www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume1 Issue 1 Oct 2012 Page No. 48-52

Cyber Crime And Thier Solution

Titu kumar,Rohit kumar jha,Sitanshu Mohan Ray

Corresponding author:-Mr Rohit Jha Institute of Engineering &Management Salt Lake, Electronics ComplexSector-v, Kolkata-700 091 INdia Email: jharohit999@gmail.com

Abstract

This paper deals with the cyber crime & its realistic facts which blocked our working capability, efficiency & revealed the privacy of victims. This paper also deals with the futuristic cyber crime & its prevention.
We are very thankful to Prof. Sitanshu Ray for his tireless support and his lucid way of explaining us the salient points really helped us to write this paper.

Keywords- Cyber Crime, Cyber Space, Cyber Criminals , Weapons of Cyber Criminals, Futuristic Cyber Crime

I. CYBER CRIME

In every creation there are both good and bad sides but when a new one is created for the betterment of people the inventor does not think for its evil sides as great men always thinks for the betterment of society. In the year 1950s and1960s with the development of computers and the thinking power of scientist and research scholars when internet was invented for point to point communication between Mainframe Computers and terminals they did not think for its bad behavior as there necessity for creation was for noble purpose. At the initial stage it was known as ARPANET (Advanced Research Project Agency Network) and it was funded by US military for communicating and distributing information between geographically dispersed computers. With the advent of time Tim Berners Lee and Vinton Cerf took the lead to the birth of modern internet for the common people in the form of World Wide Web (www).

But the criminal mentality of human psychology started its misuse by using internet as a tool of crime, which gave the birth of the word "Cybercrime" and world is facing a huge challenge from these cybercriminals. The cybercrime is the crime, which occurs in the cyberspace. In cybercrime computer is used as a tool, a target, as incidental, and as associate.

Ii **Cyber Space**

"**Cyberspace** is the electronic medium of computer networks, in which online communication takes place." This term was first used by science fiction author William Gibson in 1982 in his short story "Burning Chrome" on the plot of two guys, who were software and hardware expert respectively and used to hack computer system for their profit. Cyberspace is not merely the operation of computers but also include all the virtual relationships and transactions that are carried out by those who enter the world through a computer in a virtual world.

III.CYBER CRIMINALS

Computer experts and persons, who are working is this field as an cyber crime investigator in the regular life have classified the profile of cyber criminals as follows;-

1) **Disgruntled Employees**: - A police officer during working in practical field as an investigator got some complaint about hacking and causing economic huge loss from the companies. Investigation revealed that this was the disgruntled employees of the complainant company, who was retrenched by the complainant company.

   Here is a real life case study from his personal experience. He got a complaint from an ITES company that someone hacked one of their customer's website and deleted the entire customer database of that company and the owner of that company resides in USA and he has suffered a huge loss for that. The complainant is liable for

this as they main the website with the Annual Maintenance Contact. Investigation revealed that it was their employee, who did so by sitting in his house. Then law took its own course.

In another case it was found that the HR manager of a company did not recommend fair increments for all the employees and as a result one of their employees hacked the computer of HR Manager by using internal network hacking technique and sent the entire future recommendation of the HR manager to the CEO of that company by sending mail from a cyber café.

2) **Teenagers:** - They hack or crack as an adventure and showing their expertise and due to ignorance they commit crime. Most of the person, who keeps news about science and fiction and internet they know that a teenager guy hacked the NASA website and Ankit Fadia, who is now a security expert, hacked Microsoft website when he was a teenager. Few months ago a Govt. agency of a country got an mail from a young guy of 15 years old " Your website is vulnerable and it can be penetrated by anyone and here is the vulnerability"

3) **Political Hacktivists**: - Sometime the political parties hire professional hackers for hacking the opponent parties' websites or important email ids for knowing their confidential information.

4) **Professional Hackers**: - They are the experts and find the vulnerability of the target in the internet always and hack for illegal gain or honest purpose for repairing the vulnerability. They are classified as 1) Black Hat hackers 2) White Hat hackers and 3) Grey Hat hackers.

