3G Widens the Scope for Cyber Crime in India

By Vivek Saini & Ashok Kumar Saini

NIMS University, Shobha Nagar, Jaipur

Abstract - The revolutionary decline in price and complexity of computers, laptops and mobile phone has changed the whole statistics of internet users. Considerable decline in price of internet charges also has contributed to the gigantic rise up of the curve of internet users. 3G introduction in India has act as a catalyst to the phenomena of rising the rectangular boxes in recent two or three year, so as the index of Cyber Crime.

3G WIDENS THE SCOPE FOR CYBER CRIME IN INDIA

Strictly as per the compliance and regulations of:

3G Widens the Scope for Cyber Crime in India

Vivek Saini [α] & Ashok Kumar Saini [σ]

Abstract - The revolutionary decline in price and complexity of computers, laptops and mobile phone has changed the whole statistics of internet users. Considerable decline in price of internet charges also has contributed to the gigantic rise up of the curve of internet users. 3G introduction in India has act as a catalyst to the phenomena of rising the rectangular boxes in recent two or three year, so as the index of Cyber Crime.

Keywords : cyber crime, 3G, India, virus, threats

I. Introduction

The 3G technology recently launched by the mobile service providers is in much rage nowadays. The 3G technology allows a user to access internet on a good quality network on the cellphone as well as on the computer. As such hackers will now target the 3G users for accessing their personal information and this in turn will result into increased cyber-crime.

Research shows that best cyber infrastructures can not prevent cyber crime to occur. This paper investigates the possibility of increase in the scope of cyber crime in India with the introduction of 3G technology.

II. India's Vulnerability To Cyber Crimes

With the advancement in technology, cyber crime rate has been doubling each year. In 2010, the Cyber Crime police station of the Crime Investigation Department (CID) has registered 54 cases. But, in the first three months of 2011, the CID has already registered 18 cases and combined with the newly launched Hyderabad and Cyberabad commissionerate police stations, the cyber crime cases registered this year is over 50 in the first three months alone. . The government said 386 'phishing' incidents were reported to the Indian Computer Emergency Response Team (CERT-In) between January and October 2011[1].

Most of the cases booked by the Cyber Crime sleuths fall under three categories: hacking, data theft and obscenity. Due to the high speed internet with features like video calling, mobile TV available with 3G technology, the amount of time an individual spends using internet on the mobile phone will increase and so

Author [α] : NIMS University, Shobha Nagar, Jaipur (Rajasthan)
E-mail : saini.vivek@yahoo.com
Author [σ] : Banwari Lal Jindal Suiwala College, Tosham, Bhiwani (Haryana) E-mail : drashokksaini2009@gmail.com

the vulnerability. Through a technique called `smishing' a hacker will send an SMS to the target, enticing him to click on a web link. Upon clicking the link, malware gets downloaded and settles in the mobile phone memory, enabling the hacker to read all the data stored in the phone.

a) Interesting Findings Of Norton Cybercrime Report

8% Indians do not expect to be cyber-crime victims ever as compared to 3% globally and 10% Indians feel that they are completely safe online.

57% Indians feel that cyber criminals will NOT be brought to justice as compared to 79% globally.

Once an individual has fallen prey to cybercrime, 58% of them change the way they conduct themselves online while very few individuals call Police or Banks to ensure safety!

It takes average of 44 days and Rs. 5262 to resolve a cybercrime in India, while globally the average is 28 days and over USD 334 (Rs. 13500 approx.)

55% of Indian online users have lied about their personal details as compared to 45% globally. 36% Indians have used fake online IDs (33% globally)

19% of Indian regret as to what they have done previously online and 41% believe that once your online reputation is ruined, nothing can be done about it.[2]

b) Internet User Statistics For India

Year	Population	Internet Users	Penetration
2006	1,096,780,312	26,846,957	2.45%
2007	1,111,696,524	35,607,411	3.20%
2008	1,111,476,292	47,779,667	4.28%
2009	1,119,256,061	63,457,201	5.67%
2010	1,162,300,000	77,641,640	6.68%
2011	1,220,200,000	121 million	9.91%

Table -1

Table-1 shows the statistics of internet users and internet user penetration data in India through different years. Here we can see a steep rise in the internet user statistics in India in recent years[4].

