Presented by:

D.R.Esesve, III/IVB.Tech,
SBI-10/7, MVP COLONY,
VISAKHAPATNAM.
PIN: 530017.
PH: 0891 504389.

Mail: *Dresesve@yahoo.com*
Dresesve@rediffmail.com

URL: *members.rediff.com/dresesve/ccacl.htm*

D.R.Esesve Abstract *dresesve@rediffmail.com*

"Anybody with a computer and modem can become a potential terrorist", says Howard Schmidt, an OIS chief of U.S. Some people trade secrets over the Internet on how to break into government systems, how to build weapons and engage in terrorism", Schmidt said.

Cyber crimes have become a common piece of vandalism in the present computerized world. There are many laws in enforcement and many new devices, which are used to prevent such crimes. But these all devices resemble a seismograph, which records the amount of quake but cannot prevent the same. In 1997 in China a 22-year-old had broken out into a computer network and discovered passwords of 500 users. In U.S an Argentine broke into the Harvard computer network and stole a few accounts and passwords through which he could gain access to many military bases in us.

It did not stop here. It also affected the Microsoft networks in the recent past. To the oddest of odds, the world's toughest unbreakable code, created by the U.K-Indian expert, Mr.Simon Singh, was cracked.

The present scenario is Kevin Metnick who misused the net to crack some of the most secure computer secrets is now the subject of the film "Take down" & he is sought by all the MNC's to keep their connections safe.

What is the solution to this?

INTRODUCTION

... As said by great authors like Robert Lynd every human being has some sadistic instincts hidden in him, by which he enjoys wreckage. This is the one great feeling embedded in the minds of all the hackers, who tried to spoil the massive systems. There would be some reason for all these people to involve in such worse activities.

Most of the crimes, in past, present or may be even in future are mainly done only for one reason that is money. When a person comes to know those huge amounts of wealth is kept open to him then it is obvious that he tries to have it. That is one much bigger force driving people with good knowledge and with bad intentions towards stealing, hacking etc.

In China it was estimated that over $60 billion worth assets are exposed on the net. In the past two years China has recorded a highest theft score of 100 cases involving thefts of$1.2 million. Even there are feature films, which show how money can be manipulated through the net. The passwords, which are specified to do lock and key work, are not safe at all times. Hackers can easily obtain passwords and the respective information can be obtained.

In the recent years, crimes have taken a new angle. People started destroying systems rather than getting some profit from them. Hackers started capturing the systems by their programs and started destroying the host information, which is loaded in its memory. There were instances where data or systems worth millions were destroyed.

In the world of increasing users of the net, it is quite obvious that the security will get reduced. For example in 1997, china had a score of 620000 users. However, to their surprise the score at a sudden exploded to two million by the start of the millennium year (2000). In America, for an example, a certain university has a bandwidth of two gigabytes, by that it can be estimated how many users are present. So, if that is the scenario, then optimum security cannot be provided by any antivirus software or even by any great passwords. These all play a very nominal role. This can be explained so; when we visit a site or access our mail account we certainly

load some information pertaining to us which is expected to be secret is displayed out. We do not know this but when we find some unnecessary mailings in our inbox then we can be acknowledged of this fact.

In a computer, a folder named cookies is found, which stores the information about the site, which is visited. If that is so then there can also be a folder in the visited site's computer which record information about the visitor. Then it means that you are on the show. Therefore, when a system is online it means that its user has opened a gateway for the entire web users to come in and play. This experience can be had when a user uses a chat facility. The user can find people talking with him whom he does not really know. So now, it can be understood what a security can anybody have when they are on the net.

CRIMES

It would be better to discuss this part in an order. Starting with the recent disorder…

- *This has occurred in the recent months disturbing the entire network of an ISP's users. An email conveying greetings to Diwali was sent to many users. This was sent to all the customers of that particular ISP. This was attached with a virus, which on opening of the mail was activated and ruined the host computers creating loss of huge data. Later on a compliant, by one of the subscribers the police investigated and found the recipient's IP address. It was from a mail id called magus@satyam.net.in. Later it was found that it was called as "Anti-X" and it (virus) has destroyed many systems and their data.*

There is a lot of anxiety among the major companies whose net transactions run into some billions of dollars which rose up due to an instance in the recent past …….

- *A hacker penetrated into the Microsoft internal network with a Trojan horse type virus through which the hacker gained access to the sensitive source codes of upcoming products. This virus, names QAZ, was found out to be originated in China and also was found to be a notepad extension. This file, once downloaded into the system, by some means like an email attachment, will start fetching for the notepad.exe file and then*

converts into note.com. Then this sends a notification to the hacker with the Internet protocol of the affected computer.

