White-hat Hackers Contrary to Cybercrime In Context to Indian Banking Sector

[1]Ms. Swati Prajapat, [2]Dr. Nupur Ojha
[1]Research Scholar, [2]Assistant Professor
[1]School of Business and Commerce,
[1]Manipal University Jaipur, Jaipur, India

Abstract : This paper explores the fast growing Cyber world and its penetration in the Indian financial institutions. Financial institutions mainly banks has emerged cyber world in its day to day routine. But, this inclusion in the Indian banking sector has become one of the major hurdles. According to the survey report of "Internet World Stats", India has positioned second following China. This report has showed that about 9% increase in the internet uses has been noticed by 31st December, 2017. With this increase, cybercrime is also growing continuously. In this paper, cybercrime and its security has been focused upon in context to Indian banking sector. It also conceptualizes on the role of white-hat hackers to reduce the vulnerability caused due to cybercrime.

***IndexTerms* - Indian banking sector, cyber world, cybercrime, vulnerability, white-hat hackers.**

I. INTRODUCTION

Indian banking sector is making a tremendous effort to emanate equivalent to developed economy. This effort has made the Indian banking sector to the world of cyber. Mostly the transactions of the Indian banks are carried out with the help of cyber. With the latest wits taken by the Government of India, the Indian banking sector is rapidly moving towards the complete digitalization in the recent years. The introduction of the cyber world in the Indian economy has uplifted the scope of banking sector globally. But, with the increase of involvement of cyber world, many hurdles have paved the way for cybercrime. It is a crime in which a computer is the object of the crime or is used as a tool to commit an offense. In this paper, an effort is inculcated to reduce cybercrime as cybercrime cannot be reduced rapidly. It also highlights the role of white-hat hackers against cybercrime.

1.1 Hacking

The word 'hacking' refers to the hobby or profession to work with computers. It can be described as a part of rapid development of new program of existing software to make code better and efficient[1]. It can be of two parts: ethical hacking and unethical hacking.

Ethical hacking, also known as penetration testing, intrusion testing, or red teaming, is the debated act of detecting weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers.

An Ethical Hacker, also known as a white-hat hacker, is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. Nowadays, certified ethical hackers are among the most sought after information security employees in large organizations.

1.2 Cybercrime

Cybercrime is the leveraging of a target's computers and information, particularly via the Internet, to cause physical, real-world harm or severe disruption of infrastructure[1]. Cybercrime is now amongst the most important revenue sectors for global organized crime[2]. Cyber-Crime incidents include but are not limited to credit card fraud, spamming, spoofing, e-money laundering, ATM fraud, phishing, identity theft and denial of service[3].

II. OBJECTIVE OF THE PAPER

- This paper identifies the various cybercrime variants which are increasing in the Indian banking sector
- It also highlights the various applications and illustrates its uses from the point of view of white-hat hackers on the Indian banking sector.

III. LITERATURE REVIEW

Indian banking sector has put a step forward towards digitalization. This digitalization scenario could not be possible without the help of IT department. Banks cannot imagine of introducing something new without the consult of Information technology. However it has an adverse level too [4]. Vulnerability information is serious for the safety of information systems everywhere. In India, the major cybercrimes reported are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber-squatting, cyber stalking and phishing [2]. However, the central bank of India, RBI, is taking measures to stop cybercrime. For this purpose, it has introduced 'Ethical hackers'. Ethical hacker refers to security professional who apply their hacking skills for defensive purpose and constructive purpose[1]. He also explained various tools through which ethical hacking can be done i.e. firewall, gateways, IPSec, DMZ, network auditing, etc. evaluating the breaches and mitigating them[1].

In spite of all these tools, white-hat hackers cannot control the cybercrime. Cybercrime is continuously increasing. On the other hand, black-hat hackers are extremely patient and will spend large amounts of time going after a goal [5]. Black Hats are not powerful but they know and use more tricks. Traditional White Hat testers are performing unrealistic tests to their customers which do not emulate what real attacks do[5]. We have to use every potential security dealings like Honey Pots, Intrusion Detection Systems and Firewalls etc. [6].

IV. CYBERCRIME VARIANTS AND INDIAN BANKING SECTOR

There are number of cybercrime variants. Some are discussed for the completion of the study. They are:

4.1 Cyber stalking

Cyber stalking is a crime in which the victim is harassed by the attacker by the way of e-mails and websites. It is different from spam as the attacker of the latter is focused upon a multitude of victims and in the former case a single user is targeted. In general, Stalking includes distressing or intimidating behavior that an individual engages in repeatedly. A cyber stalker depends on upon the secrecy afforded by the internet to allow them to stalk their victim without being detected[7].

4.2 Hacking

Hacking is very common crime in the Indian banking sector. It is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them[7]. It is an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers [4].

