Vulnerabilities in e-banking: A study of various security aspects in e-banking

*Tejinder Pal Singh Brar,** Dr. Dhiraj Sharma, *** Dr. Sawtantar Singh Khurmi
*Department of Computer Applications, Chandigarh group of colleges, Gharuan, Mohali
**School of Management Studies, Punjabi University, Patiala
***Bhai Maha Singh College of Engineering, Kotkapura Road, Muktsar

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 [1]. Internet can be seen as a truly global phenomenon that has made time and distance irrelevant to many transactions. One industry that is using this new communication channel to reach its customers is the banking industry. The transformation from traditional banking to e-banking has been a "Leap" change. 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. But on the other hand the increase in the use of ICT facilities result in increase of criminal activities like spamming, credit card frauds, ATM frauds, Phishing, identity theft, denial of service and most of others has lend credence to the view that ICT is contributing crime in banking sector. The challenges that oppose electronic banking are the concerns of security and privacy of information. This paper aims at investigating various risks and whether these risks can be totally eradicated or not. Based on the findings this study, the paper concludes that with the help of various tools total eradication of risks is not possible but can be highly reduced if internal control measure techniques are adequately put in place.
Keywords: ICT, Phishing, MITM, Malware, Spyware

Introduction:

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 organizations like schools, businesses, institutions and even homes. Many people are surfing on the Internet each day to obtain information on the world politics, share markets, weather information, latest developments, global news, and many types of information.

People also buy and sell goods on this new e-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." [2] 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. "Internet banking" refers to systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC) or other intelligent device. [3] Electronic banking is an 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, transfer funds, request a current statement, review most recent transactions, view current bank rates and product information. Some of the banks that are currently offering this service are ICICI Bank, HDFC Bank, Punjab National Bank, State Bank of India, Axis bank etc.

Concerns about Electronic Banking

The wealth of a new technical possibilities give rise not only to new products and more efficient and effective ways of doing things ,but also to the possibility of misuse of the technology. Like other technologies ICT is essentially neutral and can be used in the ways that most of us would consider beneficial, as well as in ways that are harmful. 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 poses 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.

Businesses

Businesses also raise concerns about this new media of interaction. Since most large transfer of money is 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.

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.[2]

In May 2003 only around twenty Trojans that target financial services were reported, most of them with basic functionality. Two and a half years later the number of such malware has increased to nearly two thousand different variants [4]. Often skeptical people say that these are only theoretical attacks, which would never succeed. The growing number of examples proves the opposite, as in the case of an online bank heist in Korea in June 2005 [5]. A student with only average computer skills used a basic Trojan to steal $50,000 from other people's bank accounts.

Discovered in August 2003, PWSteal.Bancos.B [3] targeted account information from only five banks. Its newer version PWSteal.Bancos.T discovered in April 2005 [4], contained an astonishing list of 2764 monitored URLs from 59 different top-level domains.The methods used by these malware vary immensely, from basic social engineering attacks to sophisticated kernel level rootkits. Still the main functionality can be classified in a few categories, as some

attacks use the same basic principles. The main divider between the methods used is the point of attack.

Types of Online Attacks

Banks and service providers need to guard against various types of online attacks. The object of an attack may vary. Attackers may try to exploit know Vulnerabilities in particular operating systems. They also may try repeatedly to make an unauthorized entry into a Web site during a short time frame thus denying service to other customers. To simplify matters we can categorize the attacks into three main groups: local, remote and hybrid attacks. Local attacks happen on the victim's machine, remote attacks don't modify the machine but try to intercept or redirect the traffic of a session and hybrid attacks combine local and remote attacks and are the most powerful.

Remote attacks

Phishing: A very well-known online fraud is phishing, which is an attack designed to convince the victim to give away their online banking credentials to a third party. This and other similar scams or attacks which reveal credentials to the attacker fall into the class of credential harvesting [6]. An attacker sets up a copy of the web site they want to impersonate on a server they control. This copy includes all the code from the original site. The set of used images can be gathered during a previous legitimate session. This makes it hard to trace the imposter in the server logs as no suspicious access is made. Next, the attacker sends emails to a large number of email accounts. The emails contain a convincing message that should trick the recipient into visiting the spoofed web site and revealing his log on credentials.Phishing emails usually contain obfuscated links to the spoofed web site. There are many tricks to obfuscate the real server location, especially when HTML enabled emails are used. One such example is the method of translating the quartet of a standard IP address into a dot-less decimal number i.e. http://3639551848 [216.239.39.104]. Most browsers support these decimal IP addresses, as well as web authentication strings in the form of username:password@website.tld. So to obfuscate the URL even more the attacker can add a fake web authentication string that looks like the impersonated domain name, such as http://mySecureBank.tld@3639551848.This corresponds to a username of "mySecureBank.tld" with no password given on the decimal IP address representation of 216.239.39.104.This will trick many users into believing, that they are about to click on a link that leads to the mySecureBank.tld domain. Replacing characters with their Unicode

