment provider,
- ❖ Credit bureau, and
- ❖ Credit scoring company.

Methods of e-banking:

- Telephone banking
- Online banking
- Short Message Service (SMS) banking
- Mobile banking
- Interactive-TV banking

Telephone banking: It is a service provided by a financial institution which allows its customers to perform financial transactions over the telephone. Most telephone banking systems use an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate their identity through a numeric or verbal password or through security questions asked by a live representative. With the obvious exception of cash withdrawals and deposits, telephone banking offers virtually all the features of an ATM.
Usually, there is the possibility to speak to a live representative located in a call centre or a branch, although this feature is not guaranteed. In addition to the self-service transactions, telephone banking representatives are usually trained to do what was traditionally available only at the branch: loan applications, investment purchases and redemptions, chequebook orders, debit card replacements, change of address, etc.

Online banking: Online banking (or Internet banking), allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society. Online banking offers features such as: bank statements; electronic bill payment; funds transfer; loan applications and transactions and account agggregation that allows users to monitor all of their accounts in one place. It is widely recognised that online banking provides more revenue per customer and costs less per transaction than any other e-banking channel.

SMS banking: SMS banking is a technology-enabled service permitting banks to operate selected banking services over the customers' mobile phone using SMS messaging. SMS banking services are operated using both Push and Pull messages. Push messages are those that the bank chooses to send out to a customer's mobile phone, without the customer initiating a request for the information. Typically push messages could be either Mobile Marketing messages or messages alerting to an event which happens in the customer's bank account, such as a large withdrawal of funds from the ATM or a large payment using the customer's credit card, etc. Another type of push message is a One-time password (OTPs).

Pull messages are those that are initiated by the customer, using a mobile phone, for obtaining information or performing a transaction in the bank account. Examples of pull messages for information include an account balance enquiry, or requests for current information like currency exchange rates and deposit interest rates.

The bank’s customer is empowered with the capability to select the list of activities (or alerts), that he/she needs to be informed. This functionality to choose activities can be done either by integrating to the Internet Banking channel or through the bank’s customer service call centre.

Mobile banking: Mobile banking (also known as M-Banking, mbanking, etc.), or Wireless Application Protocol (WAP) enabled banking is a term used for performing balance checks, account transactions, payments etc. via a mobile device such as a mobile phone or Personal Digital Assistant (PDA). Mobile banking is most often performed via SMS or the Internet accessed through the mobile device, but can also use special programs downloaded to the mobile device.

