Study of Indian Banks Websites for Cyber Crime Safety Mechanism

Susheel Chandra Bhatt[1],
[1]Research Scholar,
Computer Science Department
Kumaun University, Nainital, Uttarakhand, India

Durgesh Pant[2]
[3]Prof. & Director,
School of Computer Science & IT
Uttarakhand Open University Dehradun Campus,
Dehradun, Uttarakhand, India

The human society has undergone tremendous changes from time to time with rapid pace at social level from the beginning and technological level ever since the rise of technologies. This technology word changes the human life in every manner and every sector. Banking field is one of them. Banking in India originated in the last decades of the 18th century. Since that time the banking sector applying different ways to provide facilities and securities to a common man regarding to money. Security issues play extremely important role in the implementation of technologies specially in banking sector. Further on it becomes more critical when it comes to the cyber security which is at the core of banking sector. After the arrival of Internet and WWW this banking sector is totally change specially in terms of security because now money is in your hand on a single click. Now user has number of choices to manage his money with different kind of methods. In this paper an attempt has been made to put forward various issues of Indian banks websites for cyber-crime safety mechanism.

Keywords- Cyber; Encryption, Phishing, Secure Socket Layer

I. INTRODUCTION

Crime is a social and economic phenomenon and is old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment"[1]. The hallmark of criminality is that, it is breach of the criminal law. Per Lord Atkin "the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences"[2]. Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. Cyber-crime is the latest and perhaps the most complicated problem in the cyber world. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber-crime [3]. Cyber-crimes are computer related as well as computer generated crimes which are increasing day by day. Cyber-crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also
used to include traditional crimes in which computers or networks are used to enable the illicit activity.

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by illegally as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail spoofing or instant messaging [4], and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users [5] and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. A phishing technique was described in detail in 1987, and the first recorded use of the term "phishing" was made in 1996. The term is a variant of *fishing* [6] probably influenced by *phreaking* [7][8] and alludes to "baits" used in hopes that the potential victim will "bite" by clicking a malicious link or opening a malicious attachment, in which case their financial information and passwords may then be stolen. Not all phishing attacks require a fake website. Messages that claim to be from a bank, tell the users to dial a phone number regarding problems with their bank accounts [9]. Once the phone number (owned by the phisher, and provided by a Voice over IP service) was dialled, it prompts the user to enter the account number and PIN. Vishing (voice phishing) sometimes uses fake caller-ID data to give the appearance that calls is from a trusted organization [10].

II. CYBER CRIME SAFETY MECHANISM

A. Password encryption

One of the most important security features used today are passwords. It is important for users to have secure, strong passwords. Most of the more recent Linux distributions include password programs that do not allow user to set an easily guessable password. User has to make sure the password program is up to date and has these features. Encryption is very useful, possibly even necessary in this day and age. There are all sorts of methods of encrypting data, each with its own set of characteristics. Most Unixes (and Linux is no exception) primarily use a one-way encryption algorithm, called DES (Data Encryption Standard) to encrypt the passwords. This encrypted password is then stored in database. When user attempt to login, the password user type in is encrypted again and compared with the entry in the file that stores the passwords. If they match, it must be the same password, it allowed access. Although DES is a two-way encryption algorithm (user can code and then decode a message, given the right keys), the variant that most Unixes use is one-way. This means that it should not be possible to

reverse the encryption to get the password from the contents of database.

B. Virtual Keyboard

A virtual keyboard is a computer keyboard that a user operates by typing on or within a wireless- or optical-detectable surface or area rather than by depressing physical keys. Such a system can enable the user of a small handheld device, such as a cellular telephone or a PDA (personal digital assistant) to have full keyboard capability. In one technology, the keyboard is projected optically on a flat surface and, as the user touches the image of a key, the optical device detects the stroke and sends it to the computer. In another technology, the keyboard is projected on an area and selected keys are transmitted as wireless signals using the short-range Bluetooth technology. Theoretically, with either approach, the keyboard could even be projected in space and the user could type by moving fingers through the air. The term virtual keyboard is sometimes used to mean a soft keyboard , which appears on a display screen as an image map . In some cases, a software-based keyboard can be customized. Depending on the host system and specific software, the user (who may be someone unable to use a regular keyboard) can use a touch screen or a mouse to select the keys. Virtual keyboard can be categorized as:

- virtual keyboards with touch screen keyboard layouts or sensing areas [11]
- optically projected keyboard layouts or similar arrangements of "keys" or sensing areas[12][13]
- optically detected human hand and finger motions[14]

