THE SECURITY OF ELECTRONIC BANKING

Yi-Jen Yang
2403 Metzerott Rd.
Adelphi, MD. 20783

Abstract

The Internet has played a key role in changing how we interact with other people and how we do business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The electronic banking system addresses several emerging trends: customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are the concerns of security and privacy of information.

The current focus of security of information transfer is on the session layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels and a trusted code at both endpoints. The solution addresses the use of secure protocols because trusted channels don't really exist in most of the environment, especially since we are dealing with linking to the average consumers.

The solutions to the security issues require the use of software-based systems or hardware-based systems or a hybrid of the two. These software-based solutions involve the use of encryption algorithms, private and public keys, and digital signatures to form software packets known as Secure Electronic Transaction used by Mastercard and Pretty Good Privacy. Hardware-based solutions such as the Smartcard and the MeChip provide better protection for the confidentiality of personal information. Software-based solutions have the advantage over hardware-based solutions in that they are easy to distribute and are generally less expensive.

Introduction

> *Imagine yourself in this situation. You are at home alone one evening and you have your computer connected to your banking account. You are checking out your banking account to see how much money you have. Like many people, you still have a lot of money at home because you don't fully trust the banking system. Suddenly, you hear a noise outside and jump right out of your chair. You rush over to the window to see who is outside and realize that it is a burglar. You have a lot of money placed under your mattress and you fear that the burglar will take it. Since this is an age of advance technology, you have a mechanical device that lets you transfer paper money into electronic money which can then be sent to your bank via the Internet. This machine destroys the money and keeps track of the amount destroyed. You realized that you can save your money from the burglar and rush to get it immediately. You place all your money in the machine and it quickly converts the paper money into electronic money. By the touch of a button, you transfer your money to your banking account where it is safe. Now your money is safe. Now all you have to worry about is yourself.*

In today's highly technological world, the machine that destroys paper money and converts it into electronic money is far from reality. But the part on the person interacting with his or her banking account late at night is becoming more of a reality. The information superhighway has found its way into many homes, schools, businesses, and institutions. Many people are cruising the Internet each day to

obtain information on the weather, latest sport scores, local news, and many other exciting information. These people also buy and sell goods on this new media. Consequently, many businesses are reaching out to customers worldwide using the Internet as its communication channel. This new electronic media of interaction has grown to be known as the electronic commerce. "Electronic Commerce integrates communications, data management, and security services, to allow business applications within different organizations to automatically interchange information." [1] Consequently, electronic commerce is comprised of interconnected communications networks; advanced computer hardware and software tools and services; established business transaction, data exchange, and interoperability standards; accepted security and privacy provisions; and suitable managerial and cultural practices. This infrastructure will facilitate diverse and distributed companies nationwide to rapidly, flexibly, and securely exchange information to drive their business processes.

The banking industries is one such business that is using this new communication media to offer its customer value added service and convenience. This system of interaction between the consumers and the banking industries is call the electronic banking system. "Electronic banking is the use of a computer to retrieve and process banking data (statements, transaction details, etc.) And to initiate transactions (payments, transfers, requests for services, etc.) directly with a bank or other financial services provider remotely via a telecommunications network". [16]

Electronic banking is a new industry which allows people to interact with their banking accounts via the Internet from virtually anywhere in the world. The electronic banking system addresses several emerging trends: customer demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. This system allows consumers to access their banking accounts, review most recent transactions, request a current statement, transfer funds, view current bank rates and product information and reorder checks. Some of the banks that are currently offering this service are Bank of America, Centura Bank, Citibank, NationsBank, Chevy Chase, Bank One, ABN AMRO, Barnett Bank, Comerica, First Bank Systems, First Chicago NBD, Fleet Financial Group, KeyCorp, Mellon Bank, Michigan National Bank, PNC Bank, Royal Bank of Canada, and Washington Mutual Incorporated. [12] The electronic banking system can be seen as an "extension of existing banks."

