Review of Demand of Net Banking and the Insight of Various Attacks and Threats to Customers and Applied Countermeasures

Priti Saxena
PhD Scholar, Computer Science Department, UTU, Dehradun,Uttarakhand
pritisaxena82@gmail.com

Dr. R.B.Patel
Professor, Dept. of Computer Science & Engineering, Chandigarh College of Engineering & Technology, (Degree Wing), Sector-26, U.T., Chandigarh-160019,
drpatelrb@gmail.com

***Abstract*—The banking sector is on the edge of boom because of the emerging online services and e-commerce based applications provided to the customers. Nowadays customers demand for anywhere, anytime, anyplace services. With these the user becomes more sensitive to the threats and attacks that can create disaster to the user.**

***Keywords*— Electronic banking, transaction, threats, attacks, phishing, fault tolerance, confidentiality, integrity, availability.**

I. INTRODUCTION

Nowadays banking system has become very alert in terms of providing services. There is no need to carry cash in hand. Facilities like debit card, credit card, online banking make the working of the bank and the user very easy. Now we can do movie booking, hotel booking as and when required. But with all these comes the threats and attacks. The security concerns the confidentiality, integrity and authenticity of a user and its data. Talking about the solutions, both hardware –level and software based solutions are required. Counting from the hardware devices to the software applications, protocols and many more are involved to provide security. Security is applied using encryption techniques, use of public and private keys, digital signature and use of certificates, SSL (Secure Socket Layer) and many more. The paper puts emphasis on the implementation of sandboxing for banking system. Smartcard and the Me Chip provide better protection, which are hardware-based.

II. DISTRUBTED SYSTEMS IN BRIEF

Distributed computing is platform to provide services for information sharing in a controlled manner with the transparency to the user. It help in managing the various activities through proper coordination. Examples include ATM system, World Wide Web, computing system distributed geographically and many more [34].

A. Types of distributed system

In today's continuously evolving world, the types of distributed systems are categorized on the basis of the needs:

1. Cluster computing systems
2. Transaction processing systems
3. Grid computing systems
4. Enterprise application integration
5. Distributed pervasive systems

B. Some distributed systems

1. WWW
2. Network of branch offices computers for automated processing of orders.
3. Network of embedded systems.
4. New cell processor.

C. Advantages and Disadvantages and Design Issues of Distributed System

There are various benefits of using distributed systems like reliability, performance, communication and many more. Though these advantages suffer from various problems but work is going on to improve them. The disadvantages include difficulties of developing distributed software, networking problems, and security problem. The security aspect is the foundation of this review work.

Distributed system also faces some design issues. These are openness, transparency, reliability, and the main topic of this work – security. The main concerned issues for this work are communication, fault tolerance and reliability and security.

1. Communication

Communication in a distributed system is performed through:

1. Message passing
2. Remote procedure call

Communication models are of three types:

1. Client – server communication
2. Group multicast
3. Peer to Peer

2. Reliability and Fault Tolerance

In place of failures the system should continue to work, this shows the system is reliable.

It has two features:

1. Availability - In case if a system stops functioning, the other system should be ready without any delay.

2. Fault-tolerance: A system should be able to detect failures in the system and repair on time without any performance problem.

D. Models of distributed system

The distributed system is a wide field to study. Models are created to define various features of distributed system. These model models covers the way a user looks at the distributed system. The three models are:
1. Physical model: It defines the various physical components of the system. Physical structure of nodes and networks.
2. Architectural models explains communication between processes.
3. Fundamental model: Three models have been defined: interaction model, failure model, security model. Out of these three, fundamental model is of main application to the proposed objective. The fundamental is divided into interaction model and failure model. The interaction model under the fundamental is further classified into two variants. There are three types of failures named as omission, arbitrary and timing that occurs in distributed system.

The fundamental model is further categorized as security, interaction and failure model. [35]

a. Interaction Model

The interaction model deals with nodes and the type of interaction between the nodes. This includes host systems and communication channel.

b. Failure model

It enlists the types of failure than can occur in a distributed systems. The main failures are omission, arbitrary and timings failure. The omission failure is further divided into fail stop, crash, omission send, receive omission process. Coming to arbitrary failures are the worst type of failures i.e. byzantine failures. Some of the examples are:

1. A process arbitrarily omits intended process steps.

2. Message content may be altered or replay.

The timings failure include clock process, performance process and performance channel. The security model is discussed in the next section.