III. Primary Cyber Space Threats and Trends

a) Bandwidth Availability

The daily update of new virus definitions from Symantec[5] is around 130MB and McAfee's[6] is around 120MB. On a 56Kb dialup link, this can take all day to download. Although this restriction can cause frustration, it is an inherent type of risk proofing. From a business point of view, higher Internet speeds equate to more data being vulnerable to theft and other types of cyber crime. "Over a slow Internet link, it might have taken days to transfer even one 1GB of stolen data, but with 3G, the same can happen in minutes. Generally, the faster the link, the higher the amount of threats that might come. Fig. 1 shows the 3G services provided in different states in India by major operators.
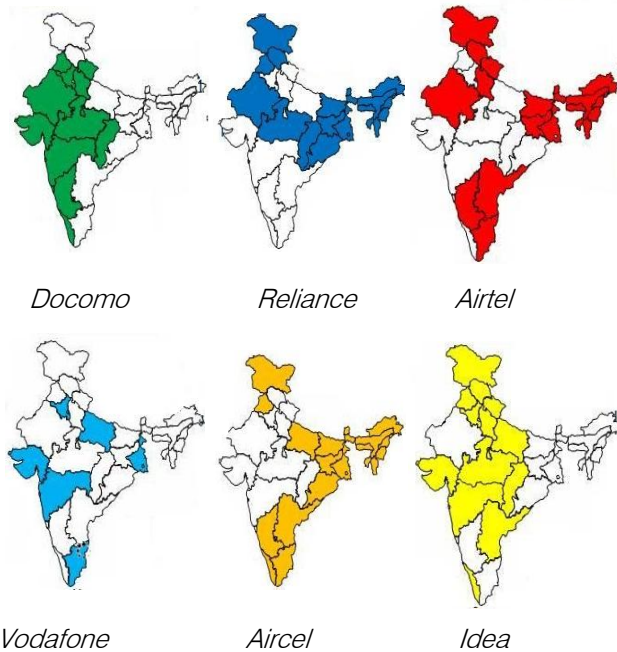

Docomo   *Reliance*   *Airtel*

Vodafone   *Aircel*   *Idea*

Fig. 1

b) *Affordable Hardware And Internet Charges*

Due to the steep decline in price of handheld devices and computers, these can be easily acquired by every person. And the price charge of high speed internet has made every Indian to a tech savvy person. The 3G rates in different circles of India are very cheap to afford. Here we are given the details of 3G Data Packages available on different 3G service providers in India (Table-2). A detailed price comparison of major 3G operators in India are presented in Table-2.[3]

c) *Absence Of Indian Languages*

Though the India is the second largest English speaking population in world. The absence of Indian languages in cyber space stands in direct relation to a shortage of IT education. It has a direct impact on the vulnerability of the Indian cyber space due to lack of cognizance.Though a mass of people have acquired computer skills, language is still a problem because the computer is dominated by English. In many instances, computer users willing to learn about cyber space are restricted to do this, because Indian languages are used minimally in cyber space. Many Indian computer users do not necessarily understand error messages or warnings about cyber fraud that are not presented in their mother tongue. As a result, the absence of Indian languages in cyber space poses a potentially serious threat to cyber space fraud and vulnerability to cyber space fraud.

d) *Third Party Application Vulnerabilities And Zero Day Exploits*

Third party applications are programs written to work within operating systems, but are written by individuals or companies other than the provider of the operating system. For example, Microsoft® systems come packed with several software applications. Of these, any program authored by Microsoft is a first party application. Any program authored by a different company or an individual is a third party application.

A zero-day (or zero-hour or day zero) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or the software developer. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability.