C. Secured Socket Layer

Secure Sockets Layer (SSL), are cryptographic protocols that provides communication security over the Internet [15]. SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. To be able to create an SSL connection a web server requires an SSL Certificate. When users choose to activate SSL on web server he will be prompted to complete a number of questions about the identity of the website and the company. The web server then creates two cryptographic keys - a Private Key and a Public Key. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) - a data file also containing the details. User should then submit the CSR. During the SSL Certificate application process, the Certification Authority will validate the details and issue an SSL Certificate containing the details and allowing user to use SSL. The web server will match issued SSL Certificate to Private Key. The web server will then be able to establish an encrypted link between the website and the customer's web browser. The complexities of the SSL protocol remain invisible to the customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session - the lock icon in the lower right-hand corner, clicking on the lock icon displays the SSL Certificate and the details about it. All SSL Certificates are issued to either companies or legally accountable individuals. Typically an SSL Certificate will contain domain name, company name, address, city, state and country. It will also contain the expiration date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate. When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user letting them know that the site is not secured by SSL.

D. SMS Alerts

SMS as used on modern handsets was originated from radio telegraphy in radio memo pagers using standardized phone protocols and later defined as part of the Global System for Mobile Communications (GSM) series of standards in 1985 [16] as a means of sending messages of up to 160 characters[17] to and from GSM mobile handsets[18]. SMS stands for short message service. An SMS alert is a message sent to a cellular device, such as a phone, to notify the receiver of something. An SMS alert is received in much the same way as a phone call is received. There is normally a sound or vibration that will indicate that the message has come in. There are various types of SMS alerts that people may consent to. These include appointment reminders, banking transactions, and specials or sales offered by businesses they patronize. In many instances, an SMS alert is sent out to large numbers of people at once. This means that if two people are scheduled to receive the same SMS alert, they should receive them at about the same time. SMS alerts that contain personal information, such as banking transactions or requests for payment, are not usually handled this way. Sending an SMS alert is often viewed by the sender as a service. In many cases, the senders do not charge the receivers for such messages. There may, however, be a fee charged to both the sender and the receiver by their cellular companies. In other cases, an SMS alert can be part of a subscription. This is a service where a person pays a fee to receive certain types of notifications. These can include news, sports, and weather updates.

E. User Awareness Programs

User or Customer is the key of any field. We can develop number of software or technology by which we can secure the things but these all software are waist if the end user is not getting the proper information regarding to these software. In Banking sector there are new gadgets and technologies are coming day by day by which the bank can provide secure transactions to end user. Using these gadgets the banks also has to run some awareness programs for the end users by whom they can also understand the meaning of secure transactions as well as the user will able to learn how to use these gadgets for secure transactions.

III. STATUS OF INDIAN BANKS WEBSITES

In this paper we take five Indian banks and try to find out the security features using by the bank for online transactions. The data is collected by various reports from web, newspaper and media. For every security feature we provide 5 points. The banks are-

- State Bank of India (SBI)
- Punjab National Bank [PNB]
- Central Bank of India [CBI]
- Bank of Baroda [BOB]
- Allahabad Bank

TABLE 1. POINT TABLE

Bank	PE*	VK*	SSL*	SMS*	UAP*	Total
SBI	4	4	4	3	0	15
PNB	4	4	3	4	0	15
CBI	3	4	3	2	0	12
BOB	4	4	3	4	0	15
Allahabad	3	4	4	3	0	14

**PE- Password Encryption, *VK- Virtual Keyboard, *SSL-Secure Socket Layer, *SMS- Short message service alerts, *UAP- User Awareness Program*