E. Security features in a system

1. Confidentiality: The information should not be disclosed to unauthorized person.
2. Integrity: the content of the message must not be altered.
3. Availability: the resource must always be available.
4. Authenticity: The user accessing the data and the data must be authentic.
5. Authorization: User must be authorized to access the data or service on the network.

The security encompasses various features for complete protection of data and communication channel.

III. Banking Distribution System

The whole system of internet and online banking is based on distributed system. This section gives of overview of distributed system.

A. An Overview banking distribution transformation

- 1980-2000: Payments have been digitalized. In this period, ATMs (Automated Teller Machine), credit card have replaced paper-based payments as new cost-saving opportunities have come.
- 2000-2010: Next step was the digitalization of the banking system. During the first Decade, customers have started using the bank services remotely 24/7 for low value added activities. This approach has greater benefits and was cost efficient for the banks.
- 2010-2015: Banks were fully digitalized. Mobile banking has become one of the ways to perform transactions. It has increased the business scenario with online marketing.

B. Problems faced by distributed system designers

- The system resources are allocated to wide variations of applications. Applications like web pages, some have millions of hit and some may have very few. Different types of workloads have been assigned, different geographical location.
- In a distributed system, heterogeneity of hardware, software, operating system and network exists. Beginning from a simple LAN (Local Area Network) going up to a wireless network, wide environments range is present which can have different types of complexities.
- Various internal problems like concurrency, nonsynchronized clocks, and software failures, unavailability of various resources or components.
- Security issues like threats and attacks on user and data integrity, denial of service, ensuring integrity and confidentiality, checking authenticity and accessibility.

IV. Brief History About Internet Banking

In the early time, online banking was in the form of distance banking products and services. Online services started in 1990s. The first service was began in 1981 by the collaboration of four banks which provide services for banking from home [3].

A. Ventures of Electronic Banking

Consumer trust is necessary point for the transactions in the online banking. Banks advertiseabout secure on-line service, which allow customers to do various online activities. Federal agencies supported the bank to provide assurance to consumers to try for electronic banking. For an appropriate system, a bank should be able to connect to other banking institutions as well as the customers. Privacy and security are the two main issues to be looked after for safe online banking.

B. Past Disastrous Ventures in Electronic Banking

In August 1995, first successful attempt of penetrating the system of Citibank which has transferred trillions of dollars around a day costing a fraud of $10 million. With the increase in the number of online transactions, number of online attacks

are increasing and new forms are emerging. Another such example was of eBay's database accident. It was hacked in the mid-2014 disclosing personal information including e-mails. Just after the attack, 8% fall occurred in the share prices and affected up to 145 million people [8]. PayPal has faced a problem of flood of numerous requests which has slowed down the server and took it offline. It took an estimate of £3.5 million, three weeks to repair and installation of new hardware and software. It was a persistent attack from 2010-2011[9]. A state –sponsored attack was done on a London company with a revenue loss of £300 million [10].One case of impersonation was attempted by a person claiming to be James Grant, owner of a Canadian Bitcoins owner [11].

V. Issues And Challenges Faced By Internet Banking

As an estimate, an amount of Rupees 42.2 crore has been spent in 2012/13 for cybersecurity in India, which was an increase from 35.45 crore spent in 2010/11. This has included CERT-In. In comparison to this, US spends much more. Agencies in India don't have enough money contributions. More amount of money has to be contributed for the proper functioning and control of cyber-attack. One of the most common attack are stealing the credentials means user's login and password. Some of these attacks include phishing, cross-site scripting, pharming and many more.

A. Attack Vectors

Four types of attacks are seen on e-banking, out of which credential theft means stealing the identity and transaction modification are well known. Other two includes the denial of access to the institutions and transaction observation, but these are also well consideredp19]. An attack tree model [32] is a good example of the attack description.The two main categories of attacks along with the known attacks are:

(1)Credential Harvesting: some of the examples include Denial of service, Transaction snooping, Pharming and many more.

