NOTRE DAME UNIVERSITY

Security of Electronic Banking in Lebanon:

Status and Prospects

By

Joelle P. Abboud

A Thesis

Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science in Computer Science

Department of Computer Science
Faculty of Natural and Applied Science

June 2005

N. D. U. LIBRARY
26 AUG 2005
RECEIVED

Security of Electronic Banking in Lebanon: Status and Prospects

By

Joelle P. Abboud

Committee members:

Dr. Marie Khair: Associate Professor of Computer sciences
Advisor

Dr. Hoda Maalouf: Assistant professor of Computer Sciences and Chairperson
Member of committee

Dr. Khaldoun El-Khalidi: Assistant Professor of Computer Science.
Member of committee

Dr. Holem Saliba: Assistant Professor of Mathematics
Member of committee

Approved on 20th of June 2005

Table of Contents

Abstract

Internet banking is somehow a new technology used by banks to interact with their customers providing them with a wide range of services available online. These services can be classified into 5 categories: informational, administrative, transactional, portal and others. However with these come new challenges, risks and threats when adapting internet banking that are either inherited from the internet or that are specific to the open banking environment. Therefore, specific security requirements to the internet banking environment should be adopted aiming to control these risks and manage them. These generally can be categorized as: authentication, non repudiation, data and transaction integrity, data confidentiality and system availability.

Basel Committee, a part of the oldest international financial institution BIS (Bank for International Settlement), has proposed some internal and operational security practices. This thesis is trying to map the Lebanese market to these practices and to assess, to which level the later is compliant to these requirements as Lebanon is already compliant with the previous guidelines. For this reason, we performed a survey on the web sites of all of the Lebanese banks and we tried to map the Lebanese market to the standard categorization proposed by Basel.

Later, two surveys were issued. The first directed towards the Lebanese customers, in order to evaluate their security awareness and fears, along with their evaluation of the Internet banking technology. The other, directed towards the banks, in order to evaluate the bank's security practices and to which level they are compliant to the Basel Committee's requirements.

The result is a description on the different aspects adopted in the Lebanese internet banking activities describing security, risks management and actual internal practices implemented from the bank's side and their impact on the different bank services in addition to the customer's interaction to the out coming services provided. This was somehow limited due to the small number of banks that replied the questionnaire but gave a clear view of the current status and the main points needed to be developed in order to adapt all the guidelines of Basel.

List of Figures

List of Tables

Acknowledgements

To accomplish anything we need support and encouragement.

To my advisor Dr. Marie Khair thank you for help and support to finish my work.

To all the persons who answered the surveys, for their support and encouragement, thank you.

To my parents, my husband and daughter who encouraged me, I can never thank them enough for what they did.

Nothing can be done without all mighty GOD.

Thank you.

Chapter 1

Introduction

1.1. Introduction and problem definition

Continuing technology developments and innovations are having significant impact on the way banks interact with their customers, outsourced vendors and counterparties, and how they undertake their operations. Banks face the challenge of adapting, innovating and responding to the opportunities posed by computer systems, telecommunications, networks and other technology-related solutions to drive their businesses in an increasingly competitive domestic and global market.

The internet banking in particular offers major opportunities for banks to reach new markets and expand the range of products and services they provide to customers. However, by its nature, the accessibility and dynamism of the internet brings both benefits and risks. Benefits, risks and their management are detailed in this thesis.

The aim of this thesis is to give a detailed description on the different aspects of internet banking activities describing security, risks management and internal practices from the bank's side and their impact on the different bank services in addition to the customers' interaction to the out coming services provided.

Finally this thesis objective is to determine the level of security of internet banking applied in Lebanon and to focus on security, management, technology, integrity, availability, and outsourcing.

To achieve this objective, two methods were used:

- Bibliographical research: based on references, note that there was no much of security documents directly related to internet banking.
- Survey: based on questionnaires along with direct visits to several Lebanese financial institutes.

1.2. Thesis Organization

This thesis consists of 7 chapters where the first chapter is the introduction. Chapter 2 describes Internet banking, its categories, advantages and disadvantages, as well as mobile banking. In this chapter, we mapped the Lebanese market to the standard categorization using a survey on the Lebanese bank's web sites.

Chapter 3 introduces general security threats and countermeasures. Chapter 4 studies Basel's committee specific risks in Internet banking, threats and security requirements in Internet banking stressing on real case examples.

Chapter 5 stresses on internal security practices directly related to daily procedure and functionalities like training, outsourcing, management etc. Chapter 6 addresses operational security practices applied like authentication, communication, customer education etc.

Finally, chapter 7 describes the results of surveys conducted among the Lebanese customers and banks to identify the level of security applied compared to the standard of the Basel committee.

Chapter 2

Internet and Mobile Banking

The objective of this chapter is to describe the different categories of internet banking and to highlight its advantages and disadvantages in order to identify the possible risks and counter measures that will be described in the subsequent chapters.

A survey of the Lebanese market has been conducted to identify the size and types of the services provided by this market. The identified services are then mapped to the standard internet banking categories.

2.1. Internet Banking Categories

Internet banking provides a high range of services. These services can be classified into 5 categories [41, 42, 50]:

- Informational
- Administrative
- Transactional
- Portal
- Others

The first 3 categories form the subdivision that is used by most literature and standards. They are directly related to Internet banking activities. Note that the standard categorization is the one used throughout this research.

2.1.1. Informational

Informational service is limited to a simple web site that is used by banks to provide information and publicity. It does not require any interaction with the bank's network, it is a one-way communication.

General bank information is posted on this informational web site (i.e. branch network, phone numbers, ATM network, employment information, achievements etc.)

In other words the informational web site is the bank's online brochure.

2.1.2. Interactive / Administrative

Interactive/administrative services allow customers to conduct inquiries on their accounts. This service does not involve money transactions, but holds customers' private banking information.

A breach of the security in this area does not affect either customer or banks accounts, but it can easily disclose information which might affect the bank's reputation and the customer's private information.

The services available in this category are:

- Application: users can download applications to be filled and delivered at any of the bank's branches, or they can fill the applications online as ordering a new check book, loan application etc.
- Stop payment on a check: customers can issue a stop payment order, or inquire about the status of check.
- Account balance: customers can check their balance(s) online, anytime, anywhere.
- Account history: statement of accounts can be checked and downloaded.
- Mail notification: it is used to inform and alert customers. Email notification in case an account balance rises above or drops below a certain amount, monthly statement etc.

2.1.3. Transactional

Transactional services allow bank customers to actually conduct business through the web site. As can be inferred from the name, the services presented deal with all money related transactions. With this type of services, security is of high importance, as any breach will eventually affect balances.

In addition to the services provided by the previous types, transactional web sites provide:

- Transfer: users can transfer money from one bank account to another, using a transfer function that asks for amount to transfer, from/to accounts and the effective transfer date.
- Payment: users can take advantage of online transfer facilities to transfer money to special accounts such as loan accounts, pay bills, or even schedule automatic recurring bill payments.

2.1.4. Portal

Introduced by Holland and Westwood, is the service of linking the customer, through the bank, to other web sites of interest. These sites can provide local information, financial information, stock market, weather etc.

2.1.5. Others

The other functionality services contains features that do not fit into the previous four categories. As example of these services search function used on the web site.

2.2. Mobile Banking

In parallel with internet banking, mobile banking is used to perform electronic banking. It provides a high range of services presented to the public either through Wireless Application Protocol (WAP) or Short Message Service (SMS).

The function of WAP banking is similar to internet banking through the web. The client sends a request and gets a response with page content which is stored on or dynamically generated by a standard web server. Some of the services provided by WAP are: list of latest transactions, intra account transfer.

SMS is used to transmit messages up to 140 bytes. Banks could generate messages, alerts from its data like: account balance, account movements (withdraw, deposit, ATM transaction...) or receive messages from the customer like: request statement, order check book, etc. [36]

2.3. Internet and Mobile Banking Services in Lebanon

The list of banks and financial institutions having web sites can be found on the following link from the central bank's website: http://bdl.gov.lb/otherlnks/bankklink.htm.

The result of surfing the websites of 30, as of 1st of March 2005, banks is stated in table 2.1:

13 banks are already providing internet banking with services varying from administrative to fully transactional while 4 banks are planning to provide these services in the near future. In addition to Internet banking, 3 banks are already taking advantage of mobile technology and providing their customers with some kind of mobile banking like SMS alerts, balance inquiry, order statement.

Table 2.1: List of banks with web site visited as of the 1st of March 2005

Bank Name	Informational Web Site	Interactive	Transactional	Mobile Banking
Al Baraka	www.al-baraka.com		Soon	
Al Mawarid	www.almawarid.com		Available	
Allied Bank	www.alliedbank.com .lb			
Arab Bank	www.arabbank.com		Available	Outside Lebanon
Banca Di Roma	www.lb.bdroma.com			
Bank of Beirut	www.bankofbeirut.com.lb	Available		
Banque Audi	www.audi.com.lb		Available	
Banque de l'habitat	www.banque-habitat.com.lb			
Banque de l'industrie et du travail	www.bitbank.com.lb			
Banque Lati	www.banquelati.com			
Banque Libano-Francaise	www.eblf.com		Available	
Banque Misr	www.bml.com.lb			
Banque Saradar	www.saradar.com			
Bank of Beirut and Arab Countries	www.bbacbank.com		Available	
Banque Europenne pour le Moyen Orient	www.bemo.com.lb			
Banque du Liban et d'Outre-Mer	www.blom.com.lb		Available	SMS (alerts)
Banque Nationale de Paris Intercontinentale	www.bnpi-liban.bnpparisbas.com		Available	
Byblos Bank	www.byblosbank.com.lb		Soon	
Credit Libanais	www.creditlibanais.com		Available	WAP
CreditBank	www.creditbank.com .lb		Soon	Soon
Fransabank	www.fransabank.com			
HSBC	www.lebanon.hsbc.com/ lebanon.html		Available	
Jammal Trust bank	www.jammalbank.com.lb			
Lebanese Canadian Bank	www.lebcanbank.com		Soon	
MEAB	www.meabank.com			
National Bank of Kuwait (Lebanon)	www.nbk.com.lb	Available		SMS
Saradar	www.saradar.com/sfp /sfp_ef_html/ public_page.html		Available	
Societe Generale de Banque au Liban	www.sgbl.com.lb/sgbl/french		Available	

Bank Name	Informational Web Site	Interactive	Transactional	Mobile Banking
Standard Shartered	www.standardcharter ed.com.lb			
Syrian lebanese commercial bank	www.slcb.com.lb/eng lish/index.html			

After having identified the banks providing Internet banking services, table 2.2 is used to classify these services into interactive/administrative and transactional based on the categorization already described.

Table 2.2: Lebanese Banks' Internet Banking Services

	Internet Banking Services	Credit Libanais	BOB	Arab Bank	Audi	BBAC	BLOM	SGBL	NBK	HSBC	BLF	BNPI	Saradar
Interactive / Administrative	View account and balances	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Statement of account	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Download statement	Y	Y		Y	Y	Y	Y	Y	Y	Y		Y
	Update personal details (address, phone number)	Y		Y						Y			
	Order checkbooks	Y	Y	Y		Y	Y						
	Request stop payment on a check	Y				Y		Y					
	Status of checks for collection						Y		Y				
	Request for domiciliation of bills		Y										
	Deposit details			Y			Y						
	Report a lost card					Y							
	Report loss of a saving passbook					Y							
	Check pending transactions						Y						
	Check visa card balance						Y						
	Set visa card safety limits						Y						
Transactional	Transfer funds between accounts	Y		Y	Y	Y	Y	Y		Y	Y	Y	Y
	External transfer of funds	Y		Y				Y		Y		Y	
	Bill payment	Y		Y				Y		Y			

Legend: Banque of Beirut (BOB), Bank of Beirut and Arab Countries (BBAC), Banque du Liban et d'Outre Mer (BLOM), Societe Generale de Banque au Liban (SGBL), National Bank of Kuwait (NBK), Banque Libano-Francaise (BLF), Banque Nationale de Paris Intercontinentale (BNPI).

Three banks are providing mobile banking in Lebanon with different services. Details are listed in table 2.3 below.