These banks are catering to a very large population of Internet users. Heidi Goff, Senior Vice President for Global Point of Interaction of Mastercard, estimated that there will be more than 100 million users by the year 2000. Many other estimates conclude similar results, which lead to the indication that the Internet will play a major role in everyone's life and promote the electronic banking industry.

This paper will first discuss the motivations and ventures in Electronic Banking. Second, it will talk about the disastrous ventures in Electronic Banking with an example. Third, this paper will discuss the concerns about Electronic Banking from various perspectives. Fourth, the security issue and attacks will also be discussed, with solutions in both software-based and hardware-based systems. Fifth, this paper will examine the privacy technology and conclude with some final thoughts.

Motivations of Electronic Banking

The Internet is growing at an exponential rate. According to a survey, the Internet has doubled its size from 6.6 million hosts[2] in the mid 1995 to 12.8 million host in mid 1996. [23] As a consequence of the popularity of the Internet, hundreds of thousands of Internet users are trying electronic banking. Joshua Reymer, an analyst at Boston Consulting Group, estimates that 700,000 to 800,000 people currently are trying out PC banking, with Citibank being the leader among the banks. [24] As the

1 Source: Information Infrastructure Technology and Applications (IITA) Task Group, National Coordination Office for High Performance Computing and Communications, February 1994, pp.13-4

2 A host is defined as a domain name that has an IP address record associated with it.

Internet continues to expand, the convenience associated with electronic banking will attract more customers. One expectation of electronic banking is that it will replace the need for writing checks. In today's market, "According to preliminary data from the latest Federal Reserve survey of patterns of consumer spending, almost four-fifths of consumer expenditures are handled by checks, directly or indirectly.". [2] This means that electronic banking has a very large potential for use since many people expect that electronic checks will substitute paper checks. Moreover, for consumers, electronic money (electronic cash and electronic checks) means greater efficiency than using coins, paper bills, and traditional banks. The electronic banking system brings the convenience of 24-hour, seven days a week, banking by offering home PCs tied directly to a bank's computers. In addition, electronic money also offer greater security than a paper-and-coin system. Users are able to make a backup copy of their funds and if the electronic money is stolen, the users can invalidate the serial number just as they now stop payment on a paper check.

Ventures in Electronic Banking

Domestic

In order for this industry to expand further, secure transactions with the trust of the consumers are necessary. Many banks are advertising secure on-line service, allowing their customers a wide range of activities that they can do. Security First Network Bank is the first federally approved on-line bank that is certified by the Office of Thrift Supervision, the federal regulatory body for the saving bank industry. With the support of the federal agencies, Security First Network Bank can give their customers more than just their assurance, but the assurance of the government, which gives consumers a large incentive to try electronic banking.

For a truly convenient system, banks need to connect to customers as well as to other financial institutions. Creating a common link between multiple banks so that banks can better and more safely communicate amongst themselves is becoming more of a reality. Fifteen of North America's leading banks and IBM are working together to form an integrated network called Integrion Financial Network. The banks will be able to offer their customers access to their services through the public Internet and parallel private network access, with security and privacy.

International

In Europe, the Inter-bank Standards Association Belgium has established the Belgium's electronic banking system to connect Belgium's three largest banks together to develop uniform standards for electronic payments in Belgium. This system, developed by Utimaco uses electronic signatures according to the RSA method to guarantee accountability and security against the forging of electronic transaction.

Internationally, GENDEX Bank International is trying to connect the banking systems of various nations, states, independent principalities, and sovereign individuals to form an international banking system. This integration of electronic banking communities will promote the standardization of this industry. However, the primary concern today is the security issue.

Disastrous Ventures in Electronic Banking

In August of 1995, Citibank had problems with outsiders breaking into their system. A $10 million computer fraud against Citibank was the first successful penetration by a hacker into the system which transferred trillions of dollars a day around the world. Of the $10 million dollars illegally transferred, $400,000 were not found. Many banking experts predicted that these break-ins were bound to occur with banking business being done electronically at a time when more sophisticated personal computers are available. Since this break-in, Citibank has required its customers to use an electronic device that creates a new password for every transfer.