(2)Attack Vectors: It includes hardware keyloggers, Evil Tor nodes, Evil public access points, DNS poisoning, Local router hacks, Trojans.

B. Issues from Various perspectives (Government, Businesses, Bank, Individual)

With respect to government view, laws are the major point of concern. Concerns of consumer protection for transfer of money, deposit of insurance, reserve requirement of banks requires strong support of encryption algorithms. Business concerns have issues of the security of the transfer of large amount of money through organizations. One more concern is that when business becomes wide spread, pressure come on the company to include online services. Banks gets the pressure to provide financial services to the customers of the financial institutions. In return, banks gets the profit by investing the funds embraced between various spans of time. They charge fees from the customers for any transaction performed. Thesethings also increases the need of security. Talking about the individual, concern comes with the unwanted access to the account, to their systems while performing online transactions like shopping, bookings or money transfer. Electronic cash and checks are some of the privacy issues. The RBI (Reserve Bank of India) has released a summary of policies, risk assessment, personal security, and information asset-cycle, user training for awareness, online monitoring processes and many more for information security [1].

C. Technology Issues

Technical issues are related to security, privacy authenticity and divisibility which are briefed as follows:

- Security-This means maintaining integrity of the messages. This is necessary for electronic banking systems. These transactions includes online transactions, online fund transfer, etc.
- Anonymity (Privacy) - The privacy speaks about the confidentiality of the user and his data. Elaborated, it is the confidentiality of the personal information and the transactions of the online user. Privacy is the subset of the security.
- Authentication -Generally speaking, through encryption data can be secured but it should not be altered at either end of the transacting parties. This can be dome though hash algorithm [4] and also through certificates.
- Divisibility -Electronic divisibility of the money accounts for nickels and pennies.

D. Security Issue

Non-reputability is an important which guarantees the identity of the sender and the receiver. Panida in paper [2] has compared different categories of the security features in Australian banks. Security related attacks includes brute force attack, encryption algorithm attack, server based attack and client's system attack.

VI. Current Work In The Said Direction

Five basic security features of a security system includes: Confidentiality, integrity, access control, authentication and authorization, confidentiality, integrity, access control. Following gives a review of the techniques applied for implementing these features.

The main participants of the financial system are the financial institutions, commercial banks, stockbrokers and other non-banking financial companies. Banks are divided into public and private banks. R.Jassal has compared these banks for the security features provided by them. [12]. ICICI bank, was the first bank which has offered the internet banking facilities in 1998. Since then, almost all public and private banks have started giving internet services [13].

A. Various security measures have been developed which are summarized as follows:

1. Anti-phishing measures [14]

Starting with TLS, stands for Transport layer security protocol is used for providing confidentiality and integrity. Next is the spam filtering measure which analysis and give scores to the emails based on the likelihood of being spam? One is the take down measure means complete take down reaction which is reported to the ISPs later for questioning. For some primitive phishing attacks password wizards are used.

2. Web browser security

Microsoft phishing filter, available with Microsoft Internet Explorer1, Version7, is an anti-phishing filter. Based on the

feedback form and metadata delivered by the server and use of heuristics from web page, a site is classified as a safe site [15]. Some more examples are Firefox Phishing protection, Opera fraud protection etc.

3. Banking measures

One of the common measure is TANs stand for Transaction Authorization Numbers [21] (TANs) are one-time passwords used by banks, protect against credential snooping. It is not effective for man-in the middle (MIM) attack. Another example is SecureID. It's a two-factor authentication provided by RSA [22]. This is a time synchronized encrypted code weak against MIM (Man in the Middle) attack. One form is multi-factor authentication derives from the EMV [23], known as chip authentication protocol [24]. This has been rolled out by Barclays in UK [25]. It is not time- dependent and weak against MIM attack. Mobile phones are a good option for secure channel, but because for the advancements in technologies, these have become similar to personal computers and faces same types of vulnerabilities. Operating systems like Symbian [26, 27] and WinCE [28] have been focused for various viruses, Trojans and same is the story of iPhone [29]. Citibank in UK has introduced PIN (Personal Identification Number) entry system, in order to avoid keyboard sniffing, [30].

4. Third party measures

For the prevention of phishing in Pay Pal and e-bay websites, an E-bay toolbar is introduced [16]. McAfee site advisor assigns three types of ratings as safe, caution and warning to the sites visited by the user [17]. Trust Bar is an enhancement of TLS to check the websites [18]. Spoof guard is a heuristic –based approach to work on phishing [19]. Dynamic Security Skins (DSS) [20] is proposed by Dhamija and Tygar as an anti-phishing measure. But it is restricted for use in case of a compromised system and key loggers.

VII. Hardware And Software Based Solutions

While developing secure system for the internet banking, two methods can be used. First, a solution which is based on software and second, a hardware based solution.

A. Systems based on Software

A software is made to secure a set of programs. Encryption is one of the common method used in security systems. Various authors have proposed methods for providing confidentiality, integrity and access control. An authentication method in which a short-time password is used for challenge/ response system. The method can be implemented for the mobile banking to evaluate the security concern [7].

1. Digital Signature

It has been proposed in 1976. The receiver comes to know about the sender and verifies it through digital signature. First Digital Bank was one of the first electronic bank to use this feature [5].

2. SET

It stands for Secure Electronic Transaction system, utilized for secure card payments in online banking. Lockhart, the CEO of MasterCard said, "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."[6].

3. PGP

PGP stands for Pretty Good Privacy, introduced by Philip Zimmerman, hybrid based cryptosystem of asymmetric and asymmetric algorithm to provide encryption. Advantage is, it signs the message to be sent by encrypting it with the sender's private key.

4. Kerberos

It is user for encryption of data packet, known as a ticket, which is used for secure user identification. NetCheque is created by the Information Sciences Institute which utilizes Kerberos for authenticating signatures on electronic cheques to confirm the registration of Internet users with an accounting server.

5. Secure Sockets Layer

SSL is now a very widely used technology which establish an encrypted and secure link between a web server and a browser. It is Netscape protocol made over an improvement to IETF.Here when a session is created, the server responds. When work is over, the server quits and closes the session [33]. In a TLS/SSL connection, the application creates a session and after completion of task, the server closes the session [32].

B. Hardware-Based Systems

Hardware-based systems are less portable and more effective. Two are briefed below:

1. Smartcard System

Small chips are used in smart cards. It is encoded and assigned to a user. It avoids viruses. The drawback is it cannot handle huge amount of information. Because of practical limitations it is not broadly accepted. It only protects the user identification but does not provide secure transfer.

2. MeCHIP

It connects directly to the PC's keyboard. Secured information is transferred to MeChip by passing vulnerable microprocessor. This information is sent to the bank in secure form.The information is verified every time it is transmitted or received to avoid tampering. In case of deviations the session id terminated. This is useful for confidentiality.

C. Privacy Technology

Privacy technology assures the confidentiality of the transactions. This technology is applicable for e-cash for secure electronic cash transfer. It provides a complete digitization of money.

VIII. Conclusion

Various security measures like encryption, digital certificates, VPN, SSL, Kerberos and many other are available to provide confidentiality, integrity and availability to the users, organizations and banking system. Every minute new threats and attacks are emerging for which new technologies are created. Sandboxing is also a very well-known method to secure ports and personal computers. The paper shows an insight of various threats and attacks in an electronic banking system, along with the description of various methods and techniques proposed during the span of time. In this paper, a very important concern has been taken as a task of analysis, which is security. It shows various types of security techniques (software and hardware), applied in securing online banking. The second section shows the distribution of banking system. The third section covers the brief history, advantages

and disadvantages of online banking system. The fourth section covers the issues and challenges currently online banking is facing. Fifth section throws light on the current work done in the said direction.

REFERENCES

[1] The RBI Guidelines Summary, 2012.

[2] Panida Subsorn and Sunsern Limwiriyakul, "An analysis of Internet Banking security of foreign subsidiary banks in Australia: A customer's perspective." IJCSI, vol.9, issue 2, No2, March 2012.

[3] Yi-Jen Yang, "The security of electronic banking", 2403 Metzerott Rd. Adelphi, MD.20783.

[4] Pfleeger, Charles P., Security in Computing, Prentice Hall, 1997.

[5] Chaum, David, Scientific American. August 1992.pp.137-42.