Table 2.3: Lebanese Banks' Mobile Banking Services

Mobile Banking Services	Credit Libanais	BLOM	NBK
Balance inquiry	Y		Y
Statement (mini)	Y		Y
Statement order			Y
Transfer funds between accounts	Y		
Checkbook request	Y		Y
Stop payment on a check	Y		
Credit card balance	Y		
Credit card statement	Y		
Stop a lost ATM or credit card			Y
Message from bank (alerts)	Y	Y	Y

Legend: Banque du Liban et d'Outre Mer (BLOM), National Bank of Kuwait (NBK).

2.4. Advantages and Disadvantages

Internet banking presents several advantages for both banks and customers. [24, 43]

Concerning banks, the main advantages are:

- Cost reduction: where the cost of inquiries and transactions conducted online is less than the ones conducted at the branch
- Relieve pressure from branches.
- Better customer service and satisfaction: "banking is no longer tied to time and place" [24], banking is provided to customer anywhere anytime.
- Reaching new segments of the population (expatriate).

As for the customer, advantages are:

- Convenience: money can be transferred, bills paid without having to wait in queues at branches, or writing checks.
- Accessibility and availability: services are available anywhere anytime.
- Time saving: as the customer can conduct a wide range of available services without having to travel to the bank.
- Privacy: customers can enjoy a higher level of privacy while interacting with their bank.
- Range of services: high level of services is available online, making it easier for customers to maintain and manage their accounts.

The main disadvantage of internet banking is that, by its nature, it is cashless and that it opens new ways for security breaches.

Chapter 3

General Security Threats and Countermeasures

3.1. Network Security

Communication over the network is done usually using TCP/IP (Transmission control protocol / Internet protocol) protocol. TCP ensures the correct sequencing of packets and integrity of data in transmission within these packets, while IP uses Internet addressing scheme known as IP.

The fact that this protocol allows data to pass through intermediate computers makes it possible for a third party to listen and/or interfere with data in transit. In addition, hackers can create some network vulnerabilities: eavesdropping, tampering, impersonation, denial of services.

Eavesdropping

Because network involves data in transit, the easiest attack is to listen. If data is not encrypted, the listener, known as eavesdropper, can obtain valuable information like password, sensitive conversation or even a credit card number simply by listening to the communication. Information however remains intact.

Tampering

Information in transit is altered and replaced then sent to the recipient. For example someone could alter an order for goods. We can subdivide tampering into:

- Session hijacking: carrying a session began by a third party that intercepts the traffic and carries on the established session in the name of one of the legitimate parties. This is usually done at the end of the session. For example, let a web site carry on the hard part of convincing users, and the session is hijacked when users actually do the purchase.
- Man in the middle attack: similarly to session hijacking, it involves an intruder participating in the session, but this time from the start.

Impersonation

In this attack, the third party (attacker) pretends to be another entity (legitimate party). We can also subdivide it into two forms:

- Spoofing (masquerade): a host pretending to be another. For ex: URL confusion. Domain names can be easily confused. For example create a domain bankXYZ.com, make it look like bank.XYZ.com and collect user names and passwords. Or take advantage of easily mistyped names, like Citibank.com and Citybank.com.

- Misrepresentation: a person or an organization can misrepresent itself. For example a site pretending to sell goods, while in reality it only takes credit card payments with no goods in return. Or a site pretending to be a cyber bank which is a bank that is totally operating on the web with non existence of any brick and mortar branches.

Denial of Service(DoS)

This attack is directed towards availability of web site that is preventing legitimate users from logging to the application.

Different forms exist for this attack:

- Transmission failure: communication fails for many reasons such as line is cut, hardware or software failure.
- Connection flooding: attacker sends data as much as the communication system can handle, in other words floods the system. As example we can state the ping of death where the attacker sends a flood of pings to the victim, i.e. attack from 100MB towards 10 MB where the ping packets will saturate the victim's bandwidth.
- Smurf: attacker sends broadcast request to network with victim's address. All networks will reply the victim, therefore, flooding it.
- Synflood: the handshake protocol needs 3 steps to be completed. Normally, the client sends a SYN packet to the server, which responds with a SYN_Acknoledge. The client responds to the SYN_ACK and the conversation is started. The Synflood attack takes advantage of this characteristic, where the attacker does not respond the SYN_ACK and keeps on sending SYN messages and this before the time out of the SYN waiting stack.
- Traffic redirection: in this case the router is flooded
- Distributed DoS: in this case, the victim has to defend against multiple attacks. The attacker sends Trojan files to many systems referred to by zombies. Once he chooses the victim, he will activate zombies to launch attack. Not all zombies need to use same attack: smurf, flooding and Synflood can be used simultaneously.

3.2. Security Management

As a counter measure for the threats existing on the web, different security management exists. These are mainly: encryption, public key protocols, digital signature, certificates and authentication.

3.2.1. Encryption

Encryption is the process of encoding a message so that its meaning is unintelligible for the outside observer. Encryption allows two communicating parties to disguise, scramble information they send to each other. The sender encrypts information or message before sending it. The receiver decrypts the message after receiving it. The encrypted information is unintelligible to any outside observer or intruder while in transit.

A cryptographic algorithm, also called a cipher, is a mathematical function used for encryption or decryption. Two types of encryption exist: symmetric and asymmetric. With symmetric encryption the algorithms use the same key for both encryption and decryption. Asymmetric encryption uses algorithms based two related keys one for encryption, the other for decryption.

3.2.2. Public Key Infrastructure

Public key infrastructure (PKI) is an asymmetric encryption algorithm. Each user has a pair of keys, one public and one private. The user can send his public key through email, or post it in a public library while preserving the secrecy of his corresponding private key. A message encrypted with a public key can only be decrypted by its corresponding private key. The advantage of this method is that user has only to manage 2 keys.

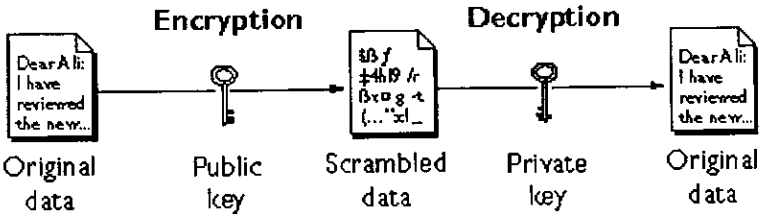


Figure 3.1: Public key infrastructure

3.2.3. Digital Signature

Like real signature, it is a mark that only the sender can make and is used to confirm agreement to a message. Digital signature is used to ensure non-repudiation, i.e. once signed; it is difficult for a party to deny the fact. It is done using the inverse property of PKI that is a message encrypted using the private key can only be decrypted with the public key.

The sender uses his private key to sign data. Since his corresponding public key is known, the receiver can decrypt signature and ensures it is from the sender. To ensure integrity of transferred data, sender uses a one-way hash function, encrypts it with his private key and sends the result along with the message. The receiver uses the same hash function and compares the results. If both results match, data is from the sender and it had not been tampered with.

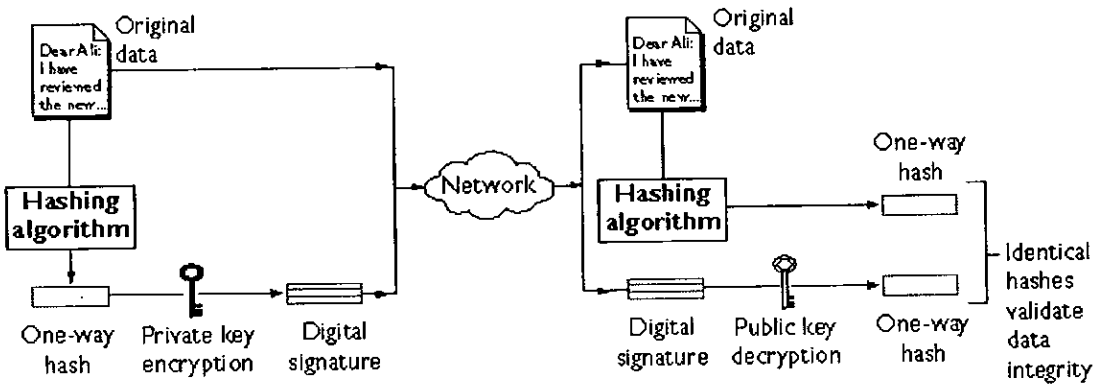


Figure 3.2: Digital signature

3.2.4. Certificates

Although digital signatures are used to ensure integrity and non-repudiation, it does not provide certification about the sender's identity. This is done using certificates, special type of digitally signed document.

Not only do they bind the name of the entity and its corresponding public key, certificates include an expiration date, a serial number, the name of the certificating authority (CA) and its digital signature. They are used to prevent impersonation.

Certificates can be revoked. The CA issues a certificate revocation list (CRL). This list is periodically updated; note that it holds only invalid certificates and not expired.

Certificate authorities are usually a trusted party that validates certificates and post them. Certificates are issued using a traceable chain of trust or a hierarchy. In the certificate hierarchy, each entity is the CA for its subordinates. In the chain of trust, verification is used. If the CA is a trusted authority, verification stops, otherwise, system will check the CA of the issuer in a loop until it reaches the trusted authority. If for any reason, the verification couldn't reach the trusted authority the certificate is rejected.

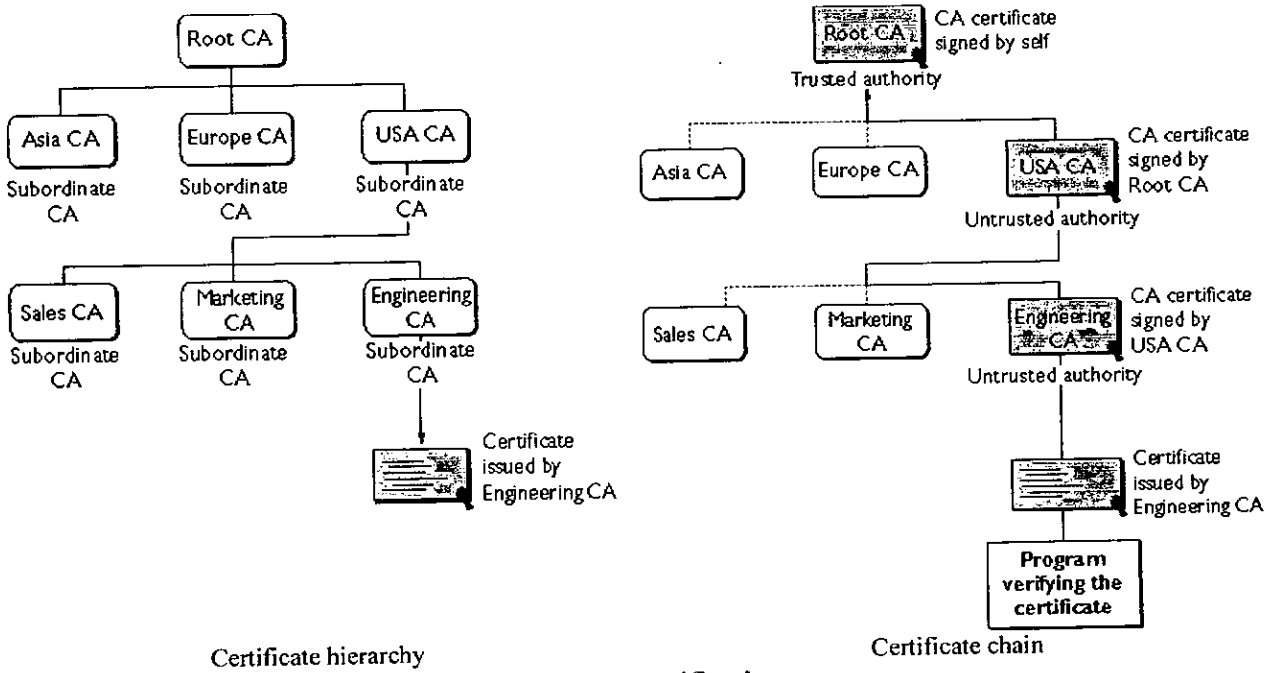


Figure 3.3: Certificates verification

3.2.5. Authentication

Authentication is the process of verifying identity. It is done with something the user:

- knows (password, pin, certificates)
- has (credit card, driver license)
- is (fingerprint, pattern).