The term derives from the age of the exploit. A "zero day" attack occurs on or before the first or "zeroth" day of developer awareness, meaning the developer has not had any opportunity to distribute a security fix to users of the software.

e) *Social Engineering*

Social engineering is commonly understood to mean the art of manipulating people into performing actions or divulging confidential information. While it is similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victims.

f) *The Insider*

The insider threat or insider problem is cited as the most serious security problem in many studies. It is also considered the most difficult problem to deal with, because an insider has information and capabilities not known to other, external attackers. But the studies rarely define what the insider threat is or define it nebulously. A system administrator at a bank accesses a financial system that she is responsible for. She notices that Rs. 100000 was transferred from account 1011 to account 6734. The account of a close friend is number 6834. She moves the money to her friend's account, alters the original log file entry to change the number to that of the friend's account, and deletes the log entries showing the money being moved from account 6734 to account 6834. This seems to qualify as "unauthorized access by an insider".

IV. Secondary Cyber Crime Threats or Trends In India

a) Smishing

Through a technique called `smishing' a hacker will send an SMS to the target, enticing him to click on a web link. Upon clicking the link, malware gets downloaded and settles in the mobile phone memory, enabling the hacker to read all the data stored in the phone. Cyber crime police have been receiving several complaints from women about people blackmailing them using the intimate videos captured on web or cell phone cameras. Police are apprehensive that if an individual is not careful, video calling facility can also be misused in similar manner.

AIRTEL		IDEA		VODAFONE		RELIANCE		DOCOMO	
Data	Price	Data	Price	Data	Price	Data	Price	Data	Price
200 MB	99	100 MB	102	100 MB	109	--	--	10 MB	11
500 MB	200	250 MB	198	512 MB	375	--	--	25 MB	21
1200 MB	450	600 MB	450	3 GB	850	2 GB	749	50 MB	39
4 GB	750	1GB	598	5 GB	1250	5 GB	1199	100 MB	90
2.5 GB	675	2GB	749	1 GB	650	--	--	250 MB	201
10 GB	1250	3GB	850	6 GB	3250	--	--	500 MB	351
--	--	5GB	1250	18 GB	4250	--	--	1 GB	601
--	--	--	--	30 GB	6250	--	--	2 GB	751

Table – 2

b) Lack Of Anti Viruses

The hacker can record all the audio conversation and video files. Not many people in India install anti-virus in the phones. I would recommend them to install anti-virus and fireballs while using 3G and recommend switching off the bluetooth function of the phone when not required to protect the user's password. Due to high speed internet and lack of antiviruses in our system, crucial informations from our system can be easily hacked within seconds.

c) Film And Music Industry

Not limited to an individual's privacy issues, the 3G technology will also lead to increase in piracy of films and music, thereby giving a staggering amount of losses to the entertainment industry that is battling the piracy threat.

"It will become extremely easy for anybody to download an entire Bollywood film in few minutes using 3G. This is going to lead to further tremendous growth of websites like torrents," says advocate Pavan Duggal, a cyber-laws expert.

The Internet and Mobile Association of India (IAMAI) points out that Bollywood would be hit most by the 3G and wants service providers to adopt a stricter approach to check cybercrimes.

d) Absence Of Awareness Towards Internet

If we are to believe the official figures (1350 cybercrime cases in 2010 in India), then India is the most cyber secure country in the world, which is utter nonsense. Internet users in the country need to be educated about cybercrime. In many cases they might not even know that they have been a victim of cybercrime. The particulars of the law need to be made common knowledge. Cyber bullying is rampant in chat rooms and social networks. Children are most exposed to it and often not aware of consequences. Symantec Corp's Norton Cybercrime Report 2011 reported that four in five online adults have been victims of cybercrime in India.

e) Cyberwarfare

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare, although this analogy is controversial for both its accuracy and its political motivation.