representations or adding escape symbols to the URL makes it even harder to identify the real domain name behind a link.

Vishing

Vishing is both a recent and a very old scam. It is the age old fraud where the attacker phones the victim and uses social engineering to trick the victim into revealing secret information such as credit card information. What is new is the use of voice-over-IP and how this changes the expected trust in the phone system.[6]

Cloned voice-banking systems Many banks have systems for voice-banking. Many vishing attacks clone these systems so that they sound the same as the official systems. Emails similar to those used in phishing attacks solicit customers to call a number purporting to be their bank. Telephone numbers have none of the normal clues to identify their owners so it is very hard for users to distinguish those owned by their bank. This was used to attack Santa Barbara Bank and Trust in 2006 [7].

Voice-over-IP Traditionally the phone service has been a trustworthy source. With caller ID a number could be traced easily to a customer and while phreaking and other attacks were possible, they were quite difficult and specialized. With the advent of voice-over-IP and gateways from IP telephony to the public switched telephone network associating a number with a real person has become a whole lot harder. Caller-ID is easily spoofed by an attacker and there can be a much more convoluted trail between a VoIP connection and a real person.

Automated answering systems The automated answering and menu systems used by most large companies, including banks, can also be used by an attacker. Combined with VoIP and war-dialing techniques an attacker can automatically try hundreds of numbers and use an automated system which, like banks, solicits details like credit card numbers in the name of ease of use or security.

DNS cache poisoning

Domain name checking toolbars decrease the success rate for phishing attacks described above, but other remote attacks are immune to them. In March 2005 a large-scaled DNS cache poisoning attack [9] started to fill vulnerable DNS servers with false domain name - IP address pairs. As a result, machines relying on these poisoned DNS servers received a false

IP address resolution for certain domains, which led them to malicious Web sites. Detailed analyses of aspects of DNS attacks can be found in the paper from Ollmann [10]. This shows that sometimes even typing the URL address by hand in the browser might lead to a malicious site. DNS manipulation attacks are nothing new and have been around for many years. They gained media attention as attackers started to use them on a larger scale to steal logon credentials. This method of attack is sometimes referred to as pharming. Pharming [8] is a specific phishing technique where the attacker alters the DNS responses to a client computer causing a legitimate URL to resolve to the IP of a machine under the control of the attacker.

DNS Hijacking

In January 2005 the American ISP Panix experienced a social engineering attack [11]. Due to lax domain change verification processes, someone was able to modify the registered details of the domain panix.com. The actual DNS records were moved to a company in the United Kingdom, and Panix.com's mail was redirected to a company in Canada. Users of the domain panix.com were redirected to false sites and could have fallen victims to fraudsters if a transaction site existed at this address.

Local attacks

One of the biggest misconceptions is that users believe when they use an SSL connection, their online banking session is perfectly safe from a third-party. In nearly all security advice given by online services, the security experts say that if the user can see the yellow padlock symbol in the browser window the traffic between the site and the user are secured. This is true, but little does the user realize that SSL was designed to secure the channel from the user machine to the bank computer, and not the end points themselves. Whatever is done with the data before the start point and after the end point of the SSL channel is completely out of the SSL encryption context.

This fact is exploited by the PWSteal.Bankash.A Trojan [12], which captures information entered into web forms before it is encrypted by SSL and sent to the financial institution. To achieve this, the Trojan drops a DLL and registers it as a browser helper object (BHO) within Microsoft's Internet Explorer. This threat is thus able to intercept any information that is entered in any web site visited by the browser, before it is encrypted. Loading a DLL as a BHO is not the only way to intercept entered information: injecting code into the browser's memory space or hooking common API functions achieves the same result. Displaying a

spoofed web site on top of the real web site can also steal the same information for specific targets. PWSteal.Bancos.B [13] does the latter for a handful of banking web sites. When a user infected with this threat visits one of the predefined Web sites, the Trojan will generate a pop-up window, which is a copy of the real log on form. This fake window then overlays the real browser window, so that the user will enter their logon credentials into the fake form. This approach defeats the SSL encryption, as the data is never entered into the browser and therefore never encrypted.