[6] Visa, Master Card to set standard for electronic commerce.

[7] SyedaShazmeen and Shyam Prasad, "A practical approach for secure Internet Banking based on cryptography", IJSRD, volume 2, Issue 12, December 2012. Department of IT, Balaji Institute of Technology and Science, Warangal, A.P. India.

[8] The Telegraph: eBay admits cyber-attack has hit sales, 16 July 2014.

[9] BBC: Anonymous hackers cost PayPal £3.5m, 22 November 2012.

[10] Computing: Corporate espionage on an industrial scale targeting the UK, 26 June 2012. 15

[11] Cyber security Newsletter75, the Nation Security Group, April 2014.

[12] R.Jassal et al.,"Comparative study of online banking Security System of various banks in India", International Journal of Engineering, Business and Enterprise Application, 6(1), September- November, 2013, pp.90-96.

[13] Ankit Kesharwani, "Exploration of internet banking website quality in India::AWEBQUAL approach introduction literature review", IBS, Hyderabad, Ritesh Tiwari, IBS, Hyderabad in Great Lakes Herald Vol 5, No 1, March 2011.

[14] Matthew Johnson, Technical Report, "A new approach to Internet Banking", UCAM-CL-TR-731,ISSN 1476-2986,University of Cambridge,2008.

[15] Microsoft phishing filter: "A new approach to building trust in e-commerce content." White paper, Microsoft Corp, 2005.

[16] eBay. eBay toolbar. http://pages.ebay.com/ebay_toolbar.

[17] Poor advice from SiteAdvisor. Light Blue Touchpaper, Richard Clayton. Aug 2007.

[18] Amir Herzberg and Ahmad Gbara, "Security and identification indicators for browsers against spoofing and phishing attacks." Cryptology ePrint Archive, Report 2004/155, 2004.

[19] Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C. Mitchell,. "Client-side defense against web-based identity theft." In 11th Annual Network and Distributed System Security Symposium, February 2004.

[20] RachnaDhamija and J.D. Tygar, "The battle against phishing: Dynamic security skins." In Proceedings of the 2005 ACM Symposium on Usable Security and Privacy, pages 77–88. ACM Press, July 2005.

[21] Two-factor authentication: An essential guide in the fight against internet fraud. Technical Report GP WP 2W, GPayments, Feb 2006.

[22] John Leyden, Phishers rip into two-factor authentication. The Register, July 2006.

[23] EMVCo LLC. EMV 4.1, Book 4—Cardholder, Attendant, and Acquirer Interface Requirements, June 2004.

[24] MasterCard International. Chip Authentication Program—Functional Architecture, Sept 2004.

[25] Gemalto. Press release, April 2007. http://www.gemalto.com/press/archives/2007/04-18-2007- arclays.pdf.

[26] Virus List. Worm.SymbOS.Cabir.a. Virus Encyclopedia, June 2004.

[27] Trend Micro. SYMBOS COMWAR.C. Virus Encyclopedia, Oct 2005.

[28] Virus List. Virus.WinCE.Duts.a. Virus Encyclopedia, July 2004.

[29] Charlie Miller, Jake Honoroff, and Joshua Mason. "Security evaluation of Apple's iPhone." Technical report, Independent Security Evaluators, July 2007.

[30] Sarah Hilley.Citibank cuts off bank spies with virtual keyboard. Infosecurity Magazine, Feb 2005.

[31] Bryan Parno, Cynthia Kuo, and Adrian Perrig, "Phoolproof phishing prevention." Financial Cryptography and Data Security, volume LNCS of 4107, pages 1–19. Springer-Verlag, 2006.

[32] G. Dalton, R. Mills, J. Colombi, and R. Raines, "Analyzing Attack Trees using Generalized Stochastic Petri Nets." 2006 IEEE Information Assurance Workshop, 2006, pp. 116-123.

[33] Ole Martin Dahl, Limitations and Differences of using IPsec,TLS/SSL or SSH as VPN-solution. [ole.dahl@hig.no]. October 29, 2004.

[34] G. Coulouris, J. Dollimore and T. Kindberg, "Distributed systems, Concepts and Design", Addison Westley, 2001.

[35] www. Mscs.mu.edu