Passwords are widely used, but it is important to note the password selection criteria that should be used: use of upper and lower case, long passwords (Length greater than 5; this makes it longer to crack), choose an unlikely password, avoid replacing the letter 'o' by zero, as hackers already use these substitutions in their search table. It is a good practice to change password regularly and keep it private (don't tell anyone about it).

Note that authentication, especially how it is needed in the banking sector, is studied, in details, in chapter 6.

Chapter 4

Risks, Threats and Security Requirements in Banking Environment

The objectives of this chapter is to describe the risks faced by banks in Internet banking environment specially as described by the Basel committee, identify possible threats and provide the appropriate security requirements needed to preserve the security of the entire system.

4.1. Basel Committee

The Basel Committee is part of the oldest international financial institution BIS (Bank for International Settlement) that has currently 55 members of central banks. The Committee was established by the central bank governors of the group of ten countries "G-10" at the end of 1974. These countries are Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States.

The committee does not possess any authority or legal force, but it formulates standards, guidelines and recommendations that can be adopted by individual authorities in order to promote for common standards in the banking sector.

The committee published many documents related to electronic banking. These documents identify and classify the risks banks are exposed to in electronic banking and provide guidance for the management of these risks.

Although not a member, Lebanon usually applies the recommendations of the committee.

4.2. Risks in Internet Banking

According to the Basel Committee different types of risks are associated with Internet banking. [8, 10, 11] They are mainly: operational, reputational, legal, cross border and others.

4.2.1. Operational Risk

Due to the fact that internet banking relies heavily on new technology, operational risk is the most significant one. It might be the result of human error such as customer misuse, or not well designed online banking system. It is also related to security where banks can be subject of external or internal attacks.

According to the Basel Committee operational risk can be subdivided to different components: technology, security, data integrity, system availability, internal controls/audit and outsourcing.

- Technology: Electronic banking is a new technology to be integrated with the already existing legacy systems. This integration might also require cooperation with multiple service providers and partners. It also falls under budgetary restrictions, especially to reply for the need for new hardware and software, and for training up to date technical staff. The bank is exposed to risks from errors in both transaction processing and/or poorly designed or implemented systems. The bank is also responsible for ensuring that operations are controlled and managed even in the case of a third party providing internet banking application.
- Security: Security risk is the primary constraint to internet banking for both banks and customers. Security risks can be divided into internal and external. Internal threats come from employees acquiring authentication data, or stored value cards. External threats such as hacking, sniffing, spoofing, and denial of service are inherited from the open nature of the web. Banks must ensure controlled access to their systems using strong authentication, confidentiality and integrity of information as well as non repudiation.
- Data integrity: Data integrity is very important to system security. Banks must ensure that data in transit between the bank's legacy system and internet banking application is translated and integrated accurately. Effective controls should be enforced to verify the accuracy and integrity of data in transit.
- System availability: The definition of internet banking is the availability 24 hours a day, 7 days a week. Risks rise from denial of service attack where the bank looses its ability to serve its customers or even from a problem in the availability of the internet network.
- Internal controls/Audit: Banks must provide a sufficient level of control to prevent fraud. Banks' responsibility is to ensure that internet banking is properly controlled and easily audited.
- Outsourcing: Outsourcing provides banks with internet banking technology but adds the burden of managing risks from third parties. This is by far more complex in the context of multiple vendor/service providers. Minor disruptions by third party expose banks to financial loss, legal or reputational risks. Additional privacy risks might arise, as the bank may not be always aware of the amount of information collected by third parties.

4.2.2. Reputational Risk

Reputational risk is the risk of facing bad public opinion, which can lead to significant loss of funds or customers. The bank's reputation suffers if it fails to deliver secure, accurate and timely internet banking services on a consistent basis. The reputation can

also suffer if the bank: fails to respond to inquiries posted via email, does not provide proper disclosures, or violates customer's privacy.

Any problem with data, any breach by external or internal attack not only undermines the public confidence in the corresponding bank, but also in the entire electronic business.

4.2.3. Legal Risk

Electronic banking is conducted via the web. Laws related to digital signature and enforceability of electronic contracts are still under development and not well established. For example, if a bank makes his web page available in another language, a country where this language is spoken might consider that this bank is marketing to its citizens and should be compliant to the local regulations.

4.2.4. Cross Border Risk

Cross border risk comes from the expanding nature of Internet banking beyond national borders. It is similar to the one faced in the international transactions conducted by banks. Banks may face different regulations and requirements when they deal with customers across borders. In addition, uncertainties may arise on the legal requirements in some countries which would expose banks to non-compliance with different national laws and regulations such as customer protection laws, record keeping, privacy rules, and money laundering...

4.2.5. Other Risks

"Other" refers to the traditional banking risks, but with less impact than the previously stated one. To state some of these risks:

- Credit risk: is the risk that a counterparty will not settle an obligation for full value either due or anytime thereafter. Internet banking allows banks to expand rapidly hence putting much pressure on internal risk controls. The expansion is also geographically which make it more difficult to control credit risk due to the challenge of understanding new market dynamics, along with the potential risk of concentrating credit to a single industry or geographical area.
- Liquidity risk: is the risk arising from the bank's inability to meet its obligations when they come due without incurring unacceptable losses although the bank may ultimately be able to meet its obligations. Internet banking increases deposit volatility. Depositors can transfer their funds in mass at any time in the day any day of the week.
- Money laundering: in case the system was used to transfer criminal funds.

4.3. Threats

A threat to a computer system is a set of circumstances that has the potential to cause loss or harm.

Different threats exist and they can be classified into physical and cyber threats. In this study, physical threat is confined to hardware malfunction due to human intervention or natural disaster like lightning strikes, power surges, etc.

As for cyber threats, they are more likely to occur. This was clearly shown by a survey conducted in April 2002 by the Computer Security Institute (CSI) / FBI Computer crime and Security Survey where 90% of respondents (of which 20% come from financial industry) detected computer security breaches in the laps of twelve months [18]

These cyber threats can be subdivided into:

- Malware.
- Denial of Service.
- Unauthorized intrusions.
- Spoofing and phishing.

The perpetrators of these security threats may be classified into two groups:

- Insiders: authorized users who can exploit the system such as employee, contractors...
- External agents: none authorized, they exploit the internet ubiquity and anonymity to accomplish their objectives such as hackers, terrorists...

4.3.1. Malware

Viruses present a high risk on internet banking. Recent examples demonstrate it. For example, "Scandinavia's largest bank, Nordea, has become the biggest European victim of the MSBlast worm. The bank was forced to close 80 branches across Finland after the infection found its way into servers in all 440 of the bank's offices."[51]

Other viruses such as Blaster, Nachi and Sobig.F had a major impact on the banking sector. As example, in August 2003, in the Baltic's states, Latvijas Unibanka and Hansabank had to shut down their services even ATM after being hit.[18]

Another example is the BugBear.B virus that targets the financial institutions. The virus tried to steal passwords and other information to help attacker gain access to the bank's networks. "BugBear.B's affinity for banks is not a complete surprise. The virus contains a list of hundreds of domain names, apparently for forging spoofed e-mail addresses, many of them containing the names of banks"[52]

4.3.2. Denial of Service

Denial of service is another threat to Internet banking. It deprives legitimate users from accessing online services and undermines their confidence in Internet banking.

In March 15, 2000 a denial of service attack targeted NASDAQ stock exchange. Another example, in October 2002, where an attack was launched against the Internet's 13 root domain name (DNS) which converts complex internet protocol addressing codes into the words, names, web addresses we use.[52]

Viruses can also create a denial of service state by targeting computers around the world in order to use them for lunching a distributed denial of service attack

4.3.3. Unauthorized intrusions

Hackers present a high risk to financial institutions. Most unauthorized intrusions are aimed at stealing customer information or company secrets.

On July 20, 2003 an attack was conducted on ABSA the leading bank in South Africa. "All you have to know is someone's bank account number and their pin, and you can set up beneficiaries, pay money over, to your heart's content. A simple spyware was installed on victim's computers and the account numbers and PIN sent back to the perpetrator. This allowed the thief to steal approximately R500000 (about US$ 65000) from various victims." [47]

In September 2000, a British computer expert, Ralph Dressel, was able to get bank accounts detail of millions of American Internet banking customers through the website of the US company Fiserv. The company runs more than 200 million accounts online looking after more than £15bn of customers' money. He obtained something called the "access log" which had all the security information needed to access any of the internet accounts run by Fiserv.

Dressel said: "I was just checking details of my US bank account and was playing around looking to see how secure the system was. I was amazed there didn't seem to be any protection at all and within five minutes I had obtained full access to account details of hundreds of thousands of people. Anybody who has basic internet skills could have done it. I guess if I wanted to I could have transferred $50m into my account" [4]

4.3.4. Spoofing and phishing

Spoofing and phishing is an attack where a system is trying illicitly to impersonate another one. Customers can be diverted from the bank's web site and user names and passwords collected. This information can be later used to impersonate the legitimate users.

In Malaysia 92 phishing cases were reported between January 2004 and December 2004. To perpetrate these attacks spoofing techniques were used to gain names and passwords of

account holders. Victims were reported being deceived to a fake website where perpetrators stole their usernames and passwords and later used the collected information for their own advantage. [1]

4.4. Security Requirements

In order to face the risks and threats of internet banking, banks must ensure the adoption of a security policy that preserves the basic security requirements and characteristics in any electronic banking application. To provide adequately protected and authenticated transactions the following security requirements should be met: authentication, non repudiation, data and transaction integrity, confidentiality, and system availability [11, 33, 35, 45]

4.4.1. Authentication

Authentication is the process of verifying the identity of someone or something. It is commonly done through the use of passwords (something the user knows). Knowledge of the password is assumed to prove the user's identity. This process is intended to prevent unauthorized users from accessing data. The weakness of this system is that passwords can be stolen, revealed or forgotten. Strong authentication can be achieved through the use of tokens, biometrics and digital signature.

Authentication can also be defined by: "the verification of the authenticity of either a person or of data, e.g. a message may be authenticated to have been originated by its claimed source. Authentication techniques usually form the basis for all forms of access control to systems and / or data." [27]

4.4.2. Non Repudiation

The recipient must be able to prove that the customer had initiated the transaction and that this one cannot deny it and vice versa. This can be achieved through public key infrastructure, digital signature and Certification authorities.

Non repudiation can also be defined by: "All parties to a transaction must be confident that the transaction is secure and it is verified as final. Systems must ensure that no party can reject the transaction. To protect and ensure the digital trust, parties may employ digital signatures, which will not only validate the sender but will also time stamp the transaction so it cannot be claimed subsequently that the transaction was not authorized or not valid." [28].

4.4.3. Data and Transaction Integrity

Data and transaction integrity is the process of ensuring that the information processed, stored or transmitted between the bank and its customer had not been intentionally or

unintentionally tampered with or even replayed, i.e. the message is accurate, reliable, and complete.

It is achieved through the use of:

- Logical access security: preventive and detective measures that restrict a user's access to permitted data.
- Physical access: controls that grant selective physical access to specific individuals.
- Processing and transmission controls: controls associated with input, processing, communication, transmission, output, storage and retrieval of data.

4.4.4. Data Confidentiality

Confidentiality is the concept of protecting the data from unauthorized disclosure and allowing authorized access only. This principle ensures that only the recipient of the message can read it and no one else. It is usually achieved by:

- Using very well established encryption algorithms, which have undergo rigorous scrutiny and been approved by international community of cryptographers.
- Protecting cryptographic keys and their secrecy. No single individual knows the entire keys.
- Using hardware security modules and tamper resistant devices to carry out encryption and decryption functions

4.4.5. System Availability

Internet banking should be reliable in order to maintain public confidence. It should be available anytime, anywhere. All of the security requirements are of little value if an online service is not available when needed.

Banks should consider maintaining high system availability, adequate capacity, reliable performance, and recovery ability. The same is required from outsourced vendors.

Internet processing requires a number of complex interdependent system and network components. The entire system may become inoperable if a critical hardware is damaged or software module is malfunctioning.