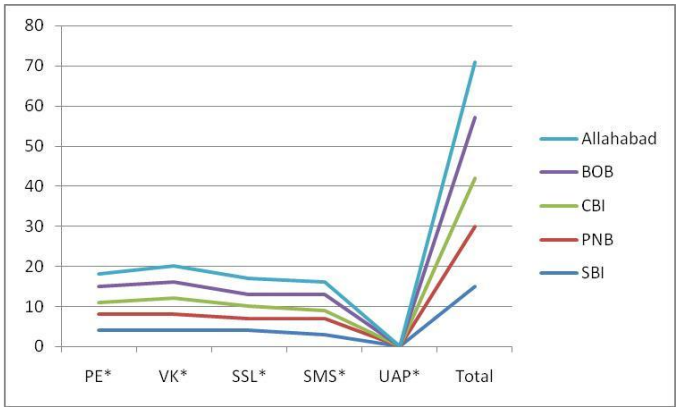

Figure 1. Graphical representation of security features

In this study we found that the all banks having the same feature for his websites. They all are providing password encryption facilities with virtual keyboard. The websites of the banks are is using secure socket layer and they also providing SMS alerts facilities to customer to know the information regarding to the money transaction. We provide 5 marks for each feature but no bank got full 5 mark for any feature and the aggregate total of every bank is vary 12 to 15 out of 25. The reason behind this is that they all have little bit loop wholes on all the security features but the biggest reason is User awareness feature. Sometime SMS alerts also come with viruses, so this is the responsibility of the bank to check either SMS alert is secure or not. Not all the bank user using the SMS alert facility because the user still in confusing mode because of the lack of awareness. One another thing is that the most of the facilities started by the bank is still not using by the customer because they have no proper information regarding these facilities and if the customer is using few facilities then this information he came to know from the other customer. So in this area all banks have to focus properly. No bank is providing special training program to aware the customer, who is the neediest person of world. Because many of the problems user face in bank sectors due to lack of his knowledge. So this is the responsibility of the bank to provide the proper information to end user.

They have to tell the user

- What is the meaning of using virtual keyboard
- What is the meaning of strong password
- What is the meaning of SMS alerts
- Don't access net banking account from cyber café or public computer.
- Use a single computer as far as possible.
- Login net banking site by directly typing site name.

  Don't click any link, if that link takes you to login page, close the page, and start over.
- Bank or its representative never asks for password and username over telephone.
- Change the password after 6 months.
- Remember the id and password, don't write it anywhere.
- Don't give any of the personal information to any web site that does not use encryption or other secure methods to protect it.
- Don't share any information to any one regarding to account
- Install good antivirus program on the system and regularly update the program.

The need for user awareness program is continuous, in addition to being multi-disciplinary and multi-dimensional. It is imperative to first digest that information security is a process, not a product. An information security awareness training program thus, needs to maintain the equilibrium between usability, productivity and security. This paper describes the security feature using by the bank for money transaction on websites and focus what banks have to do for spreading awareness. Interesting thing is that it is very difficult to stop any kind of cyber-crime especially when we talk about crimes related to the banks because many of the problems occur in bank sector by the user due to lack of awareness. So if the banks will start too aware the user then definitely the scenario will change. We can't stop the crime, we have to face this. The only one thing which we can do is prevention. We have to learn how to prevent society by this kind of smart crime and banks sector has to play key role from the front to spread awareness.

IV. CONCLUSION AND FUTURE SCOPE

In this paper we describe different safety features using by the banks for online transaction and examine where the problem is in the system. We found that all the banks use the latest technology for the online security feature but still they have small loop wholes in this feature. As well as they don't have any user awareness program to spread information and this is one of the biggest reasons of this online security. All bank users do not use online facilities because they have no proper information and the reason behind all this is the same lack of awareness. Along the same line we people also have to increase our awareness level because this is not only the responsibility of the banks. One the interesting thing is that in future these technologies will increase rapidly. It means user will have to use these facilities therefore we need to make our system more secure regarding to the safety mechanism. We have to be aware of the technologies which we are using and also need to increase our awareness level to secure humankind.

REFERENCES

[1] Granville Williams.
[2] Proprietary Articles Trade Association v. A.G. for Canada (1932)
[3] Duggal Pawan- Cyber Crime
[4] Tan, Koontorm Center. "Phishing and Spamming via IM (SPIM)". Retrieved December 5, 2006.
[5] Microsoft Corporation. "What is social engineering?" Retrieved

August 22, 2007.
[6] "Spam Slayer: Do You Speak Spam?". *PCWorld.com*. Retrieved August 16, 2006
[7] "Phishing, n. OED Online, March 2006, Oxford University Press.". *Oxford English Dictionary Online*. Retrieved August 9, 2006
[8] "Phishing". *Language Log, September 22, 2004*. Retrieved August 9, 2006.
[9] Gonsalves, Antone (April 25, 2006). "Phishers Snare Victims with VoIP". Techweb.
[10] "Identity thieves take advantage of VoIP". Silicon.com. March 21, 2005.
[11] EP application 546704 Thomas H. Speeter/AT&T: "Intelligent work surfaces" priority date 13.12.1991
[12] DE application 19734511 B. Kämmerer, C, Maggioni, H. Röttger/SIEMENS AG: "Kommunikationseinrichtung" filing date
08.08.1997
[13] WO 0003348 C. Maggioni, B. Kämmerer/SIEMENS AG: "Projection Device / Vorrichtung zur Projektion" priority date 10.07.1998
[14] EP 0554492 Hans E. Korth: "Method and device for optical input of commands or data" filing date 07.02.1992
[15] T. Dierks, E. Rescorla (August 2008). "The Transport Layer Security (TLS) Protocol, Version 1.2"
[16] GSM Doc 28/85 "Services and Facilities to be provided in the GSM System" rev2, June 1985
[17] LA Times: Why text messages are limited to 160 characters
GSM 03.40 Technical realization of the Short Message Service (SMS)