A Study on Various Types of Remote Attacks and Solutions Proposed in Internet Banking

Dr. Amit Chaturvedi*, Asha Meena**
*Assistant Prof. MCA Deptt., Govt. Engineering College
**M.Tech scholar, Bhagwant Univ.,
Ajmer, India

***Abstract*: The banking industry is one of the fastest growing sectors realizing the developments and changes in the field of technology innovation. Demand on web based banking products increased as a result of expanding customer service focused understanding, decreasing attainability cost, its competitive market structure and consumers' wish to reach banking products fast, effective, and productive way. In this paper, various types of remote attacks and solutions proposed are analysed. Among them major attacks are for DNS hijacking, in this attacker modify the registered details of the domain and were redirected to false sites. No solid fail-proof solution exists yet, and most probably would not exist in the near future. This is due to the nature of the attack, which abuses some DNS capabilities and by disabling the capabilities, the site lose many beneficial DNS usage. Some of the defenses are proposed but not very effective.**

Keywords— halftone visual cryptography(HVC), visual secret sharing(VSS),error diffusion.

I. INTRODUCTION TO INTERNET BANKING

Online access to services either, banking, marketing, etc. is increasing worldwide. Internet banking is emerging continuously for online transactions and access of bank accounts under the finger tips of bank customers. Online banking is an essential service of banks to their customers. In today's e-world no bank is able to survive without providing the internet banking services. Internet Banking is a term used to describe banking transactions that are performed via a secured Internet applications. Internet Banking transactions include things such as paying bills, transferring funds, viewing account statements and paying down loans and mortgages. Although Internet Banking has been popular among young Internet-savvy people for many years, its popularity is expected to grow rapidly as Internet usage grows internationally and people discover the many advantages that it provides. Online banking includes conventional and virtual banks, e-banking services, Internet security and some cost/benefit considerations.

The banking industry is one of the fastest growing sectors realizing the developments and changes in the field of technology innovation. Demand on web based banking products increased as a result of expanding customer service focused understanding, decreasing attainability cost, its competitive market structure and consumers' wish to reach banking products fast, effective, and productive way. Electronic banking provides an important competitive advantage to the banks in terms of time, location and cost. Currently there is a clear need for efficient security models by banks which offer online access to their banking systems. As the growing number of transactions processed through online banking systems, several new security technologies and models which aim to provide authenticated secure communications through known insecure channels have been introduced in current literature.

But, with Growing facilities there are lot of threats for internet banking security and some are common like Phishing, snooping, intruders and so on. One of the major concerns when purchasing online and accessing financial information is security. The bank created several layers of security to prevent hackers from Customer's information. However, these threats on security resulted in various other security threats. The number of malware focused on exploits online banking systems vulnerabilities has been steadily growing during in recent years. Recent reports indicate that banking Trojans were among the 50 main security threats in 2009, while Brazil figures as the source and destination of most of those attacks performed in Latin America.

II. TYPES OF REMOTE ATTACKS

There are various identified remote attacks in internet banking. They are described below.

Phishing and Vishing: Phishing is a term used to describe spoof emails and other technical ploys to trick receipts into giving up their personal or their company's confidential information such as social security and financial account credentials and other identity and security information. This form of identity theft employs both social engineering and technical subterfuge to steal account access information, identity or other proprietary information that can be sold on to

third party via specialized chat rooms established specifically for the purpose of selling such information. Selling the information on reduces the risk of being apprehended by minimizing the direct link between the hacker and those using the information to gain unauthorized access to accounts and profiting from them. Social engineering schemes use spoofed emails to lead customers to counterfeit websites designed to trick recipients into divulging financial data. Technical subterfuge schemes plant crime ware onto computers to steal credentials directly using key logging systems.

Phishing is a serious and increasingly prolific form of spam, and is one of the main tactics employed in business and consumer identity theft. Phishing actually comprises of two online identity thefts used together. In phishing scams, the identity of the target company-commonly a bank, online payment service, or other reputable business- is stolen first in order to steal even more identities: those of unsuspecting customers of the targeted company. [1]

Vishing is very old scam or banking fraud. In this banking scam or fraud, the attacker phones the bank customers and uses social engineering to trick the bank customers 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. One of the major Vishing attack is Cloned voice-banking systems.