India has received many threats of penetrating in the government computers and Indian networks for the purpose of causing damage or disruption. In an electronically linked world, nations are increasingly connected economically. In a war, destruction will be more severe and fatal if the economy collapses. And the recovery process after the war will be long winding. Cyber technology is the tool for such type of war. The future war, that is powered by cyber war, can create destruction effortlessly at the speed of light.And this speed is provided in terms of 3G services. One of the example is OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKED on 20 September 2007.

V. Influence of 3g On Cyber Crime

a) Influence Of 3G On Third Party Applications And Zero Day Exploit

With the increase in bandwidth the file transfer rate has been increased considerably. Hackers can now transfer more data in a single second. Now with the increased speed user can download third party applications with which he can have access to the others computers or mobile phones. Operating Systems

with patches are also available on the internet. So in poor contries like India people can download pirated versions of operating system and third party software easily with the help of large bandwidth internet.

b) Influence Of 3G On Social Engineering

With the increase in bandwidth and more and more people are joining into the cyber world the individual information are more prone to be attacked. For example, a person want to get the personal information of an individual, he can get it by the social networking sites(facebook, orkut, myspace, twitter) by hacking the account of that individual. A fake social networking site login page is sent to the user with an attractive link so that by loging into that page can send the user name and password of that user to the hacker. The fake login page is developed to do the so.

c) Influence Of 3G On Viruses

With the increase in bandwidth and more and more people are joining into the cyber world may potentially increase in the viruses, trojen horses and spam. Hackers can easily get into the remote computers and can infect a whole network with in seconds with the faster access of internet. With new reports suggesting that 3G subscribers will cross 107 million users in India by 2015 and most of the users would be virus infected.

d) Influence Of 3G On Film And Music Industry

With the increase in bandwidth and more and more people are joining into the cyber world may potentially affact the growth of Film and Music Industry. With high speed internet user can download a whole movie into a few minutes and song can be downloaded into few seconds. This is increasing the piracy of movies and songs. As the revenue is flowing to the illegal sites rather than the producer of movie or the songs.

e) Influence Of 3G On Cyberwarfare

Now-a-days nations have electronically connected all their economic, defense and national security establishments which will be the target for cyber attacks during a conflict or to create instabilities. With the increase in 3G user access these sites are more prone to attack as hacker can have more bandwidth and can destruct in more networks in less time.

VI. Defeating Cyber Crime In India

This research identified many areas where there are currently deficiencies in India's law enforcement response to cyber crime. Researches has shown that there is high volume of malicious computer activities in India. It is impossible to take counter measures to defeat cyber crime in India. Here we are suggesting some counter measures to defeat cyber crime in India like Emergency Response Teams, Cyber Security Awareness Campaign etc.

a) Cyber Space Initiative

A number of cyber space initiatives has to be taken to combat cyber crime in India. Speaking at the golden jubilee function of Karnataka State Bar Council President Pratibha Patil said: "Technology has thrown up issues which were unheard of a few years ago, like cyber crime and hacking. How to deal with these will require new thinking and new knowledge."

Initiatives such as the International Telecommunication Union (ITU) High Level Expert Group (HLEG) aim to develop strategies and guidance to countries in dealing with cyber crime.

The CBI chief said that during Noble's discussion with CBI officials, "we have broadly agreed that a CBI-Interpol Research and Innovation Centre for Prevention of Telecommunication Crime would be established in India".

One cyber space intitiative is Setting up Digital Forensics Centres (Cyber Forensics) where domain specific training could be provided.

Another cyber space initiative is One Laptop per Child.This initiative is trying to create educational opportunities for the world's poorest children by providing each child with a rugged, low-cost, low-power, connected laptop with content and specifically designed software. [More information on this initiative can be found at http://www.olpcindia.net/]

b) Indian Computer Emergency Response Team

Computer Emergency Response Team is a name given to expert groups that handle computer security incidents. CERT-In is operational Since Januray 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology Amendment Act 2008,CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

✓ Collection, analysis and dissemination of information on cyber incidents.
✓ Forecast and alerts of cyber security incidents
✓ Emergency measures for handling cyber security incidents
✓ Coordination of cyber incident response activities
✓ Issue guidelines,advisories,vulnerability notes and whitepapers relating to information security
✓ Ractices, procedures, revention, response and reporting of cyber incidents.