5) **Business Rivals**: - Business rivals are like political hacktivists.

   Here is a real life case study from his personal experience. A complaint was received from a BPO company that three of his employees, who were deputed for non-technical administrative job, was caught red handed with the customer database and they suspected that they would do something wrong with that database. The suspects were interrogated and learnt that they unauthorisedly accessed the central database of foreign customers and had already sent the database by email to another company, who just started to run the new BPO business and some of those customers had already shifted to them.

6) **Ex-Boyfriend**: - Police department now a days are getting huge number of complaints from girls about this. They upload fake profile with photos of intimate moments, mobile number, and residence address of their ex-girlfriend in some social networking sites.

7) **Divorced Husband/Wife**: - This type of crime happens from both end i.e. husband and wife. In a case it was found by the cyber crime investigators that the divorced wife sent mail to the colleagues of her divorced husband by creating a profile in a free email service provider in the name of her divorced husband so that his colleagues understand that he is confessing his guilt.

IV. Futuristic Cyber Crime and Prevention

Exploding chips could turn a Laptop into a BOMB

A way has been found for exploding silicon in any Computer Chip which means anyone trying to use a stolen laptop or mobile will be confronted by this message: **"This machine is stolen and will self-destruct in ten seconds ... ".**

Until now scientists have only managed to make silicon go bang by mixing it with either liquid oxygen or nitric acid. But Michael Sailor and his colleagues at the University of California in San Diego have found a way to blow up silicon chips using an electrical signal.

They say their method could be used to fry circuitry in devices that fall into the wrong hands. For instance, the American spy plane impounded by China last year could have used it to destroy its secret electronics systems.

Sailor's team hit upon this new way of exploding silicon when they applied the oxidizing chemical gadolinium nitrate to a porous silicon wafer. As colleague Fred Mikulec used a diamond scribe to split the wafer it blew up in his face, giving Mikulec the shock of his life. Luckily, only a minute quantity of silicon was involved so it was a small bang. "It's a bit like a cap in a cap gun going off," says Sailor.

1) Fast burn

The gadolinium nitrate used the energy from the diamond scribe to oxidize the silicon fuel, which burns fast because its crystals have a large surface area. "The faster the burn, the bigger the bang," explains Sailor. You would only need a tiny quantity of the chemical to do irreparable damage to delicate transistors, so it would be cheap and easy to add when the chips are being made.

In a stolen mobile phone, the network would send a trigger signal to the part of the chip containing the gadolinium nitrate "detonator", triggering the explosion. "We have shown that you can store this stuff and detonate it at will," says Sailor.

Other applications suggested for the technology include testing for toxic substances in groundwater. The device could be used on the spot to burn minute samples on a disposable chip and analyze their chemical composition. Alternatively, it could be used as a fuel supply for microscopic machines etched onto silicon wafers.

Global surveillance supermarket offered to dictators

The ease with which totalitarian regimes can buy western technology to intercept and store every electronic communication made by their citizens has been revealed in a joint document release by Wiki leaks, the pressure group Privacy International and several media organizations.

Posted online by Wiki leaks, 287 documents details the wide choice of cell phone and internet surveillance technologies on offer from 160 intelligence contractors - and show, in part, that dissidents using common tools like Google's Gmail service, or devices like Apple's iPhone and RIM's BlackBerry, stand little chance of hiding their missives from authoritarian regimes - unless they know how to use the TOR ANONYMISING NETWORK.

Many of the surveillance firms appear to be operating in two distinct ways: offering technologies that adhere to legal surveillance norms in their home markets - but when it comes to selling to other nations, they adopt an "anything goes" approach to interception functionality. Some of the them says Wiki leaks founder Julian Assange, will even tap the global network of undersea to harvest traffic going into and leaving a nation.

The data has been gathered by researchers like Eric King at London-based Privacy International, who has been examining the wares on offer at arms fairs and surveillance industry conferences - many of which have been platforms for selling the kind of

bulk email interception technology shown to have been used by the dictators recently ousted in Libya, Tunisia and Egypt.