Cloned voice-banking systems: All The banks are using systems for voice-banking that is why Vishing attacks came into existence. The main objective of these Vishing attacks clones these systems so that they sound the same as the official systems. There Emails are similar to those used in phishing attacks solicit customers to call a number and saying we are from your bank. Attackers 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.

EXISTING PHISHING METHODS

I. Domain Spoofing: Domain spoofing is famous technique in remote attacks, where attacker may use same website names as well as names that look similar to the actual domain to fool unsuspecting users into revealing bank's confidential information for example, in domain name they change few alphabets like lower case letter 'f' for capital letter 'F' because, they look similar but in domain names they are treat two different alphabets.
II. URL Modifying: Uniform resource locator phishing technique is another way to redirect web-requests to their own URL. The '@' symbol lets attackers redirect traffic to their own url as web browsers truncate all character before the '@' symbol. For example yahoo.com@192.160.1.1 will redirect to 192.160.1.1 without regarding the yahoo.com URL.
III. Website layout similarities: website layout similarities can also do the trick of phishing. Because of the same layout design, the user is not able to understand weather it is the same website or fake page with same design. For example if the attacker designs the same layout of facebook with same font size, color and same login details along with other backend facility. The common user will not understand that it the same page which he/she is using for social networking. Fake Website page is common trap for unprofessional users.

Types of Phishing Attacks

Phishing approaches used for identity thefts are constantly growing and new variants are tried and used to attack business organizations, financial institutions, and customers. Some of the most prevalent types of phishing attacks are presented here under.

- **a.** Deceptive Phishing
- **b.** Malware-Based Phishing
- **c.** Keyloggers and Screenloggers
- **d.** Session Hijacking
- **e.** Web Trojans Hosts File Poisoning Data Theft.
- **f.** DNS-Based Phishing also called Pharming
- **g.** Man-in-the-Middle Phishing
- **h.** Search Engine Phishing Spear Phishing
- **i.** Vishingor Voice
- **j.** Growth of Phishing Scams

2.2 **DNS Hijacking:** The first DNS Hijacking attack was experienced in America in 2005 [2]. The attack was implemented 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.

2.3 **DNS cache poisoning:** The concept of DNS cache poisoning is very simple. The user's DNS server sends a request to an authoritative DNS server asking for the IP address that matches a specific website address. But what if an attacker replies on behalf of the authoritative DNS server and returns the wrong IP address? If this happens the user's DNS server would return the wrong IP address to the user's computer and the computer would connect to the wrong web server. The user's DNS server would also cache this fraudulent response so that any other computer that asks it for the IP address would receive the fraudulent IP address. This attack is called cache poisoning as the DNS server's cache is now poisoned with the wrong IP address. In the early days of DNS this attack was very much possible. DNS was implemented on top of User Datagram Protocol (UDP), which is a lightweight, stateless protocol and anyone could have spoofed responses from authoritative DNS servers and poisons the DNS server's cache.

2.3.1 An Advanced DNS Cache Poisoning (Remote Attack) : The above attack assumes that the attacker and the DNS server are on the same LAN, i.e., the attacker can observe the DNS query message. When the attacker and the DNS server are not on the same LAN, the cache poisoning attack becomes more difficult. The difficulty is mainly caused by the fact that the transaction ID in the DNS response packet must match with that in the query packet. Because the transaction ID in the query is usually randomly generated, without seeing the query packet, it is not easy for the attacker to known the correct ID. Obviously, the attacker can guess the transaction ID. Since the size of the ID is only 16 bits, if the attacker can forge K responses within the attack window (i.e. before the legitimate response arrives), the probability of success is K over 216. Sending out hundreds of forged responses is not impractical, so it will not take too many tries before the attacker can succeed. To launch effective attacks, the attacker must negate the caching effect. Dan Kaminsky came up with an elegant method to do this.