Maintaining system availability is achieved through:

- The use of monitoring tools that track system performance, traffic volumes, transaction duration, and capacity utilization.
- Standby hardware, software and network components for fast recovery.

4.4.6. Requirements Summary

After having identified the security requirements of internet banking, a summary table is used to highlight the security requirements and their corresponding solutions that are to be adopted by banks providing Internet banking.

Table 4.1: Security requirements and corresponding solutions

Security Requirement	Solutions
Authentication	Use of passwords, tokens, biometrics and digital signature
Non repudiation	Digital signature and certification authority
Data and transaction integrity	- Logical access security (restrict user access to only data/information needed) - Physical access security - Processing and transaction controls
Data confidentiality	- Encryption algorithm (international standards, accepted by international community of cryptographers) - Protecting cryptographic keys and their secrecy - Hardware security modules and tamper resistant devices
System availability	- Monitoring tools to track system performance - Standby hardware, software and network components

Chapter 5

Internal Security Practices in Banking Environment

This chapter will describe different in house risk management, such as providing good internal practices and principles to reduce and limit risks from both internal and external threats.

5.1. Risk Management

Risk management is a key security practice, it can be considered the milestone used to determine the level of security needed and applied. It is the bank's responsibility to perform risk identification and assessment by studying the different types of risk, analyzing their impact and identifying appropriate measures to reduce or even eliminate them. Risk control procedures as well as security practices and measures should be put in place before implementing Internet banking. By its nature, that is money, special characteristics exist for internet banking. [9, 11, 54]

As a guideline for risk management regarding electronic banking, banks can refer to the Basel's committee recommendations "Risk management principles in electronic banking" (May 2001 and July 2003 or 14 principles). These principles are divided into 3 major categories:

- Board and management oversight: It is the board's responsibility to establish specific accountability policies and controls to manage internet banking risks (internal or outsourced). Appropriate risk analysis is to be performed in order to be mitigated and monitored. The security policy is regularly reviewed to be compliant with the evolving technology and changing customer requirements.
- Security controls: Operational risks are to be monitored. This can be applied by providing the basic security requirements such as authentication, non repudiation, data integrity, confidentiality. Clear audit trails for all transactions, separation of duties, and clear access privileges are to be ensured. It is the bank's responsibility to evaluate Internet banking technologies and products, and to determine the appropriate mix (cost/security) for the bank.
- Legal and reputational risk management: It is the bank's responsibility to maintain customer privacy and business continuity. For this, recovery and continuity planning is required as well as customer education. Clear information about the bank, its privacy policies, and disclaimers are required on the bank's web site. Any breach or suspect behavior should be documented, studied, evaluated and appropriate risk monitored.

5.2. Human Resource Management

In security, human management is very important. The security of the system relies on a very small group of personnel that should be skilled, well trained, controlled and trusted.

Very stringent criteria should be applied in order to select the personnel responsible of internet and security functions. The same can be applied to the personnel responsible of developing, implementing and maintaining websites and systems. Up to date training should be enforced.

According to a study conducted by Mr. Fuad W. Awad [22] in February 2000, in addition to in house training, banks in Lebanon can benefit from training programs provided by professional associations and training institutions with material in different banking activities including information technology. To state some:

- Association of banks in Lebanon (ABL): established in 1959. The association provides conferences, seminars, workshops as well as in house training. The training department cooperates with the member banks to understand the needs of the human resource and conduct appropriate trainings.
- Union of Arab banks: established in 1974. It provides conference, seminars and training programs for bank delegates. It targets the need of the Arab word in general and not specifically the needs of Lebanese market.
- Arab academy for banking and finance: it has offices in most of the Arab countries including Beirut, and targets the need of the Arab world.
- The center for banking studies: joint venture between the ABL and Universite Saint Joseph. It provides employees of the Lebanese banking sector with a professional banking and financial training.
- TEAM International: established in Lebanon1975. It is one of the largest engineering and management consulting firms in the Arab world.
- Starmanship: a private training and development firm established in 1996.

Internal attack by trusted personnel is one of the serious risks a bank can face. To minimize this risk, the following basic security principles should be applied: [14, 45, 54]

- Never alone principle: Certain functions are so critical that they should be performed by more than one person such as system initialization, network security configuration, contingency plans, firewall implementation, creating passwords, etc. No one should know the total value in clear of a key.
- Separation of duties: Processes should be enforced in such a way that no one person can initiate, approve and execute any transaction that can jeopardize neither the integrity nor the security of a system. Examples of such responsibilities and duties that should be performed by different groups are: database administration, security administration, data security, librarian and backup data file custody, system design an development...

- Access control principles: Only employees with proper authorization should be allowed to access confidential information and use system resources. Employee termination and transfer procedures should be implemented and documented. It is very important to restrict access rights according to job responsibilities and requirements, thus detailed job roles should be defined: employee access rights are restricted to process functions and data files required for his normal duties. Another important practice is to ensure that no person, by virtue of rank, can have access to confidential data or system resources.

It is also important to note that, external personnel from third party also provide a risk of internal attack. Thus their access should be monitored and restricted.

5.3. Outsourcing

It is the bank's responsibility to ensure that their service providers are able to deliver required services with the appropriate level of security, performance and reliability.

It is important to determine the service provider's capability, reliability and viability. This can be performed by reviews including risk analysis of the provider's financial strength, reputation, risk management policies and control, and the ability to fulfill his obligations. Banks should be able to audit the financial position either directly or by another party. Properly defined agreement is mandatory covering responsibilities, service level, availability, security, contingency planning, backup procedures, and customer protection to monitor the service provider. [11, 14, 16, 45]

As example of these agreements and requirements:

- Escrow agreement used to protect banks in case service provider is out of business. Periodic, up to date, documentation is also required.
- Access, ownership, privacy and control of confidential information such as customer information.
- Backup procedure.
- Subcontractor's responsibilities: if the bank allows the service provider to subcontract other companies then the subcontractor's responsibilities should be identified and cleared by the bank.
- Security measures: The security procedures followed by the service provider should be at least at the same level used by the bank.
- Hardware and software upgrades.
- Audit over financial reports.
- Audit over security, internal controls and contingency plans used by the server provider.
- Activity logs (audit trail) to monitor vendor's access to the system.
- Define performance expectations, under both normal and contingency circumstances.
- Training for bank's personnel.

5.4. Recovery and Business Continuity

In such a critical business, recovery and business continuity are very important. The required speed of recovery depends on the type of online services available, and the need to maintain continuity of services for the customers, thus maintaining the customer's confidence.[9, 45]

Banks should have a team responsible for managing recovery and assessing the financial impact of risks in both cases: inside production or outsourcing. Recovery and contingency plans should be revised, tested and evaluated periodically. They should be updated as soon as the business, network, system or operating environment changes.

Example of contingency plans:

- Plan to contain and recover form a denial of service attack, allowing bank to restore normal operations swiftly and effectively in case of occurrence of such an attack.
- Plan to recover from hardware, software, communication failures as well as data tampering.
- Monitor performance criteria, to ensure that systems can handle high and low transaction volume with the appropriate system performance and capacity.
- Develop processes to manage demand in case the system appears to reach defined capacity checkpoints or network traffic, etc.

Chapter 6

Operational Security Practices in Banking Environment

Internet banking is a growing area of concern for banks in managing daily operational risks. This chapter treats Internet banking security with respective to technology addressing specifically the areas of authentication, network security and customer awareness.

6.1. Authentication

Authentication is the process by which, in our case, banks determine whether the user is legitimate and has the authorization to access data and conduct transactions.

To provide secure internet banking, strong authentication is crucial. Effective authentication reduces fraud, limits unauthorized access, helps preventing money laundering and enforces electronic agreements.

In this section, different authentication mechanisms are described (fixed and dynamic passwords, challenge/response, digital signatures, and hardware tokens) along with registration and monitoring.

6.1.1. Authentication Mechanisms

Different authentication mechanisms exist. They are based on one or a combination of 3 basic factors that are: know, has, is. [20, 34, 35, 38]

The authentication methods that can be used in internet banking are: fixed passwords, dynamic passwords, challenge/response, digital signatures, and hardware tokens.

6.1.1.1. Fixed Passwords

Fixed passwords are widely used in internet banking. Systems require users to enter user name or id and corresponding password. This method is as a single factor authentication technique, as it relies only on something the user knows. This is commonly used in internet banking authentication mechanism as passwords are easy to implement and use and provide mobility for the users.

To enhance the security, without implementing a multiple factor technique, systems could be tiered. A tiered single factor authentication system would include the use of two or more passwords at different points in the authentication process [20]. Note that passwords should never be sent in clear over the network.

Fixed passwords are vulnerable to dictionary attack, password guessing and social engineering thus do not provide a real level of non repudiation. Banks should consider some basics when implementing them for authentication, such as:

- Select adequate password length and composition: at least 6 characters with combination of letters and numbers.
- Force password change every period of time.
- Lock users after an excessive number of failed login attempts.
- Review password exception reports.
- Provide guidance to customers on password selection. (Avoid easily guessed passwords: names, date of birth, phone number, words).
- Implement secure process for password generation and distribution.
- Encrypt passwords with at least 128 bit encryption key when stored or while in transit over the Internet.

6.1.1.2. Dynamic Passwords

Banks can issue to their customers a list of one time passwords also known as "scratch list number". Each password is used once. This is more secure than the fixed password as even if guessed, stolen or intercepted, the password could not be used for later authentication. But still this method is a single factor authentication mechanism. Its major drawback is that the list is difficult to memorize and users might find themselves saving the file on their systems.

6.1.1.3. Challenge/Response

In challenge/response method, the customer proves his identity to the bank not by sending the password, but by demonstrating the knowledge of the secret. This is done through the proper response to a random challenge sent to the customer.

There are two challenge response methods:

- Symmetric challenge/response: such as sending the time.
- Asymmetric challenge/response: use of digital signature to sign the challenge

6.1.1.4. Digital Signatures and Certificates

Digital signature can provide a strong customer authentication, non repudiation and confidentiality. To implement digital signature, banks usually use their own implementation, stand-alone application or applet.

Digital signature minimizes many of the vulnerabilities of fixed passwords, but it is more complicated and costly to implement. When using digital signature, banks should consider:

- Select appropriate certificate validity.
- Update regularly the revoked certificates list.
- Define circumstances for revoking certificates.

6.1.1.5. Hardware Tokens

At the difference of all the previous mechanisms, hardware tokens add the factor of something the customer has. This a two-factor authentication process where password and token form these factors.

Several of the previously described mechanisms can be implemented using tokens. Hardware tokens provide mobility as users can carry them. Different kinds of tokens exist:

- Memory/microprocessor tokens: these tokens contain the authentication data stored in magnetic, electronic or optical form. In addition to memory, microprocessor tokens contain processors and implement encryption on the card. Example private digital signature keys can be kept on smart cards. Saving the key on the token would prevent unauthorized parties from accessing the user's computer and copying the key.
- Password generators: these tokens include hardware calculator to generate one time passwords, and calculators to generate response to the server's challenge.

Note that to provide security for the whole system, each token should hold a different cryptographic key. When using public key this is not a problem. But the problem exists in case of symmetric keys. In order to reduce the overhead of maintaining a secure database for all the keys, symmetric keys can be derived from the unique serial number of the token and a common master key.

When utilizing tokens, the following should be considered:

- Educate customers to protect tokens.
- Design and implement a secure process for generation and distributing tokens.
- Determine an appropriate expiry date and renewal process.

6.1.2. Registration

Registration is the first step in online banking. If something goes wrong at this stage it would compromise the security of the whole system. Usually an initial password is issued by the bank and delivered physically to the user or through paper mail. Sometimes, user authentication by phone is required at the first login.

6.1.3. Monitoring

Monitoring is used by banks to detect unauthorized access to computer systems and customer accounts. Example sending alerts if certain transactions do not match the user's regular profile or unusual activities are detected such as money laundering. Audit logs are used to identify unauthorized activities, detect intrusions or reconstruct events.

6.2. Network Security

6.2.1. Export Restrictions

Historically U.S restricted the export of strong cryptography in common browsers. The length of symmetric cryptographic key was limited to 40 bits, as for asymmetric keys RSA were limited to 512 bits.

