International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.3, March 2013 DOI:10.15693/ijaist/2013.v2i3.1-5

Cyber Crime And Network Security

[1]K.VEERARAGHAVAN, [2]A.ANITHA, [3]P.ANITHA, [4]R.VINODHA

Department of CSE,

As-salam college of Engineering and technology, Aduthurai, thirumangalakudi

ABSTRACT:

With Internet technology revolution, all kinds of business transactions are taking place through distributed systems across the globe. The network management, database administration, secure communications are the ongoing challenges to ensure trusted transactions in ecommerce and e-governance. With increasing use of internet for ecommerce and e-governance, the volume of cyber crime also increases exponentially.

Computer forensics provides digital evidence of a specific/ general activity. It use analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is electronically stored or encoded. The digital forensic techniques can be of value in a wide variety of situations, starting from simple re tracking steps

A network is not secure unless it can ensure the three basic security concepts; confidentiality, integrity and availability. Attack on confidentiality and integrity of data are emerging trends in network intrusion. With more and more sophisticated tools being easily available the number of security incidents has been rapidly increasing. Such Tools reduce the attack preparation time thereby increasing attack frequency. The use of such tools also makes it difficult to discover attacks at an early stage before substantial damage has been done. Here we show a highly personalized attack by the use of specialized agents whose purpose is to search and transmit specific information from a private network without authorized access. This paper address the latest threats, highlights their growing complexity and the latest information on software and hardware solutions.

KEYWORDS:

Distributed Denial of Service (DDoS), Asia Development Bank (ADB), Federal Bureau of Investigation's (FBI), Cyber-slander.

INTRODUCTION TO CYBERCRIME:

The first recorded cyber crime took place in the year 1820! That is not surprising considering the taken when data has been lost, to criminal investigation or civil litigation.

There are a wide and varied the common scenarios such as employee internet abuse, unauthorized disclosure of corporate information and data (accidental and intentional), industrial espionage, damage assessment (following an incident), criminal fraud and deception cases and more general criminal cases.

Cybercriminals continue to invent increasingly cunning ways to exploit human and computer vulnerabilities to steal and extort money from computer users and companies.

There is an increasing demand for computer professionals in almost in every corporate sector especially the law enforcement, auditing/ accounting and defense sectors to deal with the challenging tasks of tracking and identification of cyber crimes and criminals
fact that the abacus, which is thought to be the earliest form of a computer ,has been around since 3500 B.C. in India, Japan and china. The area of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820,Joseph-Marie Jacquard, a textile manufacture in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

AN AGENT BASED APPROACH:

Protecting a private network connected to the internet is a challenge and nightmare for network security analysts, particularly when the attackers frequently come up with more and more sophisticated and previously unseen attacks. Most common are the Distributed Denial of Service (DDoS) attacks and the attacks by the malicious code [3] including worms and spywares. However, these are mainly directed towards the loss of availability [19]. Starting with the Morris

worm of 1988 the list goes on unending with Code Red, Nimda, and SQL Slammer as some of the devastating ones. Further, securing the ever increasing digital data on a network and ultimately on the web is a major concern .

FREQUENTLY USED CYBERCRIMES:

Unauthorized access to computer systems or networks:

This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking". The act of gaining unauthorized access to computer systems for the purpose of stealing and corrupting data.

Theft of information contained in Electronic Form:

This includes information stored in computer hard disks, removable storage media etc.

Email Bombing:

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the 169 schemes was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

Data Diddling:

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in India have been victims to data diddling programs inserted when private parties were computerizing their systems.

Salami Attacks:

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems.

Logic bombs are programmers, which are activated on the occurrence of a particular predefined event. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters..

Denial of Service Attack:

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks

Virus / worm Attacks:

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. 170 The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate.

EMAIL RELATED CRIMES:

Email has fast emerged as the world's most preferred form of communication. Billions of email messages traverse the globe daily. Like any other form of communication, email is also misused by criminal elements. The ease, speed and relative anonymity of email has made it a powerful tool for criminals.

Some of the major email related crimes are:

1. Email spoofing
2. Sending malicious codes through email
3. Sending threatening emails
4. Defamatory emails

5. Email frauds

Email Spoofing:

A spoofed email is one that appears to originate from one source but has actually emerged from another source. Falsifying the name and / or email address of the originator of the email usually does email spoofing. usually to send an email the sender has to enter the following information:

- email address of the receiver of the email
- email address(es) of the person(s) who will receive a copy of the email (referred to as CC for carbon copy)
- email address(es) of the person(s) who will receive a copy of the email (referred to as CC for carbon copy, but whose identities will not be known to the other recipients of the e-mail (known as BCC for blind carbon copy)
- Subject of the message (a short title / description of the message)
- Message
-

Spreading Trojans, viruses and worms:

Emails are often the fastest and easiest ways to propagate malicious code over the Internet. The Love Bug virus, for instance, reached millions of computers within 36 hours of its release from the Philippines thanks to email. Hackers often bind Trojans, viruses, worms and other computer contaminants with e-greeting cards and then email them to unsuspecting persons. Such contaminants can also be bound with software that appears to be an anti-virus patch. E.g. a person receives an email from Compose From To CC BCC Subject

Threatening emails:

Email is a useful tool for technology savvy criminals thanks to the relative anonymity offered by it. It becomes fairly easy for anyone with even a basic knowledge of computers to become a blackmailer by threatening someone via e-mail.

In a recent case, Poorva received an e-mail message from someone who called him or herself 'your friend'. The attachment with the e-mail contained morphed pornographic photographs of Poorva. The mail message said that if Poorva were not to pay Rs. 10,000 at a specified place every month, the photographs would be uploaded to the Net and then a copy sent to her fiancé.

Defamatory emails:

As has been discussed earlier cyber-defamation or even cyber-slander as it is called can prove to be very harmful and even fatal to the people who have been made its victims.

Email Frauds:

Email spoofing is very often used to commit financial crimes. It becomes a simple thing not just to assume someone else's identity but also to hide one's own. The person committing the crime understands that there is very little chance of his actually being identified. In a recently reported case, a Pune based businessman received an email from the Vice President of the Asia Development Bank (ADB) offering him a lucrative contract in return for Rs 10 lakh. The businessman verified the email address of the Vice President from the web site of the ADB and subsequently transferred the money to the bank account mentioned in the email. It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.

COMPUTER CRIMES AND SECURITY SURVEY:

The "Computer Crime and Security Survey" is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The aim of this effort is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States.

Based on responses from 503 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2002 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.

Highlights:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.
- Eighty percent acknowledged financial losses due to computer breaches.
- Forty-four percent (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported $455,848,000 in financial losses.
- As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).

Attacks And Abuses:

- Forty percent detected system penetration from the outside.
- Forty percent detected denial of service attacks.
- Seventy-eight percent detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).
- Eighty-five percent detected computer viruses.
- For the fourth year, we asked some questions about electronic commerce over the Internet. Here are some of the results:
- Ninety-eight percent of respondents have WWW sites.
- Fifty-two percent conduct electronic commerce on their sites.
- Six percent reported financial fraud (only 3% in 2000).

APPLICATION SECURITY AND APPLICATION NETWORKS:

