A Study on Cyber Crimes and protection

M.Loganathan[1], Dr.E.Kirubakaran[2]
[1] Research Scholar
Department of Computer Science
Vinayaka Missions University, Salem
TamilNadu, India,636308

[2] Additional General Manager
Outsourcing Department
Bharat Heavy Electricals Limited,
Tiruchirappalli, TamilNadu, India, 620014

Abstract – **Information technology has widened itself over the last two decades and has become the axis of today's global development. The world of internet provides every user all the required information and latest information making it the most valuable source of information. With the advancement of internet, the crime has also widened its roots in all possible directions which claim to be the biggest threat in the near future. The cyber crimes pose a threat to the under developed, developing and the developed nations as a whole. One such major cyber crime is Phishing. It targets not just big organization but also individual users. In this paper we explore the Cyber crimes, the online security vulnerabilities and the available strategies and techniques for protection**

***Index terms* – Security threats, Online Security, Cyber crime, Phishing**

I. INTRODUCTION

Crimes are as old as man himself and computer crimes are as old as computers themselves. The more advanced computers and technologies become, the more rise in computer crimes especially with the widespread of networks. People are very reliant on information systems and the Internet making them easy targets for cyber criminals. According to a report from McAfee based on a survey conducted globally on more than 800 IT company CEO's in 2009, data hacking and related cyber crimes have cost multinational companies one trillion US dollars. Cyber crimes take different forms and shapes and could be carried out, not only by using personal computers, but also through cell phones and PDA's.[1] To understand cyber crimes it is necessary to take a detailed view into the crimes

II. PHISHING

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details. Phishing often directs users to enter details in a fake website who's URL, look and feel are almost identical to the legitimate one. Even when using SSL with strong cryptography for server authentication it is practically difficult to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploit the poor usability of current web security systems.[2]

Once the attacker has established a realistic and convincing fake web site that mimics a trusted brand, their main challenge is how to divert users of a legitimate web site to the fake web site instead. Unless the Phisher has the ability to alter the DNS for a target web site (DNS poisoning) or somehow otherwise redirect network traffic. A technique sometimes referred to as Pharming, they must instead rely on some form of content level trickery to lure unfortunate users to the fake web site The better the quality of the lure, and the wider the net that can be thrown, the greater the chance of an innocent user mistakenly accessing the fake website and in the process potentially providing the Phisher with the victim's credentials or other personal data)

III. URL OBSIFUCATION

Using URL obfuscation techniques, the attacker tricks the customer into connecting to their proxy server instead of the real server.[2] For example, the customer may follow a link to http://www.mybank.com.ch/ instead of the original link http://www.mybank.com/

IV. PHARMING

Pharming is a hacker's attack aiming to redirect a website's traffic to another bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in Domain Name System's (DNS) server software. DNS servers are computers responsible for resolving the Internet names into their real addresses. Compromised DNS servers are sometimes referred to as "Poisoned". DNS cache poisoning is a maliciously created or unintended situation that provides data to a Domain Name Server that did not originate from authoritative DNS sources. Once a DNS server has received such non-authentic data and caches it for future performance, it is considered poisoned, supplying the non-authentic data to the clients of the server.

In recent years both have been used to steal the end user's identity information. Sophisticated measures known as anti-Pharming are required to protect against this serious threat. Antivirus software and spy ware removal software cannot guarantee to protect against Pharming.

V. ANATOMY OF PHISHING

A raw phishing message can be split into two components: the content and the headers. These components are commonly accepted as being the major components of a message.

1) Content: The content is the part of the message that the user sees and is used by phishing message producers to deceive users. It can be subdivided into two parts.

(i) The cover is the content which is made to look likea message from the legitimate organization, and usually informs the user of a problem with their account. Early phishing messages could be identified based only on their cover, due to imperfect grammar or spelling mistakes (which are uncommon in legitimate messages). Over time, the covers used in phishing messages have become more sophisticated, to the point where they even warn the users about protecting their password and avoiding fraud.

(ii) The sting is the part of the content that directs the victim to take remedial actions. It usually takes the form of a clickable URL that directs the victim to a fake website to log into their account or enter other personal details. We call this the sting, as this is the part of the content that inflicts pain, by means of financial loss or other undesirable action after the victim enters their details on the website. Typically the sting is hidden by using HTML to display a legitimate looking address, instead of the address of the fake website.