Electronic banking relied on external implementations of SSL to provide strong cryptography within applets or applications. This restriction was removed since the beginning of year 2000. [34, 35]

6.2.2. History of Internet Banking Architecture

Historically, Internet banking architecture can be classified into three methods to connect the user and the bank. These methods are: [23, 35]

- Stand alone client/server applications: due to the U.S. export restrictions, banks had to provide their customers with stronger security by using stand alone applications. But banks were faced with the problem of distributing the software and updates.
- Java applets: the applets provide the communication security. The advantage of this approach is that it is easy to maintain and update the client's software, hence reducing the overhead of distributing the software.
- Existing browser: used nowadays, the existing browsers such as internet explorer and Netscape are used. Https is used as the communication protocol. Communication security is provided by the SSL protocol which is now built in into the browser.

6.2.3. Communication Security

The http protocol does not provide the security requirements of internet banking that is: entity authentication, data authentication, data confidentiality and non repudiation. The solution that is used by almost all electronic banking systems is the SSL/TLS protocol. The communication between the browser and the server is secured at the transportation layer by the SSL protocol. SSL provides entity authentication, data authentication and data confidentiality but not non repudiation. To provide non repudiation, banks should implement mechanisms such as the use of digital signature on client data. Note that this is rarely done in practice [35].

6.2.3.1. Secure Socket Layer

The SSL protocol provides a secure communication between the client and the bank. It is inserted above TCP/IP and below the application protocol such as HTTP or IMAP. This structure preserves the use of TCP/IP on behalf of higher levels (flow control,

reliability...), allowing in the same time the establishment of authentication (server, client) and encrypted connection. [31].

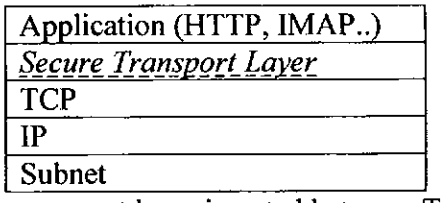


Fig.6.1: Secure transport layer inserted between TCP and Application layer

The SSL protocol is broken into:

- Handshake protocol: used to establish the connection between parties, by authenticating both server and client, exchanging certificates between parties if required (i.e. credit card purchase), allowing the selection of cryptographic algorithms supported by both sides (example select symmetric key encryption as it require less computational time)...
- Record protocol: used for data transfer. It defines a set of procedures by which data is passed from the application layer like, enforce data encryption, block size, integrity check (use of hash function)...

6.2.3.2. Security Flaws in SSL

Both SSL 2.0 and 3.0 are still used in browsers. This section is addressing the flaws that can be exploited in these versions.

Security Flaws in SSL 2.0

Despite the fact that it is an older version of SSL, it is enabled by default in most standard browsers. SSL2.0 contains a number of security flaws. Some of these security problems [25, 34]:

- Message authentication and encryption use the same cryptographic key, i.e. the security of the MAC is weakened
- A truncation attack is possible, as it simply uses the TCP connection close (FIN) to indicate the end of data. An attacker can forge the FIN and the recipient cannot tell that it is not the legitimate end of data.
- Person in the middle attack cannot be detected, as no protection exists in the handshake protocol.

Security Flaws in SSL 3.0

SSL3.0 is the new version of SSL. It was adopted, with some improvements, by the IETF working group and was published as Transport Layer Security TLS 1.0. The difference between SSL 3.0 and TLS are negligible.

But still some problems do exist [25, 34]:

- Downgrade attack: SSL/TLS supports both weak and strong cipher suite and it allows browser and server to negotiate the desired one. An entity in the middle can influence this negotiation and enforce the use of the weak suite before the handshake is completed.
- Version rollback attack: most SSL 3.0 implementations are able to handle SSL 2.0 connections. An attacker can modify the client's hello to look like SSL 2.0 in order to exploit its well known weaknesses, vulnerabilities. Further more, if multiple versions are supported by browser and server, the attacker will also try to force the usage of SSL 2.0.

Today's browsers implement SSL/TLS by default: Netscape 6.x and Microsoft Internet Explorer 5 and 6 support both SSL and TLS.

6.2.4. Operating Systems

The operating system is an important pillar in the security of the system. If not securely configured or if it contains bugs it can be used to threaten the security of the whole system. Operating systems and software should be updated on a regular basis to patch up security deficiencies that may be discovered from time to time.

Currently most operating systems can not be considered secure. There is no segregation between users and data. Software applications have access to all system resources. This is also true for malicious programs such as viruses, Trojan horses and worms. These programs can steal passwords, tamper with the installed root certificate, spoof the user interface even intercept the communication before it is securely established. [23, 34, 35]

6.2.5. Trust Anchors

Only if they have genuine copy of the browser, stand alone application, digitally signed java applets users can trust the correct execution and interface of internet banking applications.

Authentication cannot be performed without authentic root certificates. The entity's name and its public key are put into an X.509 certificate which is signed by a certification authority. Users need them in order to verify the bank's certificate during SSL/TLS authentication and in order to verify digitally signed applets. Certificates should not be issued without rigorously checking the identity of the individual requesting the certificate. Certificate revocation list (CRL) should be periodically updated and checked. The status of the certificate can also be checked online using the Online Certificate Protocol (OCSP). [34, 35]

On the other hand, users must be able to recognize when they have a secure session with the bank. Unfortunately, limited visual indicators exist such as closed clock and inexperienced users are easily fooled by a spoofed web site.

6.2.6. Firewalls

Firewalls are used to filter the traffic between protected network and a less trustworthy one (outside). They can prevent access from outside, or allow access from certain places, certain users or certain activities. Note that a firewall can protect an environment only if it controls the whole perimeter.

Some controls for firewalls in internet banking [54]:

- Internet banking is delivered through suitable and dedicated firewall architecture.
- Penetration testing is conducted regularly. Weaknesses are reported, evaluated and acted on.
- Automated tools are used to highlight log entries that suggest a penetration attempt.
- Multiple unsuccessful login attempts are logged.
- Implement audit trails.
- Logs are stored off the firewall system and reviewed for both successful and unsuccessful attempts to penetrate security.
- Firewall application system is updated with patches and other bug fixes in a timely fashion.
- Changes to firewall applications are tested before migration to the production firewall system, and impact assessment is performed to ensure that new vulnerabilities are not exposed.
- Customer's access is restricted to a virtual private network (VPN).

6.2.7. Intrusion Detection

Prevention although necessary is not a complete security control. In addition, detection during an incident is important. This is done through intrusion detection systems (IDS) that monitors the activity to identify, and detect malicious or suspicious events.

IDS is a post-event security device. It may be able to notify that someone has compromised the system, but it may not be able to stop the compromise.

6.2.8. Virus scanners

Virus scanners should be updated daily. Fileservers should be set to active scanning mode where they scan every file copied onto them. Desktop scanners that protect the user's PC should also be updated. As for attachments, they should be filtered (executable, .doc files) and scanned. System administrator should subscribe to mailing list to receive early warnings of malicious codes (www.cert.org, www.nipc.gov, listserv@netspace.com, etc).

6.3. Customer Awareness

In internet banking applications, customer's PC can be considered a weak point. And, as it is well established, the security of a whole system is as high as the security of the weakest element. Even when secure communication between personal computers and banks are established it can be bypassed if the platform used by the customer is unsecured. The threat can mainly arise from human errors and vulnerable client's platform. Not all customers are aware of security problems, and, from this ignorance come very high risks. This leads us to the importance of customer education.

Banks should inform their customers about probable threats and provide them with adequate help and maintenance. This can be done through providing, on the web site, the following information [8, 9, 21, 23, 45, 49]:

- Head office location and contact number (same for local offices).
- The identity of the bank's head office supervisory authority.
- Contact to customer service regarding problems, complaints and suspected misuse of accounts.
- Informing customers about the bank's privacy policy.
- Disclaimers on the security of external links.
- Disclaimers regarding emails where the client is informed about the good practice of not sending sensitive information regarding his account using mail (not even to bank).
- Inform customers on good practices to password selection (length, alphanumeric, not easy to guess, avoid personal information ...) and protection (memorize password, change regularly, not to be used for different web sites, etc).
- Inform customers to upgrade their browsers and application software to support SSL-128 encryption or higher.
- Inform customers to check that the web site address changes from http:// to https://, and the appearance of the security icon that looks like a lock or key.
- Provide customers with information regarding the general security practices to protect their PCs. (antivirus, personal firewall, log off, delete junk mail, do not open email attachments from strangers, do not run unknown software, etc).
- Advice customers not to use un-trusted computers (internet café, public computers, etc).
- Advice customers to not disclose personal, financial or credit card information to suspect or little known websites.

Chapter 7

Survey Results

To complete the study of Internet banking in Lebanon, two questionnaires were proposed: the first directed towards customers, while the second towards banks. The questionnaires can be found respectively in appendix 1 and 2.

7.1. Customer's Survey Results

The questionnaire's main objective is to evaluate security awareness and practices among Internet banking users in Lebanon. To achieve this goal, the questionnaire was divided into two parts:

- The first, directed towards Internet banking users referred to as "registered users" to evaluate customer's perspectives, frequency of usage, specific services used, security awareness and practices.
- The second, directed towards non Internet banking users referred to as "non registered users" to identify the reasons behind their choice emphasizing security concerns.

From the distributed questionnaire between both users (registered and non registered) 40 were answered and analyzed below.

7.1.1. Survey Results – Registered Users

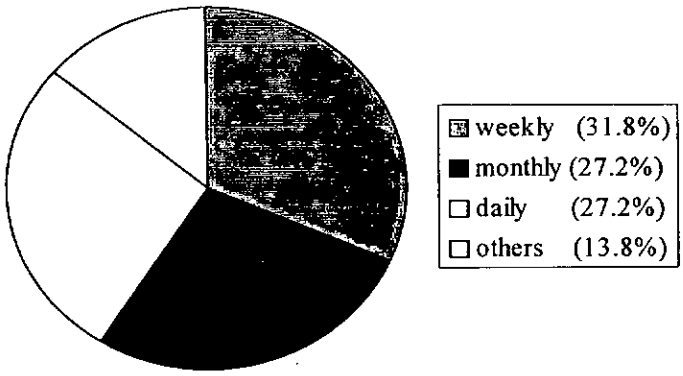
According to banks, registered users percentage should be between 7 and 20%. According to the survey, using judgment sampling, the registered users' percentage reached 55%; this difference is related to the level of education of the surveyed users.

72% out of the registered users were introduced to Internet banking through their banks, while the remaining 28% were introduced through their friends.

Convenience is the main reason of using Internet banking. This is due to the fact that banking services are available anywhere, anytime which makes it easier to maintain transaction activity.
Curiosity is another reason to register to Internet banking even if it only represents 14% of the registered users.

The frequency usage of Internet banking varies between users; the figure 7.1 hereafter represents percentages according to each frequency.

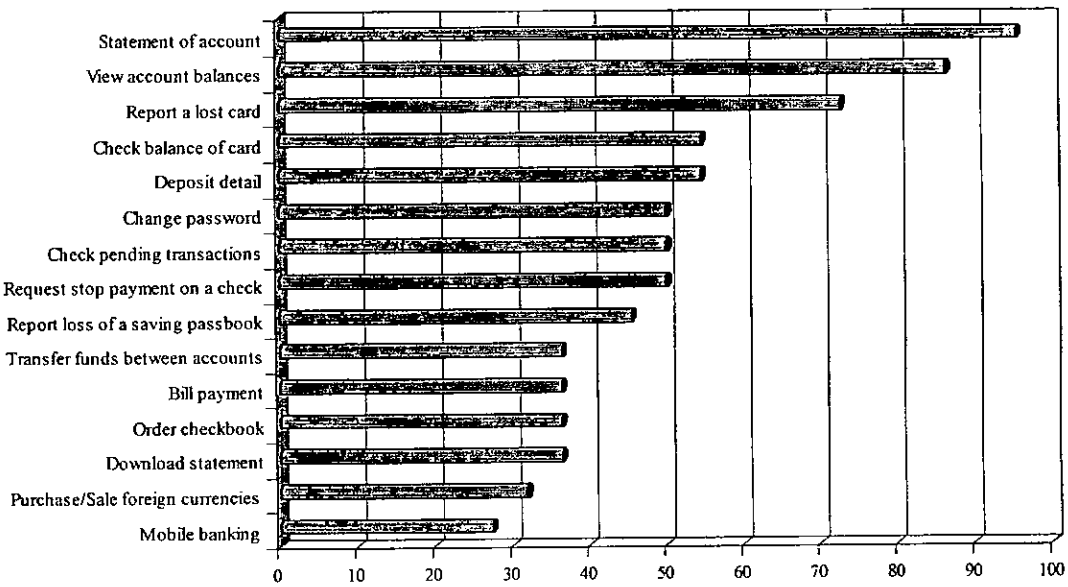
Figure 7.1: Frequency of usage of internet banking by Lebanese customers.