From the user's viewpoint, the opened Web site is the real bank site. The URL in the address bar is not spoofed and even the yellow SSL padlock reveals the correct certificate details, if any user should ever take the time to verify it. Only the overlaid fake password prompt is not part of the original web site and of malicious intent.

This method of attack also defeats virtual keyboards, which were introduced to protect against key logger attacks. By entering the sensitive user credentials with a virtual keyboard, displayed on a web page, the problem of interception is not solved. While a key logger is no longer capable of intercepting the secret information, multiple screenshots still can. Recording the position of all mouse clicks and one screenshot of the virtual keyboard contains enough information to recalculate the characters used. The same is true for consecutive screenshots on all mouse click events. For obvious reasons, if the information is entered into a fake pop up window then a virtual keyboard will not be able to prevent the leaking of the sensitive log on data. Regardless of how the information is entered, once it is in the browser's memory space a Trojan can steal it with the means discussed above.

Hardware keyloggers

If an attacker has physical access to a machine then they can use a hardware keylogger. These devices are produced commercially [14] and are very cheap and easy to disguise, typically being inserted between the keyboard and the back of the computer, which people rarely look at. One obvious place for these to be useful is on public computers, such as in Internet cafes. They may be more expensive and difficult to use than just installing a Trojan, but in the cases where the software may be monitored for Trojans, or the attacker is an outsider and doesn't have administrative privileges on the machines they may still be an option. Since they capture all keyboard input they require some processing of the data to find any credentials.

Shoulder surfing

"Shoulder surfing" is the term for surreptitiously observing someone entering credentials in person, usually by looking over their shoulder. This attack vector is normally associated with observing the personal identification number (PIN) for a bank card prior to stealing the physical card either by force or by pick pocketing it. This is usually either an opportunistic attack or a much targeted, specific one. It certainly does not scale very well in either case and is quite high risk. Someone closely connected to the thief must be physically close to the person while they are entering the PIN.

A more sophisticated variant uses closed-circuit television to observe the PIN. This is less likely to be caught, but more difficult to set up. Depending on the amount of insider help required for installation, it might also be more damaging for the insider if caught.

Hybrid attacks

Nothing limits an attacker to only one type of attack. For the attacker the most successful methods are hybrid attacks that combine strategies from both local and remote attacks. A trivial attack would be if a Trojan executed on the infected machine checked all saved bookmarks for known valuable online services and replaced the URL with a fake one, similar to phishing emails.

The obvious flaw in this plan is that the user can see the modified URL if they check the address bar of the browser. So the Trojan needs to modify the browser settings to not display the address bar or overlay it with a fake pop-up window. Even though this is feasible, it resides on the same level as basic phishing attacks and can be equally well done by remote attacks. The more sophisticated approach of the attacker would rather be to use all the power they have on the infected machine and altering the hosts file is an obvious place to start. The hosts file gives the attacker the possibility to redirect certain domains to predefined IP addresses. This technique is used by the Trojan. hosts [15].

Some other types of attacks:

1. Sniffers — Also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture logon
2. IDs and passwords.
3. Guessing Passwords — using software to test all possible combinations to gain entry into a network.

4. Brute Force — a technique to capture encrypted messages then using software to break the code and gain access to messages, user ID's, and passwords.
5. Random Dialing — this technique is used to dial every number on a known bank telephone exchange. The objective is to find a modem connected to the network. This could then be used as a point of attack.
6. Social Engineering — an attacker calls the bank's help desk impersonating an authorized user to gain information about the system including changing passwords.
7. Trojan horse — a programmer can embed code into a system that will allow the programmer or another person unauthorized entrance into the system or network.
8. Hijacking —intercepting transmissions then attempting to deduce information from them. Internet traffic is particularly vulnerable to this threat.

This scenario should make it obvious that we either need a reliable way of preventing traffic redirection or a more secure authentication scheme. Strong authentication of both parties to mutually authenticate each other is the desired goal. The security of the online service should not be solely based on the security of the end point (the user's PC), as a user might not be able to fully protect it, for example when the machine is shared with other persons at an Internet café.