Concerns About Electronic Banking

Since Electronic Banking is a new technology that has many capabilities and also many potential problems, users are hesitant to use the system. The use of Electronic Banking has brought many concerns from different perspectives : government, businesses, banks, individuals and technology.

Government

From a government point of view, the Electronic Banking system pose a threat to the Antitrust laws. Electronic Banking also arouse concerns about the reserve requirements of banks, deposit insurance and the consumer protection laws associated with electronic transfer of money. The US government is concerned with the use of high quality of encryption algorithms because encryption algorithms are a controlled military technology.

Businesses

Businesses also raise concerns about this new media of interaction. Since most large transfer of money are done by businesses, these businesses are concern about the security of their money. At the same time, these businesses also consider the potential savings in time and financial charges (making cash deposits and withdrawals which some banks charge money for these processes) associated with this system. Another businesses concern is connected to the customer. Businesses ponder the thought that there are enough potential customers who would not make a purchase because the business did not offer a particular payment system (e.g. electronic cash and electronic check). This would result in a loss of sales. On the other side of the coin, if this system becomes wide spread, this would allow more buying power to the consumer which puts pressure on businesses to allow consumers to use electronic transfer of money.

Banks

Banks are pressured from other financial institutions to provide a wide range of financial services to their customers. Banks also profit from handling financial transactions, both by charging fees to one or more participants in a transaction and by investing the funds they hold between the time of deposit and the time of withdrawal, also known as the "spread". With more financial transactions being processed by their central computer systems, banks are also concern about the security of their system.

Individuals

Individuals are mainly concern with the security of the system, in particular with the unwarranted access to their accounts. In addition, individuals are also concern with the secrecy of their personal information. 82% of American poled expressed concern over privacy of computerized data. As more and more people are exposed to the information superhighway, privacy of information and the security that goes hand and hand with this information is crucial to the growth of electronic transactions. Some privacy technologies related to the electronic banking industry are electronic cash and electronic checks which will be discussed in the software solution section.

Technology

In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

1. *Security*

Security of the transactions is the primary concern of the Internet-based industries. The lack of security may result in serious damages such as the example of Citibank illustrated in the earlier section. The security issue will be further discussed in the next section along with the possible attacks due to the insufficient protections. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.

2. Anonymity (Privacy)

Generally speaking, the privacy issue is a subset of the security issue and thus will be discussed in the Privacy Technology section later. By strengthening the privacy technology, this will ensure the secrecy of sender's personal information and further enhance the security of the transactions. The

examples of the private information relating to the banking industry are: the amount of the transaction, the date and time of the transaction, and the name of the merchant where the transaction is taking place.

3. Authentication

Encryption may help make the transactions more secure, but there is also a need to guarantee that no one alters the data at either end of the transaction. There are two possible ways to verify the integrity of the message. One form of verification is the secure Hash algorithm which is "a check that protects data against most modification." [3] The sender transmit the Hash algorithm generated data. The recipient performs the same calculation and compares the two to make sure everything arrived correctly. If the two results are different, a change has occurred in the message. The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and the receiver to verify that the electronic currency or the digital signature that they received is real.

4. Divisibility

Electronic money may be divisible into different units of currency, similar to real money. For example, electronic money needs to account for pennies and nickels.

Security Issue

Dr. David Chaum, CEO of DigiCash said that "Security is simply the protection of interests. People want to protect their own money and banks their own exposure. The role of government is to maintain the integrity of and confidence in the whole system. With electronic cash, just as with paper cash today, it will be the responsibility of government to protect against systemic risk. This is a serious role that cannot be left to the micro-economic interests of commercial organizations."