2) Headers: The headers are the part of the message which is primarily used by the mail servers and the mail client to determine where the message is going and how to unpack the message. Most users do not see these headers, but in terms of determining if a message is phishing or not, this part of the message can be quite useful. Headers can be subdivided into three parts based on the entities which add them to the message:

(i) Mail clients typically add headers such as "To:", "From:", "Subject:" and some client specific headers. Examples of mail client headers are X-MSMail-Priority, X-Mailer, and X-MimeOLE, Phishing messages may try to fake a particular header and in doing so, give away that the message is fake. For example, if the X-Mailer header indicates that a HTML message has been composed using MS Outlook but the message only contains HTML (without plaintext), this is an indication that the message is fake, as MS Outlook cannot send HTML only messages.

(ii) Mail relays will add headers along the path of the message. These are usually "Received" headers, which can be used to determine the originating IP of the message and the path taken by the message.

(iii) Spam-filters or virus-scanners will usually add headers to the message to indicate results of the tests run over the message. These headers can then be used by the receiving client to determine (based on a user-set threshold) what to do with the message.[3]

VI. MAN IN THE MIDDLE ATTACK

One of the most successful vectors for gaining control of customer information and resources is through man-in-the-middle attacks. In this class of attack, the attacker situates themselves between the customer and the real web-based application, and proxies all communications between the systems. From this vantage point, the attacker can observe and record all transactions. This form of attack is successful for both HTTP and HTTPS communications. The customer connects to the attackers' server as if it was the real site, while the attackers' server makes a simultaneous connection to the real site. In the case of secure HTTPS communications, an SSL connection is established between the customer and the attackers proxy (hence the attackers system can record all traffic in an unencrypted state), while the attackers proxy creates its own SSL connection between itself and the real server. For man-in-the-middle attacks to be successful, the hacker must re-direct the user to his proxy server instead of the real server.[2] This may be carried out through a

- DNS Cache Poisoning
- URL Obfuscation

VII. IDENTITY THEFT

Identity theft is undertaken by an individual or numerous individuals to facilitate criminal activity. [4] Specifically, it involves stealing another person's "identity"—personal and financial information—for the purpose of committing other crimes constituting fraud. More often than not, these fraudulent acts are perpetrated by someone known by the victim such as a relative, friend, employee, or coworker, etc. Further, the success of these criminal acts directly depends upon the victim not knowing about it and the perpetrator of the act having an authentic address (one, however, that is actually bogus for the criminal).

(i) Constructions of Identity

According to Finch (2003) "identity theft spans a wide spectrum of conduct and covers varying degrees of fraudulent behavior." p.86 She states that in considering the nature of identity theft, it is important and necessary to distinguish between individual, social, and legal constructions of identity, terms she developed based on the work of Goffman (1963). Clearly, her intent in making these distinctions is to establish a clear delineation between identity and identifiability. In her taxonomy, "Individual identity is concerned with the question of 'who am I'." It is "what most of us think of when we think of the deepest and most enduring features of our unique selves that constitute who we believe ourselves to be.". "It can be seen as the sense of self that is that is based upon the internalization of all that is known about oneself...Hence individual identity is more than simply self-perception; rather, it is a subjective construction of the self that is modified by reflections on the views of others and the individual's interactions in the social world. As such individual identity is not a static construction but one that is constantly evolving and readjusting in line with the individual's life experience." Social identity, on the other hand, is concerned with the question of 'what is the nature of this person.' [4]

While individual identity "can be influenced by the way an individual is received in society," social identity "is contingent upon the way in which individuals present themselves." "For Goffman, social identity is based upon the categorisation of an individual to determine the acceptability of the membership of certain social groups." The key point to consider here, according to Finch, is that while both individual identity and social identity may be affected by identity theft, neither can be stolen. Legal identity is of concern in discussions of identity theft, because given its "fixed" and "immutable" nature; it has the greatest potential of being abused. Legal identity is concerned with the question of 'who is this person.' and "is more concerned with identifiability rather than identity as it seeks to make the link between a collection of facts and the person to whom they relate. . Therefore, it is clear that "the legal construction of identity gives primacy to factual information regarding an individual; information that is largely unalterable." [4]