The most frequently used services in Internet banking are check account balances and statement of accounts, where they are considered the most important. Afterwards come card management, report loss card and check balance. At last, mobile banking is the less frequently used. This is demonstrated in figure 7.2.

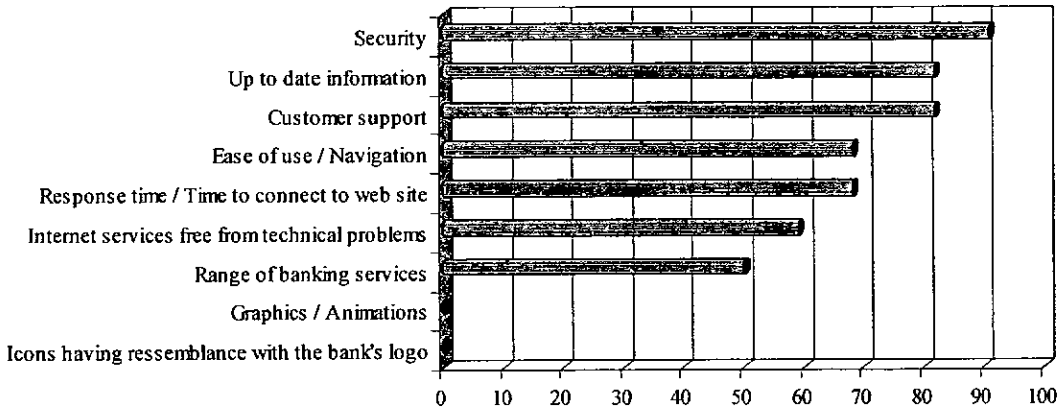
It is important to note that all users find internet banking easy to use.

Figure 7.2: Percentage of usage of services provided through the Internet



Security is the most important characteristic of Internet banking, while animation, graphics and icons resembling the bank's logo have no importance for users. The rating is shown in figure 7.3 hereafter.

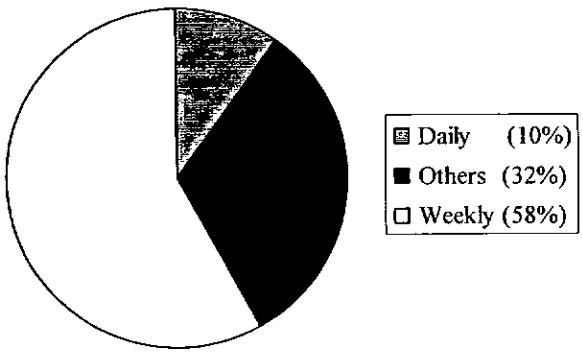
Figure 7.3: Criteria importance according to Lebanese market.



As of security awareness and practices, they can be summarized as follows:

- No user accesses Internet banking using public computers; they all access their accounts either from home or work.
- 86% of registered users have anti-virus software on their system. But not all of them update their virus list on a timely basis. Figure 7.4 is used to visualize the frequency of updates. The high percentage 32% of users with irregular updates reduces the percentage of systems protected by anti-virus software to 59%.
- 63% use personal firewall.
- 23% install software or run programs from unknown origin
- 5% open email attachment from strangers.

Figure 7.4: Frequency of virus list update among Lebanese users.



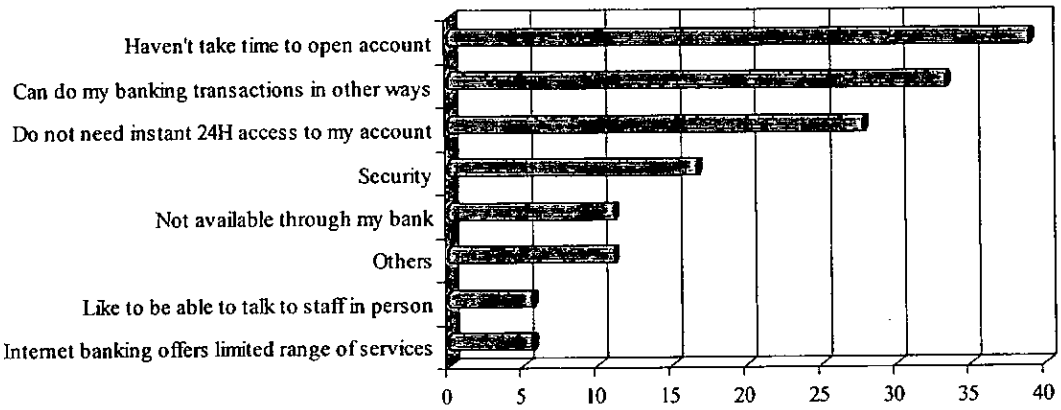
Although users are aware of the risks of using public computers, avoid junk mails and attachments from strangers, they do require awareness especially in the case of virus list update.

7.1.2. Survey's Results – Non Registered Users

The "non registered users" percentage is 45%; half of them are considering registering in Internet banking services.

Figure 7.5 shows the reasons for not registering in Internet banking services as classified by users.

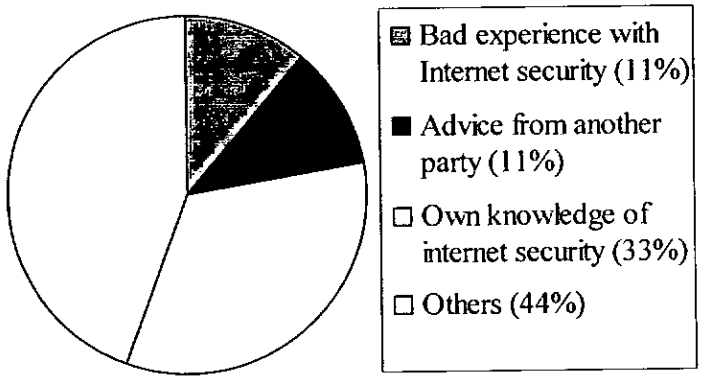
Figure 7.5: Reasons for not registering in Internet banking



For those who did not register in Internet banking for security reasons, they fear that other people may gain access to their personal data (67%), while only 10% fear intruders stealing money from their accounts.

The basis for these doubts were either not identified or based on user's own knowledge of Internet security. The percentages of doubt reasons are shown in figure 7.6.

Figure 7.6: Percentage of basis for doubt in security of Internet banking



From the users who are not considering registering in Internet banking, 33% are willing to in case banks use hardware tokens.

7.2. Bank's Survey Results

The purpose of this questionnaire is to evaluate Internet banking in Lebanon and to which extend it complies with the Basel's Committee requirements (May 2001 and July 2003) found in appendix 1.

It is important to note that not all issues were addressed and focus was mainly towards operational risk management. To achieve this goal, the questionnaire was divided into 3 parts:

- The first part addresses general information, determine the history of Internet banking as well as the reasons behind it.
- The second and third parts address web sites and transactional activities to identify security measures implemented in order to manage operational, legal and outsourcing risks.

Only 4 banks answered this questionnaire, they are: Audi Bank, Bank of Beirut and Arab Countries, Banque du Liban et d'Outre Mer, Credit Libanais.

7.2.1. Survey Results – General Information

Internet banking appeared in Lebanon since year 1997 and is evolving. Most of the banks started offering these services in the range of the 5 past years.

Only 13 banks offer Internet banking in Lebanon with interactive and transactional web sites. They are, in alphabetical order: Al Mawarid, Arab bank, Audi bank, Bank of Beirut and Arab Countries, Banque Libano-Francaise, Banque du Liban et d'Outre Mer, Banque Nationale de Paris Intercontinentale, Bank of Beirut, Credit Libanais, HSBC, National Bank of Kuwait, Saradar and Societe Generale de Banque au Liban.

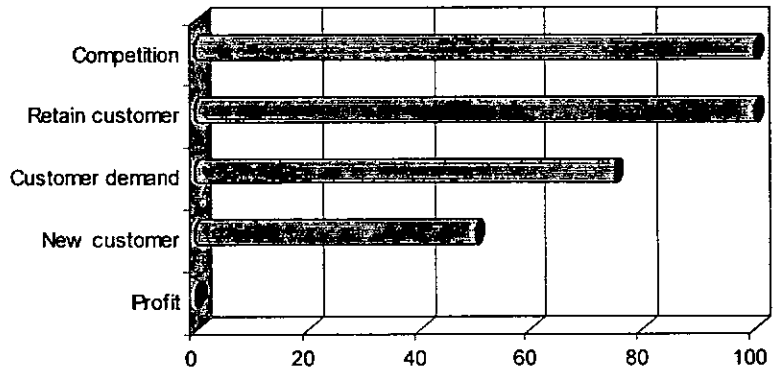
All of these banks provide their customers with the basic services: balances, statements and transfer between accounts (refer to table 2.2 in chapter 2 for more details).

4 banks are planning to provide transactional web sites in the near future. They are: Al Baraka, Byblos Bank, Credit Bank and Lebanese Canadian Bank.

Despite the fact that mobile banking (WAP and SMS) has also been offered in the same range, it is not widely available, and is only offered by 3 banks. They are: Banque du Liban et d'Outre-Mer, Credit Libanais and National Bank of Kuwait.

According to the bank's answers, they opted to provide Internet banking services mainly for competition and to retain customers, this is clearly shown in figure 7.7 hereafter.

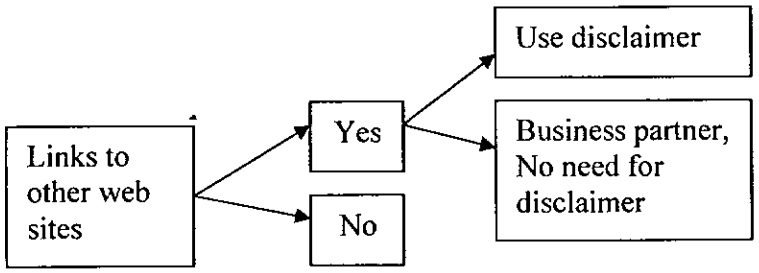
Figure 7.7: Reasons for offering Internet banking



7.2.2. Survey Results – Legal Risk and Customer Awareness

Not all banks are presenting links to other web sites. As for the ones that do so, disclaimers are present when the links are not for business partners. This is shown in detail in figure 7.8.

Figure 7.8: Disclaimers and external web sites



All the addressed banks allow email contact on their sites but only 25% of them provide disclosures about inclusion of sensitive information.

All of the banks conduct screen testing to ensure user friendliness. As for customer support and awareness, all respondents offer their customers support using different procedures to respond to demands, problems and complaints.

When provided, customer security awareness notification is presented either online or offline through documents.

7.2.3. Survey Results - Outsourcing

The banks that are outsourcing companies for Internet banking services, select the outsourced service provider based on its reputation, financial strength, viability, reliability and security features.

All the banks stated that they:

- Restrict third party's access to relevant and necessary customer data
- Conduct user acceptance test prior to the implementation of any software modifications or enhancements
- Use software escrow agreements, and keep up to date documentation

7.2.4. Survey Results - Operational

The main objective of the questionnaire is the operational risk management subject. Note that most of the banks' answers related to this subject were almost similar.