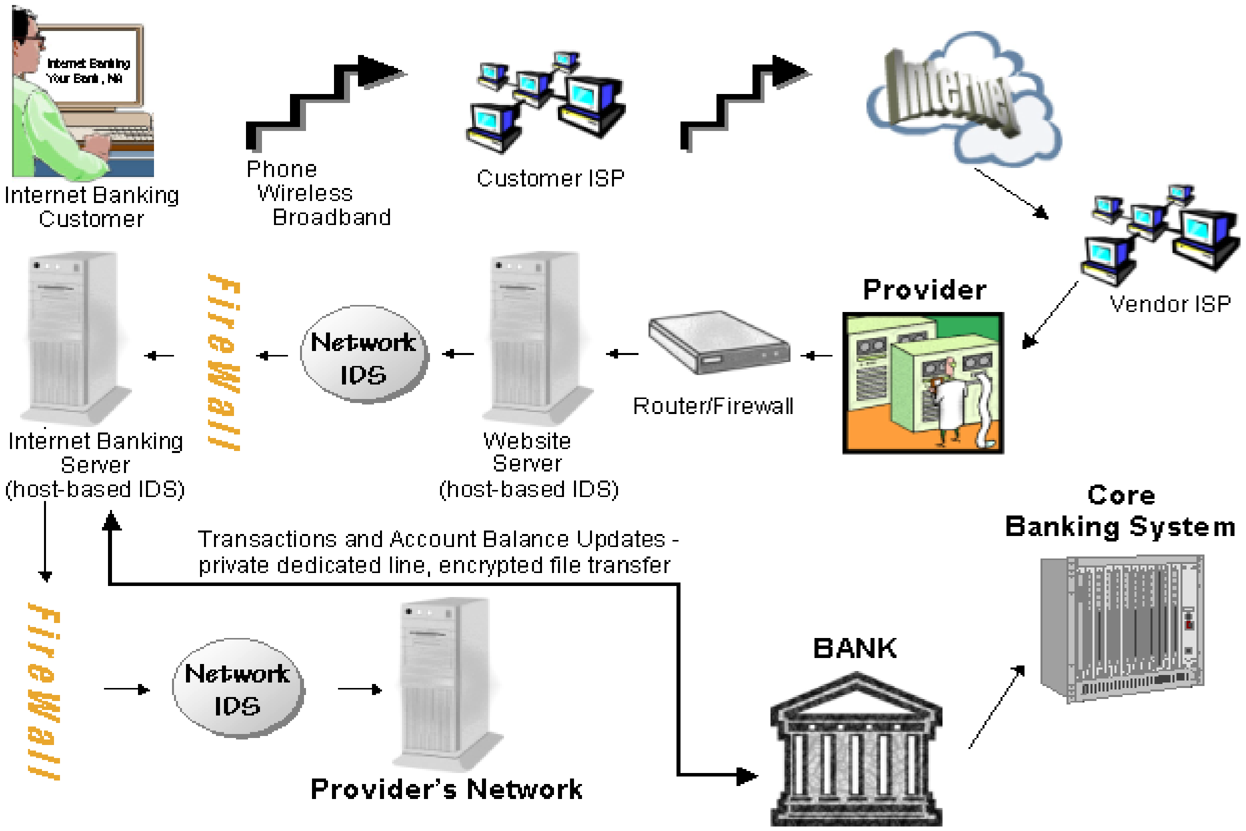
Interactive-TV banking: Interactive television is a technique that allows viewers to interact with television content as they view it. It is sometimes called interactive TV, iTV or idTV. As long as the customer subscribes to a satellite or cable television service some banking facilities, such as, checking balances, moving money between accounts, paying bills and setting up overdrafts are made available through a television set. A handful of major banks in the UK have experimented with digital banking services through cable and satellite TV companies.

E-banking systems rely on a number of common components or processes. The following list includes many of the potential components and processes seen in a typical institution:

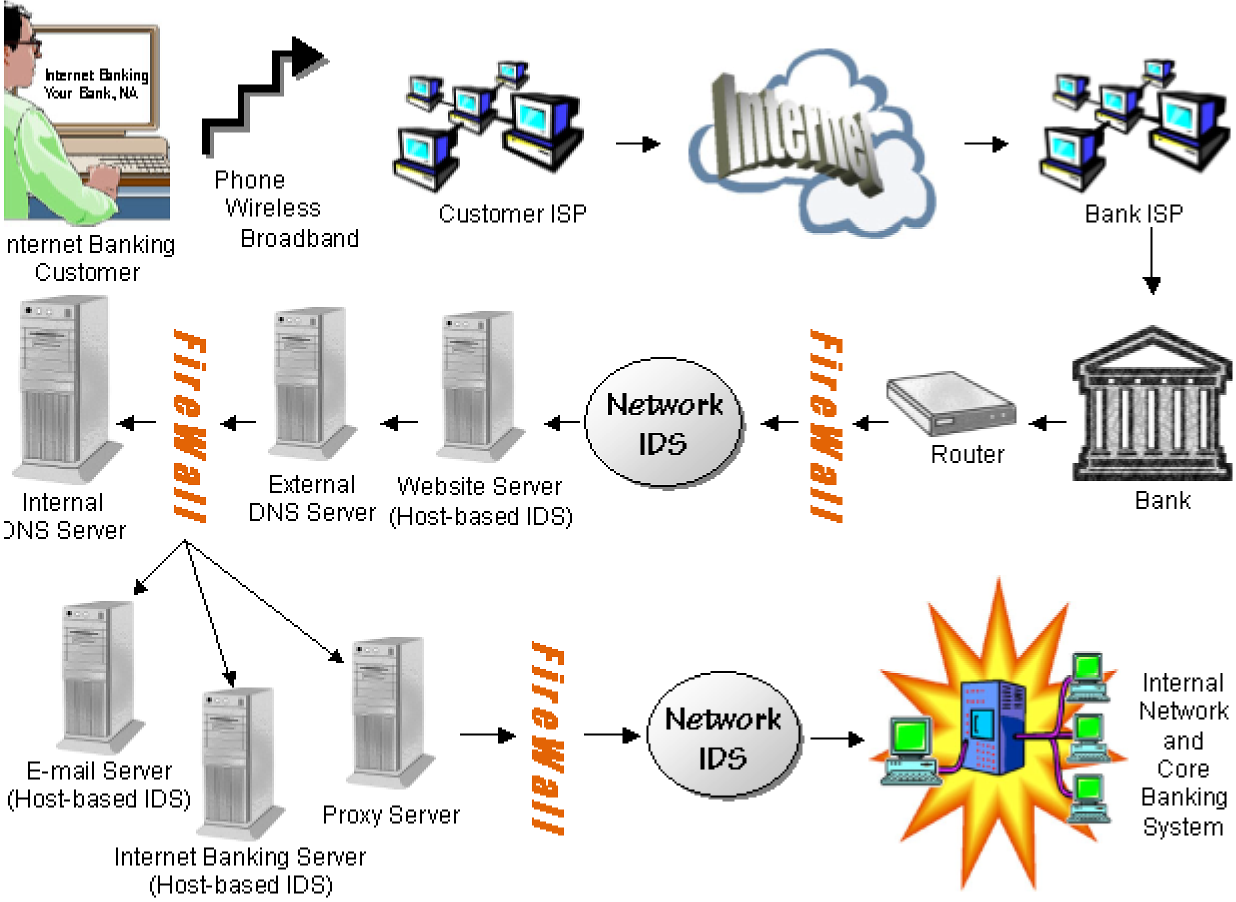
- Website design and hosting,
- Firewall configuration and management,
- Intrusion detection system or IDS (network and host-based),
- Network administration,
- Security management,
- Internet banking server,
- E-commerce applications (e.g., bill payment, lending, brokerage),
- Internal network servers,
- Core processing system,
- Programming support, and
- Automated decision support systems.