A French Company AMESYS, for example, was found to have helped Libya's late dictator, Muammar Gaddafi, monitor dissidents' webmail accounts - because it left their names in a poorly-redacted screenshot in a PDF of a sales document. "There are no rules to stop a company in a democratic country selling such software to a dictator," said one of the media groups that worked with Wiki leaks, speaking at the release event today. "This has to stop."

Calls for overseas sales of surveillance technology to be restricted are growing and BILLS have presented in the US Congress to limit such exports in the US, where the *Washington Post* reported that a trade show for vendors peddling such technologies has earned the nickname “Wiretrappers Ball”.

And in India, N Ram, editor-in-chief of the “Hindu Newspaper”, wants to see "a legal framework" established to control "the large passive interception of communications that's been going on in India since the Mumbai attacks."

RFID Tags in New US Notes Explode When You Try to Microwave Them (Tracking Cash Thru RFID)

Adapted from a letter sent to Henry Makow Ph.D.

Want to share an event with you, that we experienced this evening.. Dave had over $1000 dollars in his back pocket (in his wallet). New twenties were the lion share of the bills in his wallet. We walked into a truck stop/travel plaza and they have those new electronic monitors that are supposed to say if you are stealing something. But through every monitor, Dave set it off. He did not have anything to purchase in his hands or pockets. After numerous times of setting off these monitors, a person approached Dave with a 'wand' to swipe why he was setting off the monitors. Believe it or not, it was his 'wallet'. That is according to the minimum wage employees working at the truck stop! We then walked across the street to a store and purchased aluminum foil. We then wrapped our cash in foil and went thru the same monitors. No monitor went off.

We could have left it at that, but we have also paid attention to the European Union and the 'rfid' tracking devices placed in their money, and the blatant bragging of Wal-Mart and many corporations of using 'rfid' electronics on every marketable item by the year 2005.

Dave and I have brainstormed the fact that most items can be 'micro waved' to fry the 'rfid' chip, thus elimination of tracking by our government.

So we chose to 'microwave' our cash, over $1000 in twenties in a stack, not spread out on a carasoul. Do you know what exploded on American money?? The right eye of Andrew Jackson on the new twenty, every bill was uniform in it's burning... Isn’t that interesting?

Now we have to take all of our bills to the bank and have them replaced, cause they are now 'burnt'.

We will now be wrapping all of our larger bills in foil on a regular basis.

What we resent is the fact that the government or a corporation can track our 'cash'. Credit

purchases and check purchases have been tracked for years.

V.Conclusion

As someone rightly said that "bytes are replacing bullets in the crime world". The growth of cyber crime in India, as all over the world, is on the rise and to curb its scope and complexity is the pertinent need today. Cyber space offers a plethora of opportunities for cyber criminals either to cause harm to innocent people, or to make a fast buck at the expense of unsuspecting citizens. India's profile and wealth have risen enormously in the world due to the constructive use of information technology. At the same time, India ranks fifth in the world for cyber crime, according to a report last year by the U.S.-based Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Even under the IT Act, investigations in India are not easy. This is mainly due to the lack of what is called "cyber forensics." So we have to improve our forensics system as well as our technology .

Acknowledgement

We are very thankful to Prof. Sitanshu Ray for his tireless support and his lucid way of explaining us the salient points really helped us to write this paper.

I'm also thankful to these references, I've mentioned below, which helped me much to write this paper.

References:

1. Granville Williams
2. Proprietary Articles Trade Association v. A.G.for Canada (1932)
3. Nagpal R. – What is Cyber Crime?
4. Nagpal R- Defining Cyber Terrorism
5. Duggal Pawan – The Internet: Legal Dimensions
6. Duggal Pawan - Is this Treaty a Treat?
7. Duggal Pawan - Cybercrime
8. Kapoor G.V. - Byte by Byte
9. Kumar Vinod – Winning the Battle against Cyber Crime
10. Mehta Dewang- Role of Police In TacklingInternetCrimes