The security of information may be one of the biggest concerns to the Internet users. For electronic banking users who most likely connect to the Internet via dial-up modem, is faced with a smaller risk of someone breaking into their computers. Only organizations such as banks with dedicated Internet connections face the risk of someone from the Internet gaining unauthorized access to their computer or network. However, the electronic banking system users still face the security risks with unauthorized access into their banking accounts. Moreover, the electronic banking system users also concern about non-repudiability which requires a reliable identification of both the sender and the receiver of on-line transactions. Non-secure electronic transaction can be altered to change the apparent sender. Therefore, it is extremely important to build in non-repudiability which means that the identity of both the sender and the receiver can be attested to by a trusted third party who holds the identity certificates.

Attacks

The Citibank $10 million break-in is one example of how the system is vulnerable to hackers. Hackers have many different ways that they can try to break into the system. The problem of the systems today are inherent within the setup of the communications and also within the computers itself. The current focus of security is on session-layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels, and a trusted code at both endpoints. It is really important to have a secure protocol because the *trusted channels* really don't exist in most of the environment. For example, downloading a game off the Internet would be dangerous because Trojan horses and viruses could patch the client software after it is on the local disk, especially on systems like windows 95 which does not provide access control for files. This leads to the use of software-based protections and hardware-based protections.

Many systems today use some form of software-based protection. Software-based protection are easily obtained at lower costs than hardware-based protection. Consequently, software-based protection is more widely used. But, software-based protection has many potential hazards. For software-based systems, there are four ways to penetrate the system. First of all, attacking the encryption algorithms is

one possible approach. This form of attack would require much time and effort to be invested to break in. A more direct approach would be using brute force by actually trying out all possible combinations to find the password. A third possible form of attack is to the bank's server which is highly unlikely because these systems are very sophisticated. This leaves the fourth possible method, which also happens to be the most likely attack, which is to attack the client's personal computers. This can be done by a number of ways, such as planting viruses (e.g. Trojan Horse) as mentioned above. But, unlike the traditional viruses, the new viruses will aim to have no visible effects on the system, thus making them more difficult to detect and easy to spread unintentionally.

Many problems concerning the security of transactions are the result of unprotected being sent between clients and servers. In systems such as NFS, AFS, and Windows NT, there is no authentication of file contents when sent between the client and server. In these systems, file contents read from the servers are not authenticated in any secure fashion. Consequently, the client does not have any mechanism to determine if the bytes are indeed being sent by the server and not from a hacker's program. Given this information, one possible scenario of attack is presented as follows:

> The attacker is assumed to have network access to any machine on any Ethernet sub-net between the file/server and the clients under attack. In under a day, a software package could be designed to exploit the lack of authentication in the NFS security product to patch the object code of any executable on-the-wire as it travels between the NFS server and the client machine. When the client retrieves data from the NFS server, it sends a short request message detailing which block from the file it is interested in. The attack software is located on an Ethernet segment between the client and the NFS server, so it is able to sense this traffic. The attack software waits for any request for a particular block of a particular executable such as the block containing the session key generation code in the Netscape executable. The software then is able to forge a reply from the NFS server and transmit it to the client. If the forged packet reaches the client before the real reply, it is accepted and the real reply is discarded as a duplicate. The forged reply generally reaches the client before the real reply. Given this ability, hackers could locate the code that selects the session key within Netscape. Then they can patch only 4 bytes into the code which causes the selection of a predictable session key every time the browser engages in the SSL (Secure Socket Layer) protocol. With this, hackers are able to decrypt all traffic from the browser to secure servers, obtaining information on credit card numbers or other private information. Credit card numbers are especially easy to recognized since they are grouped in 16 digits that have a distinct mathematical relationship.