c) Cyber Security Awareness Campaign

For combating cyber crime, cyber security awareness should be created among the computer users in India. Department of Information Technology (DIT), Ministry of Communications and Information Technology (MCIT) has entrusted NASSCOM – DSCI

with the responsibility of implementing the Cyber Security Awareness Project across the country. As a part of the awareness campaign, DSCI conducted a series of events. The programs extensively covered audiences from industry sectors like IT/BPO, manufacturing, e-commerce, e-governance, telecom, banks, insurance and financial institutions, Public Sector Units (PSUs), law enforcement agencies like Police & Judiciary, Academia, Government, schools and colleges.

Indian government should come out with a PPP (Public Private Partnership) model, which includes government, private organizations and NGOs to make people more aware of the cyber attacks and increase the level of security. Through collective efforts – such as the sharing of threat intelligence and guidance, software providers making advancements in security protections and customers keeping their systems up to date, using genuine sofwares, will surely help in minimizing cyber crime while delivering a more safer and reliable computing experience.

Although cyber-security awareness among the people in India is on the rise, there is ample scope to expand awareness, which is possible through the PPP model.

VII. Conclusion

The paper examines the relationship between high bandwidth internet and the cyber security issues. With the rising number of cyber crimes, it is imperative to take specific counter measures to address crimes in cyber space. An increase in broadband access will give Internet access to more users in India. With the increase in broadband access, millions of new, computer-illiterate users will be able to connect to the internet through the 3G, potentially making the entire network more vulnerable to cyber threats and attacks.

Maintaining cyber security initiatives, establishing CERT-In and Cyber Security Awareness Campaign can help India defeating the Cyber Crime.

References Références Referencias

1. Analysis of phishing incidents, http:\\ http://www.cert-in.org.in
2. "Cyber Crime report 2011 by Norton Security" URL-http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/
3. Tariff plans for 3G services of various major telecom operators in India.URL-http:\\www.airtel.in, http:\\ www.vodafone.in,http:\\www.ideacellular.com,http:\\ www.tatadocomo.com,http:\\www.rcom.co.in.
4. "India Internet Statistics Compendium 2010" published January 2011, URL- http:\\www. estatsindia.com http://www.slideshare.net/Vicks18/ or india-internet statistics-e-statsindiacom-compendium-january-2011-pdf.
5. "Daily Updates of Symentec antivirus definitions" URL- http://www.symantec.com/security_response/definitions/download/detail.jsp?gid=n95
6. "Daily updates of McAfee antivirus definitions" URL-http://www.mcafee.com/apps/downloads/security-updates/security-updates.aspx
7. International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 July - December 2009, Vol 3 (2): 590–591.
8. Abe, Makoto. "Current issues and measures for prevention of cybercrime–Prosecution of cybercrime." *Keisatsu jihō* [Police times] 62, no. 2 (February 2007): 13–24.
9. Association for Information Service Industries: International Branch. "International trends in measures against cybercrime and the establishment of information security." *JISA Bulletin* 63 (October 2001): 77–90.
10. Babu, M., & Parishat, M.G. (2004). What is cyber crime?. Retrieved November 10, 2009,from http://www.crime-research.org/analytics/702/
11. CSI Computer Crime and Security Survey. (2008). Retrieved May 25,2009 http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
12. Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). CSI/FBI Computer crime and security survey. from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
13. Hashimoto, Naoki. "Current issues and measures for prevention of cybercrime." Sōsa kenkyū [Investigation research] 56, no. 2 (February 2007): 20–29.
14. National Police Agency. "On the prosecution of cybercrime." Heisei 19th [19th Conference] of the National Police Agency, 2008.
15. Charles Billo, Welten Chang "Cyber Warfare-An analysis of the means and motivations of selected nation states" published November-http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf.

Global Journals Inc. (US) Guidelines Handbook 2012