4.3 Phishing

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit cards details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Customers are directed to a fraudulent imitation of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account[7].

4.4 Cross site scripting

Cross-site Scripting is also pronounced as XSS. It refers to client-side code injection attack wherein an attacker can implement malicious scripts (also commonly referred to as a malicious payload) into a genuine website or web application. XSS is amongst the most widespread of web application vulnerabilities and occurs when a web application makes use of invalidated or unencoded user input within the output it generates. It includes HTML code and client-side scripts[7].

4.5 Vishing

Vishing is the fraudulent practice of making phone calls or leaving voice messages purporting to be from financial institutions or reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers. It is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial information from the public for the purpose of financial reward. It is the combination of 'voice' and 'phishing'[7].

4.6 Bot networks

A bot network, simply called as botnet, is a number of internet connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service (DDoS) attack, steal data, send spam, and allows the attacker to access the device and its connection. Bot networks create unique problems for financial organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts[7].

4.7 Credit card redirection and pharming

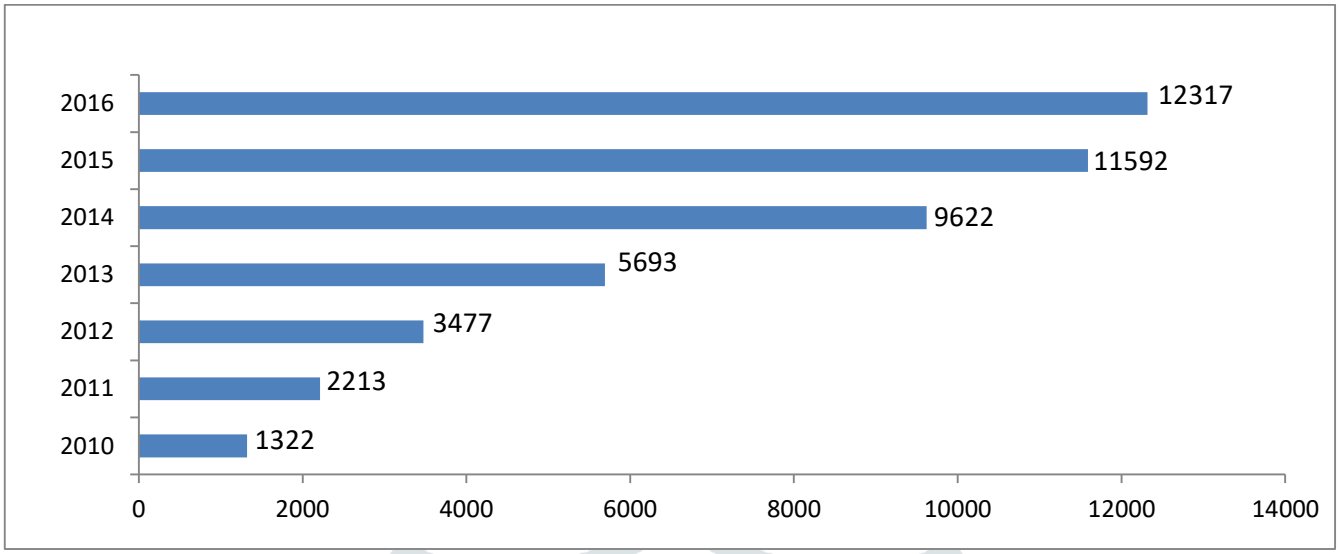
Pharming is linked with the words 'farming' and 'phishing'. In the case of Pharming, a bank's URL is take over by the attackers so that when a customer log in to the bank website they are redirected to another website which is fake but looks like an original website of the bank[4].

4.8 Malware based attacks

Malware is software aimed to secretly operate on a cooperated system without the consent of the user. It includes specific types such as ransomware, spyware, command and control, and more. It has been noticed that almost every virus has two features, one, that they secure a backdoor entry into the system and they steal credential information of a user[4].

V. GROWTH OF CYBERCRIME CASES IN INDIA (2010-2016)

Internet uses has penetrated to a high arena in the Indian economy. This usage has begun earlier but the cases of cybercrimes were not visible. According to the "Internet World Stats" survey, India has shown far-fetched record of the internet usage globally. The report of 2017 has reported a 9% hike in the use of internet and stood 2nd following China. This increase has boosted the scope of cybercrime too.



Sources: National Crime Records Bureau, Ministry Of Home Affairs, India [8]

According to the report of national crime records bureau, cybercrime has shown a boost during the period 2010 to 2016. This report also reported that Assam ranked 1st based on crime rate, followed by Maharashtra, Karnataka, Telangana respectively.

VI. Applications of Ethical Hacking

6.1 Surface Computing

Surface computing technology gives digital content a new facet where it is not constrained to just mobile phones or television sets. It is a technology in its initial stages, where even the engineers behind it cannot predict its full impact; but the possibilities are everywhere, underhand and underfoot and on every surface conceivable. This technology affords the users to discard with the mouse and keyboard and they could be replaced by more natural hand gestures on a large display screen where multiple users can interact simultaneously which will make computing and technology easier to use[7].