These components work together to deliver e-banking services. Each component represents a control point to consider.

Third-Party Provider Hosted E-Banking Diagram:


Internet Banking Your Bank, NA
Internet Banking Customer
Phone Wireless Broadband
Customer ISP
Internet
Vendor ISP
Provider
Router/Firewall
Network IDS
Fire Wall
Website Server (host-based IDS)
Internet Banking Server (host-based IDS)
Transactions and Account Balance Updates - private dedicated line, encrypted file transfer
Core Banking System
BANK
Fire Wall
Network IDS
Provider's Network

In-House E-Banking Diagram:



E-BANKING SUPPORT SERVICES

In addition to traditional banking products and services, financial institutions can provide a variety of services that have been designed or adapted to support e-commerce. Management should understand these services and the risks they pose to the institution. This section discusses some of the most common support services: web linking, account aggregation, electronic authentication, website hosting, payments for e-commerce, and wireless banking activities.

WEBLINKING:

A large number of financial institutions maintain sites on the World Wide Web. Some websites are strictly informational, while others also offer customers the ability to perform financial transactions, such as paying bills or transferring funds between accounts.

Virtually every website contains "weblinks." A weblink is a word, phrase, or image on a webpage that contains coding that will transport the viewer to a different part of the website or a completely different website by just clicking the mouse. While weblinks are a convenient and accepted tool in website design, their use can present certain risks. Generally, the primary risk posed by weblinking is that viewers can become confused about whose website they are viewing and who is responsible for the information, products, and services available through that website. There are a variety of risk management techniques institutions should consider using to mitigate these risks. These risk management techniques are for those institutions that develop and maintain their own websites, as well as institutions that use third-party service providers for this function. The agencies have issued guidance on weblinking that provides details on risks and risk management techniques financial institutions should consider.