- *Now after this, the hacker starts gaining control over the host computer and starts roaming over the system at will thereby destroying or misusing the host files. This is what happened in the case of Microsoft's disaster. Symantec, makers of the Norton antivirus software and it's competitors like Trend etc have identified this virus (QAZ) since September, 2000 yet it got past the defenses of a company which is otherwise a paranoid about security.*

- *But when it comes to Kevin Metnick, the situation is different. He was the one who misused the net to crack the most secure systems in the world. In addition, he stole commercial secrets from great companies like Motorola, Sun, Nokia, Fujitsu and NEC. He was captured in 1995 and was grilled for a few years. But to the surprise his pursuit and capture is now the subject of a feature film, "Take down", and based on the book of the same name by Tsutomu Shimomura, the computer whiz kid who concerned Metnick and John Markoff, a journalist.*

- *In a particular case in US, the international hacker invaded the Harvard computer through a broadly accessible modem bank and the Internet. He stole a series of accounts and passwords. Using these stolen accounts, Ardita gained unauthorized access to computers at various U.S. military sites across the country, including the Navy Research Laboratory, NASA's Jet Propulsion Laboratory and Ames Research Center, the Los Alamos National Laboratory and the Naval Command Control and Ocean Surveillance Center. He also tried repeatedly but unsuccessfully to enter the Army Research Laboratory computer system.*

- *In certain other occasions, once a person was able to steal many of the passwords of a particular country' military base. Moreover, once in Shanghai a 22-year-old youth was captured in a hub when he broke out nearly 500 passwords and manipulated with them. The crimes so and so on are going at higher paces. Then what is the situation? A day may come when our own resources start harming us. It is just like our living. We started with unclothed Adam and Eve. Invented clothes. Made designs and know again tending towards the bare version. Is that what is going to happen?*

So for not happening of such hazards, each country is taking it's own measures to eradicate such problems. One of those programs involves in making certain rules. Of course, rules are rules. Most of the countries, which have big numbered users, have made certain rules and made them compulsory. As mentioned all these rules etc are just like a seismograph, which records the amount of earthquake but cannot detect the same. Same way all these rules are only useful when a hacker is caught, but cannot prevent that person from carrying out his activity.

But there are certain codes and soft wares developed, which provide certain security in sending data and also act as blocking agents to certain virus packs. These detect the incoming viruses, up to their knowledge and block them at the gate itself, thereby preventing them from being embedded into the system memory.

In this way of producing codes it becomes important to discuss about Mr.Simon Singh, an UK based Indian expert, who made very good contributions in this part of web securities. He also is an author of a popular book on cryptology, entitled The CodeBook. Almost a year after the book was published, a group of Swedish computer buffs, cracked the code which was given as a puzzle in his book. Dr.Singh said, while handing over the reward to those Swedish persons, "the toughest code cracked until now was the code ENIGMA, used by the Germans in World War II.

There are different types of codes built. But conventionally there are two methods of sending encrypted or encoded data. Why are these discussed is its important to know whether data can have any security or not.

Therefore, the two types of coding are…

- *The traditional method. Digital encryption Standard employs a secret key available to both sender and user. The only hassle is that the key or code should be securely sent to the recipient.*

- *The second method is known as Public key Encryption. In this methodology, every user has certain private secret key and a public key,*

which is known to all. The sender uses the recipient's public key and the receiver uses his private key to unlock the message.

The other commonly used Private and Public Key Cryptography Algorithms ...

- *ROT13 Keyless text scrambler: very weak.*
- *Crypt Variable key length stream cipher: very weak.*
- *DES 56-bit block cipher: patented, but freely usable (But not exportable).*
- *RC2 Variable key length block cipher; proprietary.*

Skipjack 80-bit stream cipher; classified. Etc.

So that is the way information or data can be sent through the net with a better security. Actually these coding techniques are not new born; they are present from the good olden days. The great book, Kamasutra, written by Vatsayana*, describes method known as substitution method. In this method, if an alphabet of 26 letters is substituted with other letters then the chance of deciphering the code is virtually impossible. Men in contacting their paramours without their spouses' knowledge used this coding.*

So virtually there are methods to send data with certain security. But to our disadvantage, every user of the net neither can maintain such keys nor can he encrypt data. So it becomes important to have certain laws, which protect the petty users and great users of the net. For this purposes the governments of every state have made certain bills. Those can be depicted as follows ... ...

LAWS ENFORCED BY DIFFERENT GOVERNMENTS.

Earlier this year, President Clinton used the executive privileges of his office to bypass Congressional scrutiny, and to initiate a secret "war" Against the threat of what the administration calls "cyber-terrorists Hackers, crackers, organized crime figures, drug dealers, foreign military Operatives, information warfare operatives, foreign spies, terrorists, violent domestic militia members, members of hate groups, criminals, and cons And cheats, gamblers, copyright and patent infringes, child Pornographers, and others."