(ii)Traditional Versus Online Identity Theft

According to the better business bureau, "identity theft is more prevalent offline with paper than on-line." On-line channels are blamed in only 9% of cases. Traditional means of obtaining information fraudulently include:

(1) dumpster diving (going through trash bins for checks, credit card numbers, identification numbers, pins, passwords, social security numbers, mail, receipts, or other sensitive information);

(2) shoulder surfing (involving watching someone enter personal information or eavesdropping on personal conversation/information);

(3) insider abuse (stealing on the job, bribing employees, etc);

(4) and lost wallets or purses (providing access to credit cards, checks, etc).

Online Identity theft happens in a number of ways including:

(1) Social Engineering—where users are manipulated into giving sensitive information (also used in f-t-f);

(2) Phishing—As explained in detail in the previous section of this paper where a spurious site imitates a well-known site;

(3) Pharming— As explained in detail in the previous section of this paper where malware redirects traffic destined for a legitimate website to one which looks like the original site;

(4) and Hacking—where the perpetrator intrudes into the system illegally and steals files (can be a method that is part of phishing or pharming).[4]

VIII.SOCIAL ENGINEERING

Social engineering is the practice of manipulating users to obtain confidential or sensitive information. Rather than exploiting the security of the technology, the social engineer exploits the weaknesses of the human user to trust the manipulator. It can apply to either to face-to-face, telephone, or internet manipulation to gain access to the physical computer itself or the information on it. Advance-fee scams (i.e. 419 scams) are an example of social engineering. The scam artist, pretending to be anyone from a government official to a surviving spouse, uses fee solicitation to acquire personal information with the promise of sharing inheritances, lottery winnings, and other sums of money. They play on the goodness and compassion of the victim with poignant stories, polite rhetoric, and the "guarantee" of financial gain for all involved. It usually involves the victim first being persuaded to open an e-mail attachment, followed by a malicious attack on the victim's computer, and the victim's computer or information then being used for criminal purposes, be it sending spam or stealing identities.[4]

IX. PROTECTION FROM PHISHING ATTACKS

There are several technical and non-technical ways to prevent Phishing attacks:[2]

1) Educate users to understand how Phishing attacks work and to be alert when Phishing-alike e-mails are received.
2) Use technical methods to stop Phishing attackers.

In this paper, we only focus on the technical aspect. Technically, if we can cut off one or several of these steps that are needed by a Phishing attack, we then successfully prevent that attack. In what follows, we briefly review these approaches:

A. Detect and block Phishing in time

If we can detect the Phishing Web sites in time, we can block the sites and prevent Phishing attacks. It's relatively easy to (manually) determine whether a site is a Phishing site or not, but it's difficult to find those Phishing sites out in time. Here we list three methods for Phishing site detection:

B. DNS Scan

The web master of a legal web site periodically scans the root DNS for suspicious sites. (e.g. www.icci.com vs. www.icici.com)

C. Enhance the security of the web sites

The business websites such as the web sites of banks can take new methods to guarantee the security of users' personal information. One method to enhance the security is to use hardware devices. For example, the Barclays bank provides a hand-held card reader to the users. Before shopping in the net, users need to insert their credit card into the card reader, and input their (personal identification number) PIN code, then the card reader will produce a onetime security password, users can perform transactions only after the right password is input. Another method is to use the biometrics characteristic (e.g. voice, fingerprint, iris, etc.) for user authentication. For example, Pay pal had tried to replace the single password verification by voice recognition to enhance the security of the Web site. With these methods, the Phishers cannot accomplish their tasks even after they have gotten part of the victims' information. However, all these techniques need additional hardware to realize the authentication between the users and the websites, which hence will increase the cost and bring certain inconvenience. Therefore, time is needed for these techniques to be widely adopted.

D Install online anti-Phishing software in user's computers

Despite all the above efforts, it is still possible for the users to visit the spoofed web sites. As a last defense, users can install anti-Phishing tools in their computers. The anti-Phishing tools in use today are categorized as: blacklist/White list based.