ACCOUNT AGGREGATION

Account aggregation is a service that gathers information from many websites, presents that information to the customer in a consolidated format, and, in some cases, may allow the customer to initiate activity on the aggregated accounts. The information gathered or aggregated can range from publicly available information to personal account information (e.g., credit card, brokerage, and banking data). Aggregation services can improve customer convenience by avoiding multiple log-ins and providing access to tools that help customers analyze and manage their various account portfolios. Some aggregators use the customer-provided user IDs and passwords to sign in as the customer. Once the customer's account is accessed, the aggregator copies the personal account information from the website for representation on the aggregator's site (i.e., "screen scraping"). Other aggregators use direct data-feed arrangements with website operators or other firms to obtain the customer's information. Generally, direct data feeds are thought to provide greater legal protection to the aggregator than does screen scraping.

Financial institutions are involved in account aggregation both as aggregators and as aggregation targets. Risk management issues examiners should consider when reviewing aggregation services include:

- ❖ Protection of customer passwords and user IDs – both those used to access the institution's aggregation services and those the aggregator uses to retrieve customer information from aggregated third parties – to assure the confidentiality of customer information and to prevent unauthorized activity,
- ❖ Disclosure of potential customer liability if customers share their authentication information (i.e., IDs and passwords) with third parties, and
- ❖ Assurance of the accuracy and completeness of information retrieved from the aggregated parties' sites, including required disclosures

ELECTRONIC AUTHENTICATION

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. Since traditional paper-based and in-person identity authentication methods reduce the speed and efficiency of electronic transactions, financial institutions have adopted alternative authentication methods, including:

- Passwords and personal identification numbers (PINs),
- Digital certificates using a public key infrastructure (PKI),
- Microchip-based devices such as smart cards or other types of tokens,
- Database comparisons (e.g., fraud-screening applications), and
- Biometric identifiers.

The authentication methods listed above vary in the level of security and reliability they provide and in the cost and complexity of their underlying infrastructures. As such, the choice of which technique(s) to use should be commensurate with the risks in the products and services for which they control access. Additional information on customer authentication techniques can be found in this booklet under the heading "Authenticating E-Banking Customers."

- Downtime (i.e., times when website is not available) or inability to meet service levels specified in the contract,
- Inaccurate website content (e.g., products, pricing) resulting from actions of the institution's staff or unauthorized changes by third parties (e.g., hackers),
- Unauthorized disclosure of confidential information stemming from security breaches, and
- Damage to computer systems of website visitors due to malicious code (e.g., virus, worm, active content) spread through institution-hosted sites.

PAYMENTS FOR E-COMMERCE

Many businesses accept various forms of electronic payments for their products and services. Financial institutions play an important role in electronic payment systems by creating and distributing a variety of electronic payment instruments, accepting a similar variety of instruments, processing those payments, and participating in clearing and settlement systems. However, increasingly, financial institutions are competing with third parties to provide support services for e-commerce payment systems. Among the electronic payments mechanisms that financial institutions provide for e-commerce are automated clearing house (ACH) debits and credits through the Internet, electronic bill payment and presentment, electronic checks, e-mail money, and electronic credit card payments.

Most financial institutions permit intrabank transfers between a customer's accounts as part of their basic transactional e-banking services. However, third-party transfers – with their heightened risk for fraud – often require additional security safeguards in the form of additional authentication and payment confirmation.

Bill Payment and Presentment

Bill payment services permit customers to electronically instruct their financial institution to transfer funds to a business's account at some future specified date. Customers can make payments on a one-time or recurring basis, with fees typically assessed as a "per item" or monthly charge. In response to the customer's electronic payment instructions, the financial institution (or its bill payment provider) generates an electronic transaction – usually an automated clearinghouse (ACH) credit – or mails a paper check to the business on the customer's behalf. To allow for the possibility of a paper-based transfer, financial institutions typically advise customers to make payments effective 3–7 days before the bill's due date.

Internet-based cash management is the commercial version of retail bill payment. Business customers use the system to initiate third-party payments or to transfer money between company accounts. Cash management services also include minimum balance maintenance, recurring transfers between accounts and on-line account reconciliation. Businesses typically require stronger controls, including the ability to administer security and transaction controls among several users within the business.

Financial institutions can offer bill payment as a stand-alone service or in combination with bill presentment. Bill presentment arrangements permit a business to submit a customer's bill in electronic form to the customer’s financial institution. Customers can view their bills by clicking on links on their account’s e-banking screen or menu. After viewing a bill, the customer can initiate bill payment instructions or elect to pay the bill through a different payment channel.