The common answers are:

- Measures to prevent site alteration
- Controls to restrict physical access to computer hardware, software and communication equipment
- Protection of hardware and phone lines from power surges, lightning strikes ...
- Automatic log off for inactivity period
- Access disabled in case of excessive failed login
- Protect customer passwords: employee do not have access to passwords
- Safeguards to detect and prevent duplicate transactions
- Use digital certificates
- Use digital signatures
- Use 128 bit SSL encryption
- All unused services are blocked at the firewall
- Training to IT personnel
- Training to other employee
- Dollar limits per transaction time period
- Contingency plan to recover from hardware, software, communication links and data files.
- Software updates and patches are tested before implementation
- Penetration testing conducted, either internally or by third party.

- Virus list updates are done on regular basis

The main difference is in the authentication procedure adopted by banks. Different methods are found in the Lebanese market, listed below in ascending security strength and cost:

- Single factor
- Tiered single factor
- PKI
- RSA secure Id token

Similarly, password criteria and restrictions vary, details can be found in table 7.1 hereafter.

Table 7.1: Password criteria and restrictions used.

Characteristics		Percentage
Minimum length	6 characters	50%
	8 characters	50%
Alphanumeric	Enforced	25%
	Not enforced	75%
Change	Required	50%
	Not required	50%
Customer information for password selection	Yes	25%
	No	75%
Other restrictions	Reject last passwords	
Inactivity period	5 minutes	50%
	10 minutes	50%
Excessive failed attempts	3 times	75%
	4 times	25%

7.3. Summary

In table 4.1 in chapter 4, the security requirements of Internet banking have been identified with corresponding proposed solutions.
Comparing the survey's result to table 4.1, the following table 7.2 states the applied solutions in Lebanon.

Table 7.2: Security requirements and applied solutions

Security Requirement	Proposed Solutions	Applied Solutions
Authentication	Use of passwords, tokens, biometrics and digital signature	- Passwords (single factor, tiered single factor, PKI) - Tokens (RSA secure ID)
Non repudiation	- Digital signature - Certification authority	- Digital signature - Digital certificates
Data and transaction integrity	- Logical access security (restrict user access to only data/information needed) - Physical access security - Processing and transaction controls	- Restrict third party access to relevant and necessary customer data - Controls to restrict physical access to computer hardware, software and communication equipment - Safeguards to detect and prevent duplicate transactions - Contingency plan to recover data files.
Data confidentiality	- Encryption algorithm (international standards,) - Protecting cryptographic keys and their secrecy - Hardware security modules and tamper resistant devices	- Use SSL 128 bit encryption - Protect customer passwords - Firewall - Penetration testing is conducted either internally or by third party.
System availability	- Monitoring tools to track system performance - Standby hardware, software and network components	- Measures to prevent site alteration - Protection of hardware and phone lines from power surges, lightning strikes etc. - Contingency plan to recover from hardware, software, and communication links.

7.4. Discussion and Recommendations

According to the survey, Lebanese banks are already implementing most of the requirements of Basel Committee risk management regarding electronic banking. Note that the survey was not exhaustive but addressed the basic security issues in:

- Legal risks management
- Promoting customer awareness
- Outsourcing
- Operational management: authentication, communication security, alteration prevention, penetration testing etc.

In addition, some areas were considered confidential hence not answered in details.

To be compliant with the recommendations does not mean that banks will not face computer related crimes, but to be able to reduce risks, and manage them effectively. One of the banks stated that it already faced such activities.

On the 30 of March of year 2000, the central bank issued a decision holding the number 7548 [6] in order to introduce measures to control financial and banking transactions effected through electronic means. This contains all operations and activities that are concluded, carried out, or promoted through electronic or photo-electric means such as telephone, computer, Internet, ATM, etc.

This decision provides that a bank or any institution supervised by the central bank wishing to conduct electronically any of its previously approved activities should notify the central bank in advance giving it the opportunity to consider the institution's compliance with norms of transparency, integrity and security.

On the other hand, the central bank is undertaking an initiative named Secure Electronic Banking and Information for Lebanon (SeBIL) in order to provide a secure platform for electronic banking and e-services for Lebanon's financial sector. SeBIL is the mechanism to meet the existing and future financial and banking sector's requirement in Lebanon.
The project started at the end of year 2003 and is expected to finish at the end of year 2005.

This project proposes a Secure Information Technology Infrastructure (SITI), which includes all the mechanisms for secure communication including firewalls, encryption, and access control based on PKI. The central bank will be hosting the public keys of the banks, hence becoming a certification authority in Lebanon.

SITI addresses the basic security requirements of Internet banking i.e. confidentiality, integrity, authentication, non-repudiation and availability.

Currently, there are neither restrictions on the encryption, nor an existing electronic signature system but these will be addressed in the SITI project.

Lebanese banks use a variety of strong authentication to serve their customers going from single factor authentication towards the use of tokens.

As for the customers, which can be considered the weak entity in this model, education in anti virus list updates is required, or circumvented by the use of double factor authentication.

In parallel, the government is trying to elevate the Information and communication technology (ICT) factor of Lebanon by introducing information technology into the curriculum, drafting laws, etc.

More banks are needed to promote competition and keep the pressure on enhancing services and their security in the Lebanese market.

This study addresses only one aspect of Internet banking, further studies could consider role based access control in electronic banking, regulations, payment system security, and mobile banking, etc.

Bibliography

1 Ahmad Nasir Mohd Zin,Zahri Yunos, *Security issues in Internet banking: how to make it secure*, 2004, National ICT Security and Emergency Response Centre (NISER). <http://www.niser.org.my/resources/internet_banking.pdf>

2 Akram Najjar, Salam Yamout, Kamal Siblini, October 2003, *The national strategy for Lebanon. <http://www.e-gateway.gov.lb/docs/OMSAR/estrategy/ Document%203%20-%20eReadiness%20Assessment%20.pdf>*

3 Alain Hiltgen, Thorsten Kramp, Thomas Weigold, September 2004, *Secure Internet banking authentication.* <http://www.zurich.ibm.com/pdf/csc/SecureInternetbankingAuthentication.pdf>

4 Antony Barnett, September 2000, *New blow to internet banking security*, The Observer. <http://www.guardian.co.uk/internetnews/story/0,7369,372676,00.html>

5 Banque du Liban, *Banque du Liban - SeBIL-SITI Strategic Vision for SeBIL* <http://www.bdl.gov.lb/sebil/vision.htm>

6 Banque du Liban, *Circular no 1810 - Electronic Banking and Financial Transactions* <http://www.bdl.gov.lb/circ/en/circ1810.htm>

7 Basel Committee for banking supervision, July 2003, *Risk management for electronic banquing*. <http://www.bis.org/>

8 Basel Committee for banking supervision, March 1998, *Risk management for electronic banking and electronic money activities*. <http://www.bis.org/>

9 Basel committee for banking supervision, May 2001, *Risk management for electronic banking and electronic money activities*. <http://www.bis.org/>

10 Basel Committee for banking supervision, October 2000, *Electronic banking group initiatives and white papers*. <http://www.bis.org/>

11 Central bank of Nigeria, February 2003, *Report of the technical committee on electronic banking*. <http://www.cenbank.org/out/publications/BSD/2003/e-bankingrpt.pdf>

12 Charles P. Pfleeger, Shari Lawrence Pfleeger, *Security in Computing*. 3rd edition. Prentice Hall, 2003.

13 Chen Li, Claus Pahl, *Security in the web service framework*, Dublin City University. Communication of the ACM.

14 Comptroller of the Currency Administrator of National Banks, October 1999, Controller's handbook. http://www.occ.treas.gov/netbank/ebguide.htm>

15 David McGuire and Brian Krebs, October 2002, *Attack on Internet called largest ever*, Washigton Post. <http://www.securtyfocus.com/news/1413>

16 Electronic banking questionnaire, 2004, <http://www.idob.state.ia.us/bank/docs/ applica/bank/elecbankquest.doc>

17 Electronic banking, April 2000. <http:// ://www.banking.state.tx.us/ PODES/ Procedures/ebank.pdf>

18 Eric Goetz, September 2003, *Survey and analysis of security issues in the U.S. banking and finance sector*, Dartmouth College.

19 Escwa, October 2003, *Profile of the information society in the republic of Lebanon <http://www.escwa.org.lb/wsis/reports/docs/Lebanon-E.pdf>*

20 Federal financial institutions examination council, August 2001, *Authentication in an electronic banking environment.* <http://www.ffiec.gov/ffiecinfobase/resources/elect_bank/frb-sr-01-20-ffiec-guidance_authentication.pdf>

21 Fernando de la Puente, Santiago GonzPlez, Juan D. Sandoval and Pablo Hernandez, June 2000, *Viral attack to internet banking applications*, IEEE AES systems magazine.

22 Fuad w.Awad, February 2000, *Inventory of Lebanese training institutions in management and finance*, LAU. <http://www.usaidlebaon.org.lb/files/bs1.pdf>

23 Galli, Musa, Turan, May 2000, *Internet banking how secure is it?* Oregon state University. <http://islab.oregonstate.edu/koc/ece578/00report/gmt.pdf>

24 Heikki Karjaluoto, 2002, *Electronic banking in Finland: consumer beliefs, attitudes, intentions and behaviors.*

25 Hermann De Meer, 2004, *Network security SSL, IBE, IBS and Secret sharing,* University of Passau.<http://www.fmi.uni-passau.de/~fickensc/Seminars/Hauptseminar_Network_Security_-_SSL,_IBS,_IBE_and_Secret_Sharing.pdf>

26 <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html>

27 <http://www.yourwindow.to/information-security/gl_authentication.htm>

28 <http://www.yourwindow.to/information-security/gl_nonrepudiation.htm>

29 Internet banking questionnaire, Anglia Polytechnic University <http://www.geocities.com/elaineharris/>

30 Introduction to Public key cryptography. <http://developer.netscape.com/docs/manuals/security/pkin/contents.htm>

31 Introduction to SSL <http://developer.netscape.com/docs/manuals/security/sslin/index.html>

32 IS Auditing guideline Internet banking, May 2003, Information Systems Audit and Control Association. <http://www.isaca.org/contentmanagement/contentdisplay.cfm?contentId=13618>

33 JM Sahut, M. Galuszewska, April 2002, *Why does SSL dominate the e-payment market?*JIBC. <http://www.arraydev.com/commerce/JIBC/0402-08.htm>

34 Joris Claessens, December 2002, *Analysis and design of an advanced infrastructure for secure and anonymous electronic payment systems on the Internet*, Katholieke University. <http://www.esat.kuleuven.ac.be/%7Ejoclaess/pub/phd.pdf>B13

35 Joris Claessens,Valentin Dem, Danny De Cock, Bart Preneel, Joos Vandewall, December 2001, *On the security of today's on-line banking systems.* <http://www.scs.org/scsarchive/getdoc.ufm?id=2092>

36 Key Pousttchi, Martin Schurig, 2004, *Assessment's of today's mobile banking applications from the view of customer requirements.* IEEE, Proceedings of the 37th Hawaii International Conference on System Sciences.

37 Larry L. Peterson and Bruce S. Davie, *Computer networks, a system approach.* 3rd edition. Morgan Kaufman, 2003 -813p.

38 M.Sklira, A.S.Pomportsis, M.S.Obaidat, *A new design framework for bank communication networks*, Aristotle university.

39 Mukul Gupta, Alok R.Chaturvedi, Shailendra Mehta, Lorenzo Valeri, *The experimental analysis of information security management issues for online financial services*. Communication of the ACM.

40 NUS Internet banking survey. <http://www.fba.nus.edu.sg/isworld/question.htm>

41 Online banking Understanding online banking services, *March 2003.<http://www.bankrate.com/brm/green/ob/ob2.asp>*

42 Peter B. Southard, Ken Siau, 2004, *A Survey of online e-banking retail initiatives*, Communication of the ACM.

43 Rudi Hoppe, Paul Newman, Pauline Mugera, October 2001, *Factors affecting the adoption of Internet banking in South Africa: a comparative study*, University of Cape Town.