• Blacklist/White list: When a user visits a Web site, the anti-Phishing tool searches the address of that site in a blacklist stored in the database. If the visited site is on the list, the anti-Phishing tool then warns the users. Though the developers of these tools announced that they can update the blacklist in time, they cannot prevent the attacks from the newly emerged (unknown) Phishing sites which pop up in the internet frequently.[2]

X. BIOMETRICS

In addition to using antivirus software, firewalls, digital signature ... etc. to protect from cyber crimes, biometrics is used. Usually there are three different security measures used to authenticate or identify a person. [1]

1) What a person remembers: like password, personal identification number or any other keyword.

2) What a person can carry: smartcard, card key, token ... etc.

3) The person himself: the biological aspects like finger print, face, iris, or sound and that is called biometrics.

Biometrics is authentication techniques used in computer security in trying to stop cyber crimes. There are different methods of identification used. We will detail two of them:

1) Fingerprint: examination of unique fingerprints.

2) Palm Geometry: examination of the shape of the hand and fingers.

3) Voice: examination of the tone, pitch and frequency of voice.

4) Signature: examination how a person signs his name.

5) Retina: examination of the capillary vessels located at the back of the eye.

6) Iris: examination of the colored ring around the eye's pupil and this is done not by using infrared or any other type of rays but a simple camera and a person can even stand away from it. Each person of us has a unique iris that never changes as we grow old unlike the retina that does change.
The iris scan is not affected by contact lenses, eye glasses, refractive surgery, cataract surgery or cornea transplant.. . etc.

Some airports around the world have already started implementing the iris biometrics technology. The first airport to implement iris scanning technology was CharlotteDouglas International airport in North Carolina USA. By using a normal camera that shoots 30 frames per second in black and white, the images are digitized and stored in a database. The iris code with the person's name and journey details are stored on a hard drive in a 512 bytes file and a resolution of 640x480.

7) Face: examination of facial characteristics. The distance between the eyes, width of the nose, depth of the eyes, and shape of the cheeks ... etc, more than 80 nodal points are reported to a database. All these nodal points are represented by a special number for each face and stored in the database. A total of 14 to 2 2 nodal points are enough to identify a person.

This works in five different stages:

a) Detection: the software will identify the face within the range of a video camera. 2010 International Conference on Networking and Information Technology

b) Alignment: it automatically adjusts the alignment to store the details of the position, size, type ... etc of the detected face.

c) Normalization: the software will try to normalize and to fix the image by correcting the size, or to rotate the image of the detected head with the proper background.

d) Representation: all the nodal points of the face are represented as a unique number.

e) Matching: the new collected-detected data are compared with the database for matching.

The image is stored as an 84 byte face print file and could be compared to other face prints in a huge database. The software can compare six million face prints/minute from the memory or 1.5 million/minute from the hard disk. Faces are used as passwords to enter into restricted areas or any site where a password is required.[1]

XI. FUSION CENTERS

Fusion centers were created in order to provide the capability to examine seemingly disparate pieces of information and to draw from them a picture of a pending or future attack. Fusion is the key term and, according to the DHS/DOJ Guidelines, means “turning information and intelligence into actionable knowledge.” “Actionable” is the key term in this description. For fusion centers to be successful they need to not just produce vast quantities of information and reports but should instead produce knowledge that is actionable – knowledge and information that leaders can use to take actions that could prevent an attack from occurring. Again from Proceedings of the 41st Hawaii International Conference on System Sciences - 2008 2the DHS/DOJ guidelines we read that “For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across all levels and sectors of government and private industry. It goes beyond establishing an information/intelligence center or creating a computer network.

The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs.” This passage introduces the idea that fusion centers do not just rely on government organizations but have a private industry component as well. Building upon this idea the guidelines continue and state “data fusion involves the exchange of information from different sources—including law enforcement, public safety, and the private sector—and, with analysis, can result in meaningful and actionable intelligence and information. The fusion process turns this information and intelligence into actionable knowledge.” What this fundamentally means is that for fusion centers to function, they need to be gathering information not just from law enforcement and intelligence agencies but from industry and the private sector as well. To this effect, the guidelines later state “ideally, the fusion center involves every level and discipline of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances.” This is an important concept that becomes even more critical when considering cyber issues later.