By using the ploy of "protecting the Internet from potential 'cyber-threats,'" the President has begun the regulatory process that makes the free-operating Internet in the U.S. a component of "national security. On July 15 2000, President Clinton, by Executive Order, created the Infrastructure Protection Task Force ("IPTF") within the Department of Justice, chaired by the Federal Bureau of Investigation under the direct control of Attorney General Janet Reno and FBI Director Louis Freeh.

In fact, the Air Force's Office of Special Investigations, or OSI, has thought to fight against computer-related crimes. OSI will employ a new million-dollar, state-of-the-art computer lab at Bolling Air Force Base in Washington, D.C., to sniff out cyber criminals and evidence. So this is the way the axis power is taking its own course in solving these cases. In the same way, many countries have made laws to seize cyber corruption. In the same race is the small bandwidth India. It has released its policy in May 2000. This runs so…

I.T RULES IN INDIA:

1. *A good part of the new act is the fact that it recognizes digital signatures.*

2. *The requirements of maintaining electronic records would mean that all companies would have to progressively move to standardized data storage in electronic form. Though most companies do maintain*

electronic records, it would now require verification of security procedures for storing such records. In this aspect, the penalty for "tampering with computer source documents" which stands at Rs.0.2mn seems quite low.

3. *A provision allowing police officers above DSP rank to raid and arrest people for cyber-crimes without a warrant (under clause 79) was given.*

4. *A critical shortcoming in the Bill is the low penalties for crimes related to hacking. According to the Bill, the maximum penalty for hackers for "damage to computer, computer system, etc." is only Rs1mn. (This is very low as compared to the cost of damages hackers could cause. Though India is yet to see any major incident of large-scale hacking, a stiff penalty at this stage would have acted as a very effective deterrent against hacking incidents.)*

5. *The Indian IT rules specifies that the cryptography algorithms used to generate digital signatures must be considered from the IEEE standard on public key encryption.*

In this way, India has established rules, some positively and some negatively. These minor blimps will soon be soothed as India steps into the new era of Net-based business practices. Most important, is the awareness that the Brave New World of digital dealings is full of promise and danger. These rules and bills are most important in net savvy countries rather than in very small net usage countries.

In a latest concept, brief to discuss, a US firm Wear Logic has launched the world's first smart wallet, a leather purse that you can plug into the internet and, with its own display and memory that you can twist crush or fold as would do to an ordinary wallet. You can store all the numbers you need to remember and can perform e banking and payments via the net. However, there is one great feature in this, that is, you cannot loose it, i.e. you should be very careful to see that it is not stolen. So the virtual truth is there is no optimum security for anything. All the things we create are just for name, as they cannot give us 100% security.

CONCLUSION

The net, like the remaining utilities, has all the effects both positive and negative. This will only have a good effect when it is used for the good and that can only be achieved only when all the knowledged people have good intentions. Good ideas are obtained only when people see good, but most of the children, adults watch only hazardous information on the net. The net is dumped with porn, bomb making techniques, hacking techniques.

In this environment how a person can learn good?

As some great analyzers of the net say that, a high proportion of the people who face the unemployment problem and-are thus drawn towards cyber crime. And a U.S. government expert speaking at a National Information Systems Security in Baltimore on October 17th 2000 described Internet security as "a tremendous catch game"; one has to keep a step ahead of the hacker. Will this be possible always?

Can we predict future? If we can then we may think in such a way, but it is sure that a human cannot look into future. Thinking abilities have been changing from generation to generation, so it is not easy to manufacture security systems for future, keeping in mind the changes that are going to occur in future. There by, we can see that most of the anti virus software companies start including viruses only after they occur at some or the other place. Same is the situation in everything of life. It is only possible to design a medicine if and only if it has occurred somewhere or the other. There are vaccines, but not for new diseases, all those are meant for the diseases already occurred. When the entrance of the house is kept open, it is obvious to expect somebody coming in.

Anyway, I do not mean that there cannot be any security, but these securities are to be found before we destroy ourselves. Because, as the way, Metnick and others acted, shows that there is an eminent threat to the greatest of greatest securities in the world. If in the same way if codes can be intercepted and decoded then there is no security for anybody, keeping individuals apart the entire networks of any country are at threat. Thereby the whole world is at the forefront of a big virtual war.

To my opinion, it seems web has lesser secure solution and users that are more destructive. Nevertheless, we have scientists who have great brains bombarded with intelligent ideas, so therefore one or the other day these crime stories may have a full stop. The solutions are expected to come soon.

Hope we have a secure, child insensitive, peace provoking, fun filled, and knowledge filled world of web.

REFERENCES:

- The Hindu, dated- 2 November 2000. (Article: "NET SECURITY? READ KAMASUTRA, By Anand Parthasarathy.)

- Eenadu. (Article published on 25 November 2000)

- Certain references were also made from the web.