Solution options

The following general assumptions with regard to the methods of protection outlined below.

SMS challenge code

Two-factor authentication systems have been introduced to ensure secure log on validation. One system that promises good user acceptance uses the user's registered mobile phone to receive an activation code. In this scenario the user identifies themselves to the bank with their account name. Next, the bank generates a random temporary password and sends it in a short text message (SMS) to the user's mobile phone number. The user enters this challenge code into the browser and proves thus that he has access to the correct mobile phone. This two-factor authentication works fine and is quite convenient for most users. One major advantage is that most users already have a mobile phone and therefore no extra hardware token needs to be bought, deployed, and supported.

If we modify our worst-case scenario described above somewhat, then we will see that this authentication cannot withstand a man in the middle (MITM) attack. The user is redirected to

a fake web site. Once the user enters his account name into the spoofed web site, the attacker uses the received username, logs on to the real service and initiates the submission of the one-time password through SMS. The user will receive the code on his mobile phone and enter it into the fake web site still thinking it is the real web site. The attacker then uses the supplied code to authenticate him to the real service.

Image verification

The PassMark system was introduced by the Bank of America in 2005 [16]. The system is based on a shared secret between the bank and the user, consisting of an image and a verification phrase. When a user wants to log on to a PassMark enabled web service, he will be prompted for his username. If the user has already authenticated to the service a "Device ID" is sent along with the username. The Device ID is realized through an encrypted cookie that is stored on the user's machine. The service then determines if the Device ID and username match and if so, present the user the login page with the secret image and verification phrase embedded in it. Users are instructed to only login if they see their known picture with their chosen verification phrase.

Using our worst-case scenario with the redirected traffic, an attacker could outwit this system in the following way. As the infected machine sends traffic to the supposedly real domain it will also send all the cookies associated with this domain. Therefore no out of band traffic is needed to retrieve it. Still having full control over the target machine, the Trojan could read out all cookies and send them back to the attacker's server. The real online banking server should not rely on the client IP address for any authentication as it might change or be modified by intermediate systems such as proxy servers. Therefore, having the cookie with the Device ID and the username will be enough to retrieve the shared secret, even though the attacker can't decrypt the secure cookie. After receiving the secret information the attacker feeds the image and verification phrase back to the fake session with the user. Feeling secure by seeing their picture, the user will most likely enter his password into the spoofed web site opening the service to the attacker. As a side note it should be mentioned that it does not matter if the image is selected from a group on the online banking server or if the custom image rests on the user machine and only the path to it is stored on the main server. The attacker will mimic the real online service and provide whatever data the user expects.

Dynamic Security Skins (DSS)

Extending the image verification approach, dynamic security skins (DSS) as introduced by R. Dhamija and J.D. Tygar provide a trusted password window [17]. A photographic image chosen by the user is transparently overlaid on web forms that include sensitive information prompts. In addition a "visual hash" which can be seen as a unique graphical pattern, is overlaid as well. The visual hash is tied to the secure session and changes with each session. This makes it infeasible for an attacker to spoof a pop-up that is identical to the password prompt. But it does not authenticate both parties reliably to each other. Thus our worst-case scenario can trick the user into entering his login credentials in a MITM attack. For the DSS the whole spoofed web site is contained in one legitimate SSL session and the attack would be the same as for image verification protection.

PKI based software solution

With extensive use of cryptography and a well designed PKI it would be possible to not only authenticate the server to the user but also vice versa. This mutual authentication eliminates MITM attacks. Client certificates can provide this authentication. Secure distribution of the client's certificates and managing them on a large scale can become rather difficult.

PKI based hardware token

A Trojan can steal the private key and PIN for a PKI based software token. Therefore tamper resistant key storage must be used to ensure high security. Smartcards with external smartcard reader devices are the most obvious solution for this. Hiltgen et al. proposed a two-stage; smartcard PKI based implementation of such a solution [18]. Pre-generated key pairs and certificates are stored on a tamper proof smartcard. Using a PIN code on the external device's keypad unlocks the key vault in the smartcard. Therefore a key logger cannot intercept the PIN code. A signed Java applet downloaded from the bank's web site communicates with the card reader on one side and with the bank on the other. This applet authenticates itself against the card reader. Next, it can initiate a mutual authenticated SSL channel with the bank server, signing the session. This eliminates man in the middle attacks against this schema. As the smart card securely stores the private key, it can ensure a proper authentication and prevent impersonation attacks. The following table shows a brief comparison between the protection methods discussed in this paper.