6.2 Cryptography

Cryptography is a technique of storing and conveying data in a particular form. It uses mathematics to encrypt and decrypt delicate information so that it cannot read by anyone other than envisioned recipient. It keeps private information protected from unauthorized access. It is process of converting plain text into cipher text using special keys at transmitting end and converting back cipher text to plain text at receiving end[7]. Cryptographic methods are used in number of applications including exchanging sensitive information in military applications, telephonic voting system to maintain confidentiality, anonymous digital cash systems implemented in help operations during natural calamities like floods, health care services using cell phone, internet or ATM, banks and law firms, digital data storage and communication in clouds etc.[7].

6.3 Steganography

Steganography is the hiding of a secret message within an ordinary message and the extraction of its destination. It takes cryptography a step farther by hiding an encrypted message so that no one suspects it exists. Anybody scanning your data will be unsuccessful to know it contains encoded data. Stenographic techniques can be used in confidential communication and secret data storing, digital certification used for protection of data alteration, access control schemes for content distributions like video film distribution by music companies, media database systems like photos, music, movies, Multimedia Message Service (MMS) etc.[7].

6.4 Watermarking

Digital watermarking is the method of inserting data into digital multimedia content. This is used to verify the credibility of the content or to recognize the identity of the digital content's owner. Watermarking techniques are efficiently used in copyright protection, remote sensing, military image processing, multimedia achieve management, etc.[7].

6.5 QR Codes

QR Codes is a matrix code. It is also called Bar Code. A recent implementation of QR codes is India's 'Aadhar' project that gives a unique identification number to the citizens of India much like the Social Security Number (SSN) in USA[7].

VII. Precautions Taken By White Hat Hackers

Indian banking sector despite hiring white-hat hackers are not totally getting out of the cybercrime. It is known that it cannot be stopped in a while but the efforts made are not positive. However, there could be some more points that can be added to the specific task of ethical hackers. A survey report of BT Global services has given some additional task that can be encroached in the IT department of the Indian banking sector. They are:

1. Assure to beat hackers at their own game.
2. To probe defences, uncover vulnerabilities and spot security gaps.
3. Ethical hacking services are useful to several new online product or service.
4. It can be get used whenever the bank's online properties, such as its corporate web site, go through an update or major change.
5. Currency transfer services, online money ordering mandates and more, all needs to get thoroughly checked before going live.
6. Ethical hackers should tests the bank's retail banking services.
7. When the team finds a problem, it needs to describe the risk, rates the severity of the issue and suggests remedial action.

As all the problems are not even in all the banking industry, so it needs to test standard industry applications used internally in the bank.

VIII. Conclusion

Banking industry has become a crucial field in the Indian economy. By the way of digitalization, banking sectors are trying to give various facilities to their customers. But due to this increased digitalization, crime is also paving the way out regardless the attempt made by the Indian banking sector. This paper tries to identify the various variants of the cybercrime and these are affecting the security issues of the banking sector. The applications viz., surface computing, cryptography, steganography, watermarking and QR Codes have high implications on digitalization. It has covered a larger proportion but yet to achieve. These applications for preventing data are also a type of ethical hacking for the banking industry and a solution too.

As most of the banking services have gone digitalized, it has become a top priority for the banking industry to hire an ethical hacker with proper knowledge and its execution over the matter.

References

[1] N. Rathore, "RESEARCH PAPERS ETHICAL HACKING & SECURITY AGAINST CYBER CRIME," no. January 2016, 2017.

[2] M. Goyal, "Ethics and cyber crime in india," vol. 2, no. 1, pp. 1–3, 2012.

[3] A. Manvikar, V. Joshi, and J. Guru, "CYBER-CRIMES : A Growing Threat to Indian Banking Sector," vol. 5, no. 1, pp. 926–933, 2018.

[4] Sanchi Agrawal, "' Cyber Crime in Banking Sector * ,'" *udgam Vigati- Orig. Knowl.*, vol. 3, pp. 1–19, 2016.

[5] V. Smith, "Why Black Hats Always Win," pp. 1–24, 2010.

[6] M. N. Munjal, "ETHICAL HACKING : AN IMPACT ON SOCIETY," no. May, 2014.

[7] A. S. Dr. B.K. Sharma, Dr. Pratima Singh, Saroj Bala, Sanjeev K. Prasad, Anuj K. Dwivedi, Anjali Singh, "cyber crime," *J. Comput. Appl.*, vol. 8, no. 1, pp. 5–51, 2017.

[8] N. Crime, R. Bureau, N. Crime, R. Bureau, and N. Crime, "Crime in India."