44 Sue Rhee, Fred Riggins, Internet banking questionnaire.<http://www.cc.gatech.edu/gvu/usersurevey/survey-1998-04/questions/banking.html>

45 The Monetary Authority of Singapore, September 2002, *Internet banking technology risk management guidelines.* Version 1.2 <http://unpan1.un.org/intradoc/groups/public/documents/APcity?unpano11275.pdf>

46 The Risks Digest volume 23 Issue 30. <http://www.risks.com>

47 The Risks Digest, Volume 22 Issue 82. <http://www.risks.com>

48 Thomas Glaessner, Tom Kellermann, Valerie McNevin, June 2002, *Risk mitigation in financial transaction public policy issues, <http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationInFinancialTransactionsv4/$FILE/E-security-Risk+Mitigation+In+Financial+Transactions+v+3.0.pdf>*

49 V.Radha, Ved Gulati, April 2002, *Prevneting technology based bank frauds*, JIBC. <http://www.arraydev.com/commerce/jibc/0402-05.htm>

50 What is an Internet banking service. <http://www.ukinternetbanking.co.uk/internet-banking-service.asp>

51 Will Sturgeon, August 2003, *MBlast worm takes down major bank*, Silicon.com. <http://www.silicon.com/news/500013/1/5618.html>

52 William Jackson, June 2003, *BugBear learns new tricks, targets financial institutions*, Government Computer News. < http://www.gcn.com/vol1_no1/daily-updates/22367-1.html>

53 Winnie Chung, John Paynter, 2002, *An evaluation of Internet banking in New Zealand*, University of Auckland. IEEE Proceedings of the 35th Hawaii international of system sciences.

54 Work program – Internet banking. <http://www.auditnet.org/docs/internet%20Banking%20Ap.pdf>

55 Ziqi Liao, Michael Tow Cheung, 2003, *Challenges to Internet E-Banking*, Communication of the ACM.

Appendix 1 – Customer's Survey

Dear User,

The purpose of this survey is to evaluate internet banking in Lebanon.
Please be assured that your responses will be kept strictly confidential. Individual participants will not be identified in the analysis as only aggregated results will be analyzed and presented.
Note that you can choose multiple answers for the same question.

Thank you for your participation,

Regards

Are you using internet banking?

- ☐ Yes — Then complete section 1
- ☐ No — Then complete section 2

Section 1 - Yes

How did you heard about internet banking?

- ☐ Bank
- ☐ Friend

How often do you use internet banking?

- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Others

You chose to use internet banking for the following reasons:

- ☐ Convenience (anywhere, anytime)
- ☐ Curiosity
- ☐ Security
- ☐ Easy to maintain banking transaction activity

What are your reasons to choose a bank to conduct internet banking with?

- ☐ Have a traditional bank account with the same bank
- ☐ Reputation of the bank
- ☐ Variety of services offered by the bank
- ☐ Others

Where do you most often use internet banking?

- ☐ Home
- ☐ Work
- ☐ Internet cafe
- ☐ Others (Please state)

How easy do you find internet banking to use?

- ☐ Easy
- ☐ Moderately complicated
- ☐ Complicated

Have you used (or are currently using) any off-the-shelf personal finance management software programs such as Quicken or MS Money?

- ☐ Yes
- ☐ No

Is there an anti-virus software installed on the system you use?

- ☐ Yes
- ☐ No

If yes, how often is it updated?

- ☐ Daily
- ☐ Weekly
- ☐ Others.

Do you have a firewall installed on your system?

- ☐ Yes
- ☐ No

Do you install software or run programs from unknown origin?

- ☐ Yes
- ☐ No

Do you delete junk or chain emails?

- ☐ Yes
- ☐ No

Do you open email attachments from strangers?

- ☐ Yes
- ☐ No

Rate the importance of the following services offered by internet banking

	Importance		
	High	Medium	Low
View account balances			
Statement of account			
Transfer funds between accounts			
Download statement			
Check pending transactions			
Deposit detail			
Order checkbook			
Request stop payment on a check			
Report loss of a saving passbook			
Report a lost card			
Check balance of card			
Change password			
Bill payment			
Purchase/Sale foreign currencies			
Mobile banking			

Rate the importance of the following criteria of internet banking

	Importance		
	High	Medium	Low
Security			
Up to date information			
Internet services free from technical problems			
Response time			
Download time			
Ease of use			
Ease of navigation			
Range of banking services			
Attractive graphics			
Use of animations			
Icons having resemblance with bank's logo			
Little time to connect to web site			
Customer support (in case of problem)			

How secure do you think Internet Banking is?

Section 2 – No

Are you considering registering for internet banking?

- ☐ Yes
- ☐ No

What are the main reasons for not registering for internet banking?

- ☐ Concerned about security
- ☐ Never heard of internet banking
- ☐ Haven't taken time to open an account
- ☐ Not available through my bank
- ☐ Can do my banking transactions in other ways
- ☐ Do not need instant 24 hours access to my accounts
- ☐ Like to be able to talk to staff in person
- ☐ Internet banking offers a limited range of services
- ☐ Others

If your concern is about security

What scenario do you fear the most?

- ☐ Other people gaining access to your personal data
- ☐ Loosing money
- ☐ Others

On what key basis do you doubt the security systems employed by online banks

- ☐ Bad experience with internet security
- ☐ Own knowledge of internet security
- ☐ Advice from another party
- ☐ Others

If hardware tokens were to be used, would you register for internet banking?

- ☐ Yes
- ☐ No

Appendix 2 – Bank's Survey

Subject: Internet Banking Evaluation

Dear Sir,

I need you to answer the attached questionnaire which purpose is to evaluate internet banking in Lebanon and to which extends it complies with the Basel's committee requirements (May 2001 & July 2003).

I need the results of the survey to fulfill the partial requirement of my master thesis in computer science.

Please be assured that your responses will be kept strictly confidential. Individual participants will not be identified in the analysis as only aggregated results will be analyzed and presented.

I would like to thank you for your valuable time used to answer this questionnaire.

Regards,

Joelle Abboud

Notre Dame University
Faculty of Natural and Applied Sciences
Department of Computer Science

Definitions

Informational web site	:	Informational service is limited to a simple web site that is used by banks to provide information and publicity.
Interactive/Administrative web site	:	In addition to the informational services, administrative web sites allow customer to gain sensitive information such as account balance
Transactional web site	:	A transactional web site offers to customers the ability to conduct online transactions on their accounts; in addition to the services above.
Software escrow agreement	:	This agreement allows the banks to access the source code in some cases, such as, the party providing the service is out of business.
One factor authentication	:	The use, for authentication, of something the user knows such as logon Id or password.
Tiered single factor authentication	:	It is an enhanced one/single factor authentication, that include the use of two or more passwords employed at different points in the authentication.

Notes

Section 1- General information

Is your bank involved in Internet Banking?

☐ Yes Date Activated:

☐ No Date Planned to:

Has the bank checked for similar domain names?

☐ Yes

☐ No

What is the level of your bank's participation in Internet banking?

	Offered	Under Construction	Planned
Informational			
Interactive/Administrative			
Transactional			

What is the level of your bank's participation in Mobile banking in Lebanon? If offered, please state starting date.

	Offered	Under Construction	Planned
WAP banking			
SMS banking			

Reason for offering Internet banking:

☐ Profit ☐ Customer demand ☐ Retain customer

☐ Competition ☐ New customer

☐ Other:

What options are available to your customers once they accessed internet banking?

☐ View account balances

☐ Statement of account

☐ Download statement

☐ Check pending transactions

☐ Order checkbook

☐ Request stop payment on a check

☐ Report loss of a saving passbook

☐ Report a lost card

☐ Check card balance

☐ Change password

☐ Bill payment

☐ Transfer funds between accounts

☐ Purchase/Sale foreign currencies

☐ Others

Section 2 – Informational and Interactive web sites

Are applications available on the web site?

- ☐ Yes
- ☐ No

If yes, how does the customer submit them?

- ☐ In Person
- ☐ Online
- ☐ By Fax
- ☐ By Mail

Where is the web site hosted?

- ☐ In house
- ☐ Off site

If web site hosted off site, is it reviewed internally

- ☐ Yes How often?
- ☐ No

Testing

Screen testing	Has screen testing been conducted to ensure user friendliness? ☐ Yes ☐ No
Volume stress testing	Has testing been conducted to ensure system reliability and capacity? ☐ Yes ☐ No

Are security measures in place to prevent web site alteration?

- ☐ Yes
- ☐ No

Does the web site present links to other sites?

- ☐ Yes
- ☐ No

If yes, does the bank provide a disclaimer statement on the web page related to these sites?

- ☐ Yes
- ☐ No

Does your web site allow email contact to the bank?

- ☐ Yes
- ☐ No

If yes, have you included a disclosure about inclusion of sensitive information?

- ☐ Yes
- ☐ No

Software and Antivirus Updates:

Virus protection	How often is virus protection updated on server? How often is virus protection updated on workstations? Who is responsible of updates?(title)
Operating system update	When is operating system updates implemented? Who is responsible of updates?(title)
Software updates/Patches	When is software updates/patches implemented? Are they tested before implementation? Who is responsible of updates?(title)

Prevention controls and procedures:

Penetration testing	Is penetration testing performed? ☐ Yes How often? ☐ No Who is responsible for testing and reviewing? (title)
Intrusion detection	Is intrusion detection in place? ☐ Yes How often? ☐ No Who is responsible for testing and reviewing? (title)
Firewalls	Who is responsible for installing firewalls?(title) Who is responsible for monitoring firewall activity? How often are firewalls being monitored? Are all unused services blocked at the firewall?

Are there controls to restrict physical access to computer hardware, software and communication equipment?

☐ Yes
☐ No

Are the bank's hardware and phone lines protected from power surges, lightning strikes,...?

☐ Yes
☐ No

Has the bank encountered any computer related crime?

☐ Yes
☐ No

Does the bank have an electronic banking insurance policy?

☐ Yes
☐ No

List, if possible, all titles (jobs) involved with electronic banking and their duties. (If available, provide an organizational chart.)

Section 3 – Transactional web site

Percentage of customers signed up for internet banking?

Authentication is done through:
- ☐ One factor
- ☐ Tiered single factor
- ☐ Others (state)

Customer password

Initial password	What initial password procedure is adopted?
Restrictions	Minimum password length? Is alphanumeric password enforced? ☐ Yes ☐ No Is password change required? ☐ Yes How often? ☐ No What other type of restrictions on password creation is adopted (to prevent easily guessed passwords)?
Awareness	Are tips displayed on the web to help customers select passwords that are not easily guessed? ☐ Yes ☐ No

Is automatic log off available for user inactivity?
- ☐ Yes Inactivity period
- ☐ No

Do excessive failed access attempts disable access?
- ☐ Yes Number of allowed failed access attempts
- ☐ No

What procedures are used in case customer forgets his password?

Do employees have access to customer password?
- ☐ Yes
- ☐ No

Customer support:
Are you providing customers with support?
- ☐ Yes
- ☐ No

Are you providing procedures to respond to customers?
- ☐ Demands
- ☐ Problems
- ☐ Complaints

Does your web site provide customers with general security of their personal computer?
- ☐ Yes
- ☐ No

Are safeguards in place to detect and prevent duplicate transactions?
- ☐ Yes How?
- ☐ No

Is the bank using digital certificates?
- ☐ Yes
- ☐ No

Is the bank using digital signatures?
- ☐ Yes
- ☐ No

At what level is sensitive data encrypted?
- ☐ 40 bit
- ☐ 128 bit
- ☐ Other

Do IT personnel participate in training programs?
- ☐ Yes
- ☐ No

Is electronic banking training provided to other employees?
- ☐ Yes
- ☐ No

Are there dollar limits per transaction time period (day limit, ...)?
- ☐ Yes
- ☐ No

In case of system break down, does your bank have a contingency plan in place, to recover from hardware, software, communication links and data files?
- ☐ Yes
- ☐ No

Outsourcing

Criteria the vendor was selected upon
- ☐ Reliability of service
- ☐ Security features used
- ☐ Reputation, financial strength and viability
- ☐ The extend to which the vendor uses sub-contractors

Is user acceptance test conducted prior to implementation of any software modifications or enhancements?
- ☐ Yes
- ☐ No

Is the software under escrow agreement and are relevant program files and documentation kept current?
- ☐ Yes
- ☐ No

Third party has restricted access to relevant and necessary customer data.
- ☐ Yes
- ☐ No