In addition, some businesses have begun offering electronic bill presentment directly from their own websites rather than through links on the e-banking screens of a financial institution. Under such arrangements, customers can log on to the business’s website to view their periodic bills. Then, if so desired, they can electronically authorize the business to “take” the payment from their account. The payment then occurs as an ACH debit originated by the business’s financial institution as compared to the ACH credit originated by the customer’s financial institution in the bill payment scenario described above. Institutions should ensure proper approval of businesses allowed to use ACH payment technology to initiate payments from customer accounts.

Cash management applications would include the same control considerations described above, but the institution should consider additional controls because of the higher risk associated with commercial transactions. The adequacy of authentication methods becomes a higher priority and requires greater assurance due to the larger average dollar size of transactions. Institutions should also establish additional controls to ensure binding agreements – consistent with any existing ACH or wire transfer agreements – exist with commercial customers. Additionally, cash management systems should provide adequate security administration capabilities to enable the business owners to restrict access rights and dollar limits associated with multiple-user access to their accounts.

Person-to-Person Payments

Electronic person-to-person payments, also known as e-mail money, permit consumers to send “money” to any person or business with an e-mail address. Under this scenario, a consumer electronically instructs the person-to-person payment service to transfer funds to another individual. The payment service then sends an e-mail notifying the individual that the funds are available and informs him or her of the methods available to access the funds including requesting a check, transferring the funds to an account at an insured financial institution, or retransmitting the funds to someone else. Person-to-person payments are typically funded by credit card charges or by an ACH transfer from the consumer’s account at a financial institution. Since neither the payee nor the payer in the transaction has to have an account with the payment service, such services may be offered by an insured financial institution, but are frequently offered by other businesses as well.

Some of the risk issues examiners should consider when reviewing bill payment, presentment, and e-mail money services include:

- ❖ Potential liability for late payments due to service disruptions,
- ❖ Liability for bill payment instructions originating from someone other than the deposit account holder,
- ❖ Losses from person-to-person payments funded by transfers from credit cards or deposit accounts over which the payee does not have signature authority,
- ❖ Losses from employee misappropriation of funds held pending access instructions from the payer, and
- ❖ Potential liability directing payment availability information to the wrong e-mail or for releasing funds in response to e-mail from someone other than the intended payee.

WIRELESS E-BANKING

Wireless banking is a delivery channel that can extend the reach and enhance the convenience of Internet banking products and services. Wireless banking occurs when customers access a financial institution's network(s) using cellular phones, pagers, and personal digital assistants (or similar devices) through telecommunication companies’ wireless networks. Wireless banking services in the United States typically supplement a financial institution's e-banking products and services.

Wireless devices have limitations that increase the security risks of wireless-based transactions and that may adversely affect customer acceptance rates. Device limitations include reduced processing speeds, limited battery life, smaller screen sizes, different data entry formats, and limited capabilities to transfer stored records. These limitations combine to make the most recognized Internet language, Hypertext Markup Language (HTML), ineffective for delivering content to wireless devices. Wireless Markup Language (WML) has emerged as one of a few common language standards for developing wireless device content. Wireless Application Protocol (WAP) has emerged as a data transmission standard to deliver WML content.

Manufacturers of wireless devices are working to improve device usability and to take advantage of enhanced “third-generation” (3G) services. Device improvements are anticipated to include bigger screens, color displays, voice recognition applications, location identification technology (e.g., Federal Communications Commission (FCC) Enhanced 911), and increased battery capacity. These improvements are geared towards increasing customer acceptance and usage. Increased communication speeds and improvements in devices during the next few years should lead to continued increases in wireless subscriptions.

As institutions begin to offer wireless banking services to customers, they should consider the risks and necessary risk management controls to address security, authentication, and compliance issues. Some of the unique risk factors associated with wireless banking that may increase a financial institution's strategic, transaction, reputation, and compliance risks are discussed in appendix E.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

1. Physical security of the hand-held device
2. Security of the application running on the device. In case the device is stolen, the hacker should require ID / Password to access the application
3. Authentication of the device with the service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions
4. User ID / Password authentication of bank’s customer
5. Encryption of the data being transmitted over the air
6. Encryption of the data that will be stored in the device for later / off-line analysis by the customer.