	User acceptance	System invasion	Implementation cost	Portability (Web Café)	Protection againstremote phishing attacks	Protection against sophisticated MITM
Traditional passwords	High	Low	Low	High	No	No
SMS	Moderate	Moderate	Moderate	Moderate	Yes	Depends
Image verification	High	Low	Low	High	Yes	No
Dynamic Security Skins	High	Low	Moderate	Moderate	Yes	Depends
PKI based software solution	Moderate	Moderate	Low	Low	Yes	Depends
PKI based hardware tokens	Low	High	High	Low	Yes	Yes

Table 1: Protection method comparison matrix.

An enterprise that decides on protection techniques can select from a number of possible solution options. There are different options that are available reflects the fact that security solutions are still evolving to final maturity levels.

Conclusion:

Due to its lower transaction costs, twenty-four hours services, increased control over transactions, higher volume of transactions in less time, remote transaction facilities, and much wider array of banking products and services; e-banking has become an integral part of modern banking. But besides these opportunities e-banking operation increases different levels of risks for banks. Furthermore, customers who rely on e-banking services may have greater intolerance for a system that is unreliable or one that does not provide accurate and current information. Through the advent of on-line services customer have greater choice and do not need to be tied to one financial institution or another. Clearly, the longevity of e-banking depends on its accuracy, reliability and accountability.

One of the major problem areas with Internet banking appears to be with the security and safeguarding of information exchanged between customer and bank. Like every coin has two sides, if the Internet has its advantages then on the other hand there are drawbacks also. These drawbacks are so severe that they can adversely affect banking activities which in turn affect customers as well as organizations. Total eradication of online frauds, thefts, Spyware and malware proliferation is not possible but early detection and preventive measures can be quite useful if used on time.

References:

[1] Yi-Jen Yang : "The security of electronic banking**"** 2403 Metzerott Rd. Adelphi, MD.

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

[3] Comptroller of the Currency administrator of National Banks (Internet Banking Comptroller's Handbook October 1999 p-1)

[4] Joakim von Braun, Internal study Symantec Sweden, 2005.

[5] Chosunilbo, "Breaching Online Banking Security Proves Easy as Pie", 5 June 2005, http://english.chosun.com/w21data/html/news/200506/200506050007.html

[6] New approach to Internet Banking, Matthew Johnson , September 2008 Technical report (UCAM-CL-TR-731 ISSN 1476-2986)Cambridge university

[7] Firefox phishing protection bypass vulnerability. Securiteam, Jun 2006. http://blogs.securiteam.com/index.php/archives/467

[8] Gunter Ollmann. The pharming guide: Understanding & preventing DNS-related attacks by phishers, Aug 2005. http://www.ngssoftware.com/papers/ThePharmingGuide.pdf.

[9] K. Haugsness, "March 2005 DNS Poisoning Summary", March 2005, http://isc.sans.org/presentations/dnspoisoning.php.

[10] G. Ollmann, "The Pharming Guide" , 2005, http://www.ngssoftware.com/papers/ThePharmingGuide.pdf.

[11] T. Cole, B. Tonkin, "Email from Tim Cole to Bruce Tonkin [regarding the unauthorized transfer of panix.com domain]", 14. March 2005, http://www.icann.org/correspondence/cole-to-tonkin14mar05.htm.

[12] For detailed information on PWSteal.Bankash.A, http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bankash.a.html.

[13] For detailed information on PWSteal.Bancos.B, http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.b.html.

[14] KeyGhost. KeyGhost SX. http://www.keyghost.com/keylogger.htm.

[15] For detailed information on Trojan.Qhosts, http://securityresponse.symantec.com/avcenter/venc/data/trojan.qhosts.html.

[16]B. Riess, "Bank of Amercia announcement", 26. May 2005http://www.passmarksecurity.com/BofA.jsp.

[17] R. Dhamija, J.D. Tygar, "Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks".

[18] A. Hiltgen, T. Kramp, T. Weigold, UBS AG & IBM Ruschlikon,"Secure Internet Banking Authentication", 15 March 2005, http://www.ubs.com/1/e/ubs_ch/authentication.html.