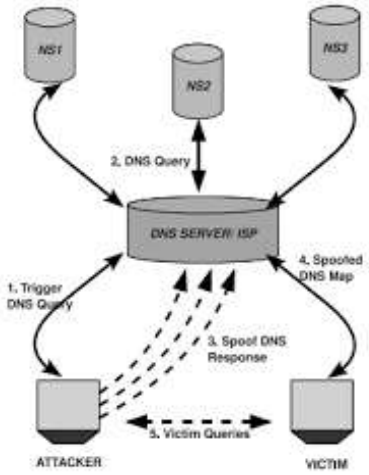

Figure 1: DNS - Phishing Attack Details

2.4 Voice over IP: Although voice over IP (VoIP) has been in existence for some years, service demands are forcing a rapid evolution of the technology. The pace of service integration (convergence) with new and existing networks continues to increase as VoIP products and services develop. Also, the promise of broadband services and the integration of voice and data at all levels further the need for VoIP applications. Critical to success is the ability to deploy value-added and high-margin services. VoIP and other IP-based technologies are best positioned to be the solution to realize these more profitable services. For example, you could deploy a unified messaging system that would voice synthesize e-mails over a phone to the subscriber. Though VoIP is still evolving, packet-based telephony is becoming more advanced. Voice protocols have further developed to offer a richer set of features, scalability, and standardization than what was available only a few years ago. Today, Juniper Networks, Inc. has solutions that enable you to deploy reliable, high-performance networks that support VoIP services [3].

III. SOLUTIONS PROPOSED FOR REMOTE ATTACKS

3.1 For Phishing Attacks:

3.1.1 Stop phishing at the e-mail level. Sending an e-mail and asking for somebody's bank account login details is a simple idea and its costs almost nothing. Each day more and more e-mails are sent with the aim of making the web users believe that the same is legitimate and from the trusted institutions. It asks the users to visit a spoofed site where they will be asked to provide their login credentials and at the end, the same will be used by miscreants for reaping financial and other benefits. As most phishing attackers send e-mails to lure victims to visit spoofed web site, one approach can be to stop this e-mail from getting delivered to the end-user.

In another work, Bergholz et al. (2010) describes new approaches, including statistical models for the low-dimensional descriptions of e-mail topics, sequential analysis of e-mail text and external links, the detection of embedded logos as well as indicators for hidden salting. Hidden salting is the intentional addition or distortion of Content not perceivable by the reader. During experiments of their work authors found that their methods outperformed other published approaches for classifying phishing e-mails.

Chandrasekaran et al. (2006) in their paper proposed a technique to discriminate phishing e-mails from the legitimate e-mails using the distinct structural features present in them. Their proposed solutions can be used to classify phishing e-mails before it reaches the user's inbox, essentially reducing the human exposure. However, the experiment base used during the work was not large enough to draw a broader conclusion. Also the classification approach adopted is only one of the many ways that could be employed, thus the choice of features plays an important role for the success of this approach. In another work Fette et al. (2007) proposed a machine learning approach to create a specialized filter named PILFER. In the new filter they used ten very specific features that are more directly applicable to phishing e-mails. They found their solutions to be more effective then available spam filters [5]. He et al. (2011) proposed a heuristic method to determine whether a web page is a legitimate or a phishing page. The solution is a combination of CANTINA (Xiang et al., 2011) method, anomaly method, and PILFER method (Fette et al., 2007), with several additions and modifications. The idea was that every web site claims a web page identity, either real or fake. If a web site claims a fake identity, abnormality may exist in a network space; therefore the proposed method could detect and differentiate between a legitimate and a phishing web site.

3.1.2 Security and password management toolbars. HTTP basic authentication protocol is vulnerable to phishing attacks because a client needs to reveal his password to the server that he wants to login. Most users have multiple password protected accounts over the internet. To avoid the headache in remembering and managing a long list of different and unrelated passwords, most users simply use the same password for multiple accounts. A phisher can effectively steal users' passwords for high-security servers, such as an online banking web site by setting up a malicious server or breaking into a low-security server, such as a high-school alumni web site. Gouda et al. (2007) proposed anti-phishing single password protocol. Proposed protocol allows a client to securely use a single password across multiple servers, and also prevents phishing attacks. The protocol achieves client authentication without the client revealing his password to the server at any point. Therefore, a compromised server cannot steal a client's password and replay it to another server. Although password is one of the most commonly adopted means to protect user accounts, most users are used to giving away the same very easily.

3.1.3 Restriction list, Malicious or the spoofed web sites are the core problem of the phishing activities: There have been various efforts to restrict users from visiting these sites. Blacklist is one such effort, where the web browsers check the URLs against a list of URLs of known phishing sites. Upon finding the requested URL on a blacklist, the system restricts access and/or generates a warning indicating the danger of a phishing site. These blacklists are constructed using a range of techniques including manual reporting, link analysis, honey pots, and web crawlers combined with site analysis heuristics (Ma et al., 2009; Zhang et al., 2008). Blacklist approaches have long been used in other areas such as detection of spam e-mail (Jung and Sit, 2004).

A spam blacklist of IP addresses can restrict delivery of spam e-mail to large extent, but a similar restriction list is not possible in case of web site as there is a possibility that the IP address can have multiple domains hosted on the same. So a blacklist of specific URLs is a better solution in case of phishing or spoofed web sites (Sheng et al., 2009). However, blacklists have a major drawback; it is mainly a reactive approach. Blacklist maintainers learn of phishing web sites only after these sites have become active. Thus, a window of vulnerability remains during which users can suffer from malicious exposure because an active entity has not yet appeared on a blacklist (Felegyhazi et al., 2010). To solve this inherent problem of blacklist Prakash et al.

3.1.4 Visually differentiate the phishing sites : Detecting phishing web pages is similar to the problem of detecting duplicate documents and plagiarism, except that these focus on text-based features in similarity measurement, whereas phishing-page detection should focus more on visual similarities (Liu et al., 2006). To differentiate between the legitimate web site and the phishing one, dynamic security skins (DSS) a new class of human interactive proofs (HIPs) that allow a human to distinguish one computer from another, has been proposed which requires users to verify visual content from the server. The rationale is that the server should have the possibility to determine whether the SSL/TLS session in which it receives the credentials is the same as the one the user employed when he sent out the credentials in the first place. If the two sessions are the same, then a session is directly established between the user and the server, whereas if they are different, then an MITM attack is likely to be taking place. With the help of TLS-SA the server can recognize this and drop the session.

Sakilkar and Saha (2008) presented a completely automated public Turing test to tell computers and human apart (CAPTCHA) solution as phishing defence which embed public key information inside CAPTCHA that client side can verify the public key as well as the destination server. However, if user is such unconscious, force validation is needed; their design requires client side installation. As their CAPTCHA challenges are customized for each user in database and create a specific image list pair for each client, it also further induces database storage issues for growing number of customers, as well as client image list revoke or recovery issues after an attack. Leung (2009b) in his work demonstrates the limitation of CAPTCHA as well as visual security in securing online banking with a series of test on a CAPTCHA implementation of a local bank. The study shows how CAPTCHA can be bypassed. In his other work Leung (2009a) proposed an extended CAPTCHA input system to depress phishing by utilizing the properties of CAPTCHA combining the time restriction of one-time-password (OTP).

3.1.5 Two-factor and multi-channel authentication : Traditionally passwords are used for authentication in any online web sites. One has to memorize the password for that site and provide the same on demand by that web site. If a third party gets to know the password then the said account is compromised (Bose and Leung, 2007). In order to solve the problem faced with the usage of passwords researches have proposed two-factor authentication. In two-factor authentication process, user should prove "what he knows" and "what he has". Here what he knows is the password, and what he has is something that only the genuine user will have. This something can be a hardware token given by the institutions which can generate PINs (Nilsson et al., 2005), or a OTP (Molloy and Li, 2011; Yang and Choi, 2010) or some personal certificate or documents which only the user can have. Though the cost of implementation will be very high one can consider biometrics based authentication also (Zviran and Erlich, 2006). With the help of OTP and separate boot USB or CD, Martino and Perramon (2010) proposed multi-factor mutual authentication.

First, the server is authenticated and next, if the result of the server authentication is successful, the user will provide his credentials. In this manner user credentials are prevented from being stolen by a hijacking server. In another work Adida (2007) proposed BeamAuth, a two-factor web authentication technique where the second factor is a specially crafted bookmark. While using BeamAuth user will be required to select a preconfigured bookmark in his client browser to authenticate himself. Many banks have altered their authentication mechanisms, suggesting their willingness to adapt and go beyond traditional and simple passwords (Herley et al., 2009). Mannan and Oorschot (2007) proposed to use mobile phone network to authenticate services on the internet through an un-trusted computer. On a similar line Mizuno et al. (2005) proposed user authentication using multiple communication channels. Their solution enables on-line service providers to strongly authenticate their users on a non-trusted communication channel via trusted communication channels.

3.1.6 Takedown, transaction anomaly detection, log files : Banks and other organizations deal with fraudulent phishing web sites by pressing hosting service providers to remove the sites from the internet so that there is nothing there for a misled visitor to see. The procedure is commonly known as take-down (Moore and Clayton, 2007). Most banks and specialist take-down companies maintain their own feed. PhishTank the online web site asks the end-users to visit their site and contribute to their source list (PhishTank, 2010). Users are invited not only to provide the content but also to verify that the entries are correctly classified. In another work Moore and Clayton (2008) gathered phishing reports from the PhishTank. After analyzing the data received from PhishTank authors concluded that any crowd-based decision mechanism like PhishTank remains susceptible to vote rigging and manipulation that
could undermine its credibility. Moore and Clayton (2007) studied the empirical data on phishing web site removal times and the number of visitors that the web sites attract, and concluded that web site removal is a part of the answer to phishing, but it is not fast enough to completely mitigate the problem. By the time they are removed, the fraudsters learn the passwords; PINs and other personal details of the users who are fooled into visiting them.
In order to detect potentially fraudulent transactions, transaction anomaly detection systems are available. Bignell (2006) in his paper outlines a framework for internet banking security using multi-layered, feed-forward artificial neural networks. Such applications utilize anomaly detection techniques which can be applied for transaction authentication and intrusion detection within internet banking security architectures. It can combine user profiling with business rules to detect suspicious account activity. Suspicious transactions are alerted to the bank's professionals so appropriate reactive measures can be taken. Emigh (2005) in his report discusses the log analysis approach, which is the analysis of audit trails in order to detect phishing lures, hooks and catches. According to his report these mechanisms can dramatically improve a bank's responsiveness to phishing attacks. Indeed, if logs are monitored in real-time, extremely quick response times could be reached. Tracking the source of phishing attacks is a difficult challenge for investigators. The attacks are frequently launched from botnets comprised of infected, innocent users and web servers compromised by malware. Steel and Lu (2008) proposed Automated Impersonator Image Identification System (AIIIS), which allows investigators to track images used in impersonation attacks back to the original download from the source. AIIIS accomplishes this by digitally encoding the IP address server and the time of the image download into the image itself through a digital watermark. If this image appears on any site then it can be easily identified. Limitation. Take down effort is not going to be effective against fast flux (McGrath et al., 2009). Web sites using fast flux typically resolve too many IP addresses, each with a short validity. Successive site resolutions often lead to a new set of IP addresses, which increases availability.

3.1.7 Anti-phishing training : Core idea of anti-phishing training is that users can be trained to actively protect themselves from phishing threats. The United States Military Academy (USMA) has been very active in implementing hands-on exercises such as the cyber defence exercise (Dodge et al., 2003). They concluded that embedded training interventions helped teach people about phishing and how to avoid phishing attacks. In another paper Kumaraguru et al. (2007b) studied an embedded training methodology using learning science principles in which phishing education is made a part of a primary task for users. The goal is to motivate the users to pay attention to the training materials. In embedded training, users are sent simulated phishing attacks and trained after they fall for the attacks. They tested users to determine how well they retained knowledge gained through embedded training and how well they applied this knowledge to identify other types of phishing e-mails. They concluded that users learn more effectively when the training materials are presented after users fall for the attack (embedded) than when the same training materials are sent by e-mail (non-embedded). Kumaraguru et al. (2009, 2010) conducted research works which focuses on educating users about phishing and helping them make better trust decisions. They identified a number of challenges for end-user security education in general and anti-phishing education in particular. They developed an e-mail-based anti-phishing education system called "PhishGuru" and an online game called "Anti-Phishing Phil" that teaches users how to use cues in URLs to avoid falling for phishing attacks.

Sheng et al. (2010) conducted a role-play survey among 1,001 online respondents to study both the relationship between demographics and phishing susceptibility and the effectiveness of several anti-phishing educational materials. Their work shows that educational materials reduced users' tendency to enter information into phishing web pages by 40 percent, however, some of the educational materials they tested also slightly decreased participants' tendency to click on legitimate links. Another method for educating users is to send fake phishing e-mails to test users' vulnerability and then follow up with training. Subsequent fake phishing e-mails can be used to measure improvements in phishing detection abilities. This approach has been used by Jagatic et al. (2007) and has shown that education can improve participants' ability to identify phishing e-mails. They concluded that people can become less vulnerable by a heightened awareness of the dangers of phishing, the importance of reporting attacks to which they fall victims, the ease of spoofing, and the possible exploitation of personal information posted on the web. Lungu and Tabusca (2010) in their work underline the need for a higher degree of awareness related to safe network use and practices. They concluded that good user education is a key component for building up the trust necessary to overcome the phishing fears. It is evident that the problem of phishing is not going away in the near future. Therefore, the need stands for organizations to take proactive steps in educating their consumers about the potential risks of phishing.

3.1.8 Legal solutions: It is clear that phishing has become part of our social and technological reality. Active development of the necessary legislation is desperately required. Bainbridge (2007) and Larcom and Elbirt (2006) in their work stated that the law, however, must take proper notice of current technical risks as well as measures taken to counter them. Granova and Eloff (2005) conducted a detailed study on phishing experience and available legal frame work in both the developing and the developed world. Mcnealy (2008) in his paper examines the existing state laws in USA aimed at stopping phishing as well as the proposed federal legislation. He concluded that adequate legal solutions would enable severe punishment of those caught phishing; the law also would allow both the victims of a phishing scam and companies whose informations were fraudulently used, to collect damages. Bose and Leung (2009) found that in Hong Kong Government advocacy for adoption of antiphishing measures influenced the adoption of two-factor authentication by banks. Larson (2010) in his paper recommended that courts should consider either large-scale damages against individual phishers or secondary liability against internet service providers (ISP) under the areas of either intellectual property (IP) or unfair competition law.

3.2 Defense & Precautions against DNS Hijacking : As of defenses and precautions for DNS Rebinding, No solid fail-proof solution exists yet, and most probably would not exist in the near future. This is due to the nature of the attack which abuses some DNS capabilities which are also used in many peaceful scenarios, and by disabling all those capabilities, the owner lose many beneficial DNS usages. There are a few defenses described here, why these defenses are ineffective against Rebind-Hijack in general:

a. **Fixing Firewall Circumvention :** This defense employs a tool such as **dnswall** that won't let external hostnames to be mapped to internal IP ranges. This precaution would disable VPNs, Since VPNs return their own websites IPs as internal IPs.

b. Fixing Plug-ins :

- **Flash Player :** Requiring a policy for every socket connection for Flash Player would require all Flash Movie servers to patch themselves, Which would not be backward compatible thus requiring a very long time to propagate, As well as a much slower Flash interactivity.
- **Java :** The Java defense requires all Java applet clients and servers to be patched, Which is - considering the Java nature - almost impossible. Many Java applets are really old and have not so clean codes to be patched.

b. Fixing Browsers :

- **Host Headers :** Host Headers makes web servers check for the Host in HTTP headers and validate it with their own (usually employed to enforce Virtual Hosts). This is in fact a very intelligent approach, And is a de-facto standard now, But has nothing to do with Rebind-Hijack since the malicious server can just ignore it and the original server is contacted by its own IP.
- **Finer Grained Origins :** As explained before, This would prevent many correct DNS usages currently under heavy traffic over the web, And the user would have no idea what is wrong with the web site.
- **Smarter Pinning :** Could be bypassed by anti-pinning approaches, and would not impact the attack much, since Rebind-Hijack requires a few rebindings.
- **Policy Based Pinning :** Almost the same as reverse DNS lookup, This is content to much debate both in Internet infrastructures and DNSSEC workgroups [6].
- **Trusted Policy Providers :** This is also included in DNSSEC and is content to debate, But even when implemented, Provides backward compatibility for older DNS servers. The generous people at [1] also stated that none of these defenses (or even the sum of them) are a 100% fail proof cost-effective way of defending against DNS Rebinding without losing much as well. We suggest, As suggested before [14] the only effective defense against DNS Rebinding is general awareness. The fact that the authorities prevented [2] from general publication due to the high risk for as long as ten years, And all the obfuscation over this not so new threat, Only makes it harder and harder to guard against. Also general awareness is costly and requires a lot of security experts to put effort into the field, It is worth the cost since the original DNS Rebinding and the Rebind-Hijack attacks are very cost-effective with high risk and huge impact and should be prioritized as soon as possible.

3.3 DNS cache poisoning : Precautions to DNS Cache Poisoning Both Microsoft and ISC have issued patched DNS server versions that fix the transaction ID flaw. ISPs and enterprises are encouraged to apply these patches. Unfortunately there is no way to force ISPs and enterprises to app .ly such patches, and many tend not to do so for various reasons. This leaves a large community of consumers at risk from DNS poisoning attacks. Additionally these patches only solve a small part of a much larger problem – pharming. Pharming can be achieved in various ways including modifications to browser configuration and hacking into DNS servers.
DNSSEC provides a more comprehensive solution for Pharming. DNSEC stands for "Domain Name System Security Extensions". It is a standard that was defined well after the DNS RFCs were written, and as such, attempts to address many of The Threat of DNS Spoofing on Financial Services 7 the security weaknesses of the original DNS protocol, particularly DNS spoofing/poisoning. However, since DNSSEC became matured during an era where the original DNS protocol was already widespread, it suffered (and still suffers) from the bootstrap problem, resulting in very low adoption rate, and an unclear future. Server-side solutions are ineffective in preventing DNS cache poisoning and pharming attacks as they are out of the financial institution's control. Relying on ISPs to solve the problem is not the best alternative financial institutions have today. Client-side solutions on the other hand can provide strong protection against DNS Cache Poisoning and pharming.

3.4 Voice-over IP: VoIP is a technique for transmitting voice data over the Internet [7]. The following steps are performed:

- digitization of the analog signal, usually performed at a frequency of 8 KHz with 8 bit per sample, thus generating 64Kbytes per second;
- packet generation of the digital signal according to the TCP-UDP/IP protocols;
- transmission of the packets on the network;
- packet reception and analog signal reconstruction at the destination.

When sending voice traffic over IP networks, a number of factors contribute to overall voice quality as perceived by an end user. Some of the most important factors are end-to-end delay in the voice carrier path and degraded voice quality. Among the factors that degrade voice quality are packet loss, delay variation, or jitter, voice compression schemes, transducers (microphones and speakers), echo cancellation algorithms, and voice activity detection at voice endpoints.

3.5 IPsec: IPsec provides security services for IP traffic by allowing a host to set up a secure IP channel with any peer it wishes to connect to. The host can choose different services depending on the level of security required. The services provided by IPsec are based on two protocols: an authentication protocol (AH) and a combined encryption and authentication protocol (ESP). The first protocol provides services such as connectionless integrity and sender authentication, while the second protocol is in charge of guaranteeing confidentiality among other services.

In order to execute any of these algorithms both the peers have to have previously agreed on pairs of secret keys. Such an agreement is performed by the IPsec key management module implementing the ISAKMP/Oakley protocol. Such a module mutually athenticates the peers, then it negotiates the symmetric keys they need to exchange messages and the cryptographic algorithms they will use. IPsec encodes the information needed to perform AH and

ESP services in two additional packet headers called AH and ESP headers, respectively.

3.6 Quality of Service : When executing VoIP applications, QoS protocols must be adopted in order to be able to meet the requirements on transmission parameters such as transmission delay, jitter and buffering delay [8,9]. QoS protocols try to meet the imposed requirements using different features such as packet classification, queueing mechanisms, traffic shaping, header compression, congestion avoidance strategies and Resource Reservation protocols. Unfortunately, such features cannot be taken advantage in combination with IPsec, as they use fields in the IP header that IPsec encrypts. Thus, when IPsec is used, the possible choices of QoS protocols are limited.

IV.Conclusion

As there are various types attacks encountered in internet banking like phishing, vishing, cloned voice-banking systems, DNS Hijacking, DNS cache poisoning, and VoIP. These attacks are explained in this paper to improve the understandability of the scenario. Various solutions are proposed for the prevention from such attacks which are explained in the section 3: Solutions proposed for remote attacks. Among them major attacks are for DNS hijacking, in this attacker modify the registered details of the domain and were redirected to false sites. No solid fail-proof solution exists yet, and most probably would not exist in the near future. This is due to the nature of the attack, which abuses some DNS capabilities and by disabling the capabilities, the site lose many beneficial DNS usage. Some of the defenses are proposed but not very effective.

Future researcher may work in this very important area for improving the secured internet banking and for improving the customer's satisfaction in internet banking.

ACKNOWLEDGMENT

We are very thankful to the referees for their valuable suggestions that have helped immensely in preparing the revised manuscript and whose valuable suggestions made this paper better in quality and presentation.

REFERENCES

[1]. Banday, M.T., Qadri, J.A. (2007). "Phishing - A Growing Threat to E-Commerce," The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83.
[2]. K. Haugsness, "DNS Poisoning Summary", March 2005
[3]. Juniper Networks, Inc. 1194, Voice over IP. www.juniper.net
[4]. M. Goncalves, Voice over IP Networks. McGraw- Hill, 2000.
[5]. S Purkait, Phishing counter measures and their effectiveness – literature review, Information Management & Computer Security Vol. 20 No. 5, 2012, pp. 382-420
[6]. DNSSEC http://www.dnssec.net/ http://tools.ietf.org/html/rfc2535
[7]. U. Black, Voice over IP. Pretice Hall, 1999.
[8]. Microsoft, (2005), "Phishing: Highly Targeted Scams", Microsoft, Corporation December,2005.
[9]. DNS Client Spoof,
[10]. Using the Domain Name System for System Break-ins (Steven M. Bellovin AT&T Bell Laboratories).
[11]. M. Goncalves, Voice over IP Networks. McGraw-Hill, 2000.
[12]. P. Loshin, Big Book of IPsec RFCs: Internet Security Architecture. November 1999.
[13]. C.-N. Chuah, Providing End-to-End QoS for IPbased Latency-sensitive Applications. Technical Report, Dept. of
[14]. Electrical Engineering and Computer Science, University of California at Berkeley, 2000.
[15]. Sayeed, RSVP & its use for Voip. Cisco Systems.
[16]. Thompson, Voice over IP Quality of Service Architecture and Performance Requirements. Cisco Systems, ENG- 53391, May 2000.
[17]. DNS Rebinding, How to defend http://www.abiusx.com/dns
[18]. S Mathiyalakan, VoIP Adoption: Issues & Concerns