The guidelines refer to the “fusion process” several times. This process is, quite simply, the steps necessary to turn information into actionable knowledge. The fusion process will:

- Allow local and state entities to better forecast and identify emerging crime and public health trends.

- Support multidisciplinary, proactive, riskbased, and community-focused problem solving.

- Provide a continuous flow of intelligence to officials to assist in developing a depiction of evolving threats.

- Improve the delivery of emergency and nonemergency services.

Building a fusion center capability is a phased process. This was true for the development of the initial creation of the fusion center concept and is equally true as entities develop their own fusion capability. The first phase is the introduction of the law enforcement and intelligence component. This is the backbone of every fusion center. The center will rely on individuals who have the training to perform an analysis of disparate data in order to form clear pictures of what might be indicated.

The second phase of building a fusion capability is the incorporation of public safety elements. This primarily means incorporating inputs from traditional first responders within communities. It also includes individuals from the transportation, agriculture, and environmental protection sectors as well.

The third phase in constructing a fusion center capability is the inclusion of the private sector component. This last phase is critical to the success of fusion centers. Nearly 85 percent of the critical infrastructures needed by the nation on a daily basis are found in the private sector. But it is not just the critical infrastructures found in the private sector that are included in the final phase of building a fusion capability, it also includes private citizens and their inputs. Similar to the concept of the neighborhood watch program found in communities around the nation, private citizens can aid fusion centers by maintaining a certain level of vigilance in observing when abnormal activities occur within their communities. Law enforcement personnel and first responders can't be everywhere; citizens need to shoulder some responsibility for maintaining the security of the communities in which they live.

What citizens, the private sector, and the first responder community bring to the fusion center process is the gathering of data that will be examined by the intelligence analysts who will transform the various pieces of information into the actionable knowledge that we keep referring to. For conventional attacks and weapons of mass destruction, what information is needed is a fairly well understood process. (That is not to say that it is an easy process, just that we can describe what needs to occur for the process to be successful.) In intelligence terminology, what is being searched for are the various “indicators” of a pending attack. In the cyber realm this is a different matter. Very little has been done in terms of incorporating cyber into fusion centers and little is understood about what constitutes an indication of a potential cyber attack. Put simply, what is needed is a list of the things that people should be looking for and reporting on that would serve to indicate an attack may be in the planning or early stages of the execution process.[5]

XII. CONCLUSION

Cyber Crime becoming a serious security threat which causes loss of sensitive data like passwords, credit card information etc. which in turn causes loss in billions of dollars to both consumers and e-commerce companies. In this paper a detailed study has been made on the existing Cyber crimes and the available mechanisms which are used to counter attack the crimes. On a complete study, it is fair to say a new revolutionary technique is the need for the hour which will incorporate cyber laws into the technological ream to counter attack the cyber crimes to a greater extent.

ACKNOWLEDGEMENT

The authors would like to thank the Lord God Almighty for pouring his grace and strength upon us. Next, we would like to thank Vinayaka Misson University. We would also like to thank Bharat Heavy Electricals Limited for its valuable contribution and continuous motivation.

REFERENCES

[1] Alex Roney MathewDepartment of Information Technology,College of Applied Sciences, NizwaSultanate of Oman, “Cyber Crimes: Threats and Protection”; 2010 International Conference on Networking and Information Technology

[2] K.Nirmal, S.E Ewards, K Geetha, “Maximizing online security by implementing a three factor authentication to counter attach Phishing”; INTERACT Conference

[3] Danesh Irani, Steve Webb, Jonathon Giffin and Calton PuCollege of Computing Georgia Institute of TechnologyAtlanta, “Evolutionary Study of Phishing”; eCrime Researchers Summit, 2008

[4] Rae Carrington SchipkeDepartment of EnglishCentral Connecticut State University, “The Language of Phishing, Pharming, and OtherInternet Fraud—Metaphorically Speaking”; Technology and Society, 2006. ISTAS 2006

[5] Natalie Granado, Gregory WhiteCenter for Infrastructure Assurance and SecurityThe University of Texas at San Antonio, “Cyber Security and Government fusion Centers”