Solutions

Software-Based Systems

In software-based security systems, the coding and decoding of information is done using specialized security software. Due to the easy portability and ease of distribution through networks, software-based systems are more abundant in the market. Encryption is the main method used in these software-based security system. Encryption is a process that modifies information in a way that makes it unreadable until the exact same process is reversed. In general, there are two types of encryption. The first one is the conventional encryption schemes, one key is used by two parties to both encrypt and decrypt the information. Once the secret key is entered, the information looks like a meaningless jumble of random characters. The file can only be viewed once it has been decrypted using the exact same key. The second type of encryption is known as public key encryption. In this method, there are two different keys held by the user: a public key and a private key. These two keys are not interchangeable but they

are complementary to each other, meaning that they exists in pairs. Therefore, the public keys can be made public knowledge, and posted in a database somewhere. Anyone who wants to send a message to a person can encrypt the message with the recipient public key and this message can only be decrypted with the complementary private key. Thus, nobody but the intended receiver can decrypt the message. The private key remains on one's personal computer and cannot be transferred via the Internet. This key is encrypted to protect it from hackers breaking into the personal computer. There are four examples of current encryption technology presented below: Digital Signature, Secure Electronic Transaction, Pretty Good Privacy, and Kerberos.

1. Digital Signature

Digital Signature was first proposed in 1976 by Whitfield Duffie, at Stanford University. A digital signature transforms the message that is signed so that anyone who reads it can know who sent it. The use of digital signatures employs a secret key (private key) used to sign messages and a public key to verify them. The message encrypted by the private key can only be verified by the public key. It would be impossible for any one but the sender to have created the signature, since he or she is the only person with the access to the private key necessary to create the signature. In addition, it is possible to apply a digital signature to a message without encrypting it. This is usually done when the information in the message is not critical. In addition, this allows people to know who compose the message. Because of the signature contains information so called "one-way hash", it is impossible to forge a signature by copying the signature block to another message. Therefore, it is guaranteed that the signature is original. One example of the use of digital signature in the electronic banking industry is by First Digital Bank. The First Digital Bank offers electronic bank notes: messages signed using a particular private key to provide unforgettable credentials and other services such as an electronic replacement for cash. "All messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on for whatever denominations were needed. These electronic bank notes could be authenticated using the corresponding public key which the bank has made a matter of record. First Digital Bank would also make public a key to authenticate electronic documents sent from the bank to its customers." [1]

2. Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) software system, the global standard for secure card payments on the Internet, which is defined by various international companies such as Visa MasterCard, IBM, Microsoft, Netscape Communications Corp., GTE, SAIC, Terisa Systems and Verisign. SET promises to secure bank-card transactions online. Lockhart, CEO of MasterCard said, " …We are glad to work with Visa and all of the technology partners to craft SET. This action means that consumers will be able to use their bank cards to conduct transactions in cyberspace as securely and easily as they use cards in retail stores today." [33] SET adopts RSA public key encryption to ensure message confidentiality. Moreover, this system uses a unique public/private key pair to create the digital signature. The main concerns for the transaction include not only to ensure the privacy of data in transit, but also prove the authenticity which both the sender and the receiver are the ones they claim to be. Digital signature is used to achieve the authenticity. A digital signature is produced by first running the message through a hashing algorithm to come up with the message digest. Next, by encrypting the message digest with sender's private key, this would uniquely identify the sender of the message. When receiving the message, the receiver decrypts the encrypted message with sender's public key. This ensures that the message was actually from the appropriate person. Besides uniquely identifying the sender, the digital signature also ensures that the original message was not tampered with in transit. The receiver can use the original hashing algorithm to create a new message digest after decrypting the message and compare the new message digest to the original digest. If they match each other, it can be sure that the message has not been altered in transit.

Although the public key encryption and the digital signature ensures the confidentiality and the authenticity of the message, there is still a potential danger existed in that the information the sender provides may not be real. For example, the sender may encrypt a bank card number which belongs to

someone else by using his/her own private key. To ensure the true authentication, there is a need for a process of certification. A third party who is trusted by both the sender and the receiver will issue the key pair to the user who provides sufficient proof that he is who he claims to be. One assumption lies in the receiver's trust that the CA's own key pairs, which are used in the certification process, have not been compromised. "Assuming SET will impact the deployment of RSA encryption for home banking and bill payment services online, one might wonder whether the banking industry should just adopt SET for other non-credit card transactions, as well. A senior banking executive at a major US bank contends, SET has the capability to allow payments that are not card-based. The processes in SET are not specific to card transactions. They are generic: authentication, certification, encryption and so on." [27]

3. Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP), created by Philip Zimmermann, is a "hybrid cryptosystem that combines a public key (asymmetric) algorithm, with a conventional private key (symmetric) algorithm to give encryption combining the speed of conventional cryptography with the considerable advantages of public key cryptography." [20] The advantage of PGP is that it does not require a trusted channel of transmitting the encryption key to the intended recipient of your message. Furthermore, it has the ability to sign the messages by encrypting them with sender's private key which can not be replaced by any other key. Once the receiver received the message, he/she can then decrypt the message with the sender's public key which can not be forged and represents the true identity of the sender.

4. Kerberos

Kerberos is named after the three-headed watchdog of Greek mythology and it is one of the best known private-key encryption technologies. Kerberos creates an encrypted data packet, called a ticket, which securely identifies the user. To make a transaction, one generates the ticket during a series of coded messages by making exchanges with a Kerberos server, which sits between the two computer systems. The two systems share a private key with the Kerberos server to protect information from hackers and to assure that the data has not been altered during the transmission. One example of this encryption is NetCheque which is developed by the Information Sciences Institute of the University of Southern California. NetCheque uses Kerberos to authenticate signatures on electronic checks that Internet users have registered with an accounting server.

Hardware-Based Systems

Hardware-based systems offer a more secure way to protect information, but, it is less portable and more expensive than software-based systems. The hardware-based security system creates a secure, closed channel where the confidential identification data is absolutely safe from unauthorized users. There are two hardware-based systems discussed in this section: Smartcard system and MeCHIP.

1. Smartcard System

Smartcard System is a mechanical device which has information encoded on a small chip on the card and identification is accomplished by algorithms based on asymmetric sequences. Each chip on the Smartcard is unique and is registered to one particular user, which makes it impossible for a virus to penetrate the chip and access the confidential data. However, practical limitations in the Smartcard system prevent it from broad acceptance for major applications such as home banking or on-line distribution. One draw-back for the Smartcard is that it can not handle large amounts of information which need to be decoded. Furthermore, the Smartcard only protects the user's private identification and it does not secure the transfer of information. For example, when the information is keyed into the banking software, a virus could attack the information, altering its destination or content. The Smartcard would then receive this altered information and send it, which would create a disaster for the user. Nevertheless, the Smartcard is one hardware-based system that offers confidential identification.

2. MeCHIP

MeCHIP which developed by ESD is connected directly to the PC's keyboard using a patented connection. All information which needs to be secured is sent directly to the MeCHIP, circumventing the client's vulnerable PC microprocessor. Then the information is signed and transmitted to the bank in

secure coded form. A closed, secure channel from the client to the bank is assumed in this case. All information which is transmitted and received is logged and verified to ensure that it has not been tampered with. If there are any deviations, the session is immediately terminated. This hardware-based solution offers the necessary security at the personal computer to transfer confidential information.

Privacy Technology

Privacy technology can be used to assure that consumers, merchant's, and the transactions themselves remain confidential. For instance, companies sending important, secret information about their marketing strategy to one of its partners would like to keep that information private and out of the hands of its competitors. This technology will keep all information secure and can be applied to electronic cash, also known as "e-cash". The privacy technology provides a fully digital bearer instrument that assigns a special code to money, just like a bank note. The security of e-cash is superior to paper cash because even if it is stolen, it can not be used. However, e-cash has its share of disadvantages because it lacks the privacy of use. "This system is secure, but it has no privacy. If the bank keeps track of note numbers, it can link each shop's deposit to the corresponding withdrawal and so determine precisely where and when Alice spends her money." [1] This would make it possible to create spending profiles on consumers and threaten their privacy. Furthermore, records based on digital signatures are more vulnerable to abuse than conventional files. Not only are they self-authenticating, but they also permit a person who has a particular kind of information to prove its existence without either giving the information away or revealing its source. "For example, someone might be able to prove incontrovertibly that Bob had telephoned Alice on 12 separate occasions without having to reveal the time and place of any of the calls." [1] One solution to this lack of privacy is the implementation of "blind signatures". How it works is that before sending the bank note number to the bank for signing, the user multiplies the note number by a random factor. Consequently, the bank knows nothing about what it is signing except that the note has a specific digital signature belonging to a person's account. After receiving the blinded note signed by the bank the user can divide out the random factor and use it by transferring it to a merchant's account as a payment for a merchandise. The blinded note numbers are untraceable because the shop and the bank cannot determine who spent which notes. This is because the bank has no way of linking the note numbers that the merchant deposited with the purchaser's withdrawals. Whereas the security of digital signatures is dependent on the difficulty of particular computations, the anonymity of blinded notes is limited only by the unpredictability of the user's random numbers. The blinded electronic bank notes protect an individual's privacy, but because each note is simply a number, it can be copied easily. To prevent double spending, each note must be checked on-line against a central list when it is spent which makes this verification procedure unacceptable for many applications, especially for minor purchases. Thus, this technology currently, is only applicable for large sums of money.

Conclusion

The Internet has grown exponentially, with more than 30 million users worldwide currently. The Internet enhances the interaction between two businesses as well as between individuals and businesses. As a result of the growth of the Internet, electronic commerce has emerged and offered tremendous market potential for today's businesses. One industry that benefits from this new communication channel is the banking industry. Electronic banking is offering its customers with a wide range of services: Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time restrictions.

Electronic Banking is offered by many banking institutions due to pressures from competitions. To add further convenience to the customers, many banking institutions are working together to form an

integrated system such as the Integrion Financial Network and the Gendex Bank International. On the other hand, this has not been readily accepted by its users due to the concerns raised by various groups, especially in the areas of security and privacy. Moreover, there are many potential problems associate with this young industry due to imperfection of the security methods. The example of Citibank's disaster due to hackers has led to more concerns about this system.

In order to reduce the potential vulnerabilities regarding to the security, many vendors have developed various solutions in both software-based and hardware-based systems. Generally speaking, software-based solutions are more common because they are easier to distribute and are less expensive.

In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard.

Bibliography

Books/ Magazines/Government Documents

1. Chaum, David. Scientific American. August 1992. pp.137-42
2. Government. Emerging electronic methods for making retail payments. June 1996.
3. Pfleeger, Charles P. Security in Computing. Prentice Hall, 1997.

Internet Sources:

4. 15 North American banks and IBM form company to offer electronic banking and commerce services. Http://www.ibm.com/Newsfeed/bankingpr.html
5. A $10 Million Lesson In The Risks Of Electronic Banking. Http://www.nd.edu/~astrouni/zhiwriter/spool/46.htm
6. About Encryption. Http://www.tropsoft.com:80/tropsoft/aboutenc.htm
7. BankNet Electronic Banking Service. Http://mkn.co.uk/bank
8. Basic Flaws in Internet Security and Commerce. Http://HTTP.CS.Berkeley.EDU/~gauthier/endpoint-security.html
9. Basic Reflections On Security. Http://www.esd.de/eng/secu/secu.htm#10
10. Basic Reflections On Security. Http://www.esd.de/eng/secu/index2.htm
11. Belgian Banks Put Their Money On a Security Solution From Utimaco. Http://www.mergent.com/html/electronic_banking.html
12. Big Blue Goes E-Banking. Http://iw.com/1996/12/news.html#bigblue
13. Cracking Crypto Keys on the NOW Cluster. Http://HTTP.CS.Berkeley.EDU/projects/isaac/crypto-challege.html
14. Electronic Banking. Http://www.electrobank.com/ebaeb.htm
15. Electronic Banking Resource Center. Http://www2.cob.ohiostate.edu/%7Erichards/bankpay.htm
16. Electronic Banking System. Http://www.electrobank.com/ebaeb.htm
17. Electronic International Banking. Http://www.wwwebport.com/biz/gendex/elec_bank.html
18. Encryption Crash. Http://www.iw.com/1997/01/news.html#crash
19. Encryption Issues. Http://www.muc.edu:80/cwis/person/student/lockett/encryption.html
20. How PGP works. Http://rschp2.anu.edu.au:8080/howpgp.html
21. Internet Security. Http://cfn.cs.dal.ca/Education/CGA/netsec.html
22. Introduction to PGP. Http://sun1.bham.ac.uk/N.M.Queen/pgp/pgp.html
23. Off the Charts The Internet 1996. Http://www.iw.com/1996/12/charts.html
24. PC Banking Services Spread, but Success is Still Uncertain.

Http://conceptone.com:80/netnews/nn942.htm
25. Security Comes First With Online Banking at Security First Network Bank.
Http://www.hp.com/ibpprogs/gsy/advantage/june96/custspot.html
26. SET Specification. Http://www.visa.com/cgi-bin/vee/sf/set/intro.html
27. Solving the Puzzel of Secure Electronic Commerce. Http://www.rsa.com/set/bankset.htm
28. The comp.security.pgp FAQ. Http://www.gpg.net/gppnet/pgp-faq/faq-01.html#1.3
29. The comp.security.gpg FAQ. Http://www.pgp.net/pgpnet/pgp-faq/faq-05.html
30. The comp.security.gpg FAQ. Http://www.pgp.net/pgpnet/pgp-faq/faq-03.html
31. The comp.security.gpg FAQ. Http://www.pgp.net/pgpnet/pgp-faq/faq-06.html
32. The MeCHIP. Http://www.esd.de/eng/chip/index3.htm
33. Visa, Mastercard to Set Standard for Electronic Commerce.
Http://www.cnnfn.com/news/9602/01/visa.mastercard/index.html

Glossary

Authentication
A process that grants access to a local or remote computer system, a network, or online information.

CA (certification authority)
An entity or service that distributes electronic keys for encrypting information and electronic certificates for authenticating user and server identities.

Digital Signature
A coded message added to a document or data that guarantees the identity of the sender.

Electronic Banking
The use of a computer to retrieve and process banking data (statements, transaction details, etc.) and to initiate transactions (payments, transfers, requests for services, etc.)
directly with a bank or other financial services providers remotely via a telecommunications network.

Electronic Commerce
The use of an information infrastructure through which businesses can speed the exchange of information, improve customer service, reduce operating costs, and increase global competitiveness.

Encryption
The scrambling, or encoding, of information to prevent anyone other than the intended recipient from reading the information. There are many types of encryption, and they are the basis of network security.

Hash Code
A unique, mathematical summary or “fingerprint” of a document that serves to identify the document and its exact contents. Any change in the hash code is an alert that the document’s contents have been altered.

Internet
A worldwide system of computer networks. Networks connected through the Internet use a particular set of communication standards, known as TCP/IP, to communicste.

Kerberos
A distributed security system developed by the Massachusetts Institute of Technology. It uses private-key security.

Private-key security
Also known as symmetric-key security, this is a security mechanism based on both parties have the same encryption key, as in secret-key cryptography. The client and server share a key to encrypt and decrypt information on a network. A common implementation of private-key security is the Kerberos distributed security system.

Public-key security
Also known as asymmetric-key security or public-key encryption technology, this is a security mechanism for securely distributing encryption keys that are used to “lock” and ”unlock” data across an unsecured path. Public-key security is based on encryption key pairs, in contrast to private-key security, which is based on having a single, shared key.

RSA
An encryption mechanism by RSA Data Security that uses both a private and a public key. RSA is also used for authentication.

Secure Socket Layer (SSL)
A security protocol developed by the Netscape Communications Corporation to encrypt sensitive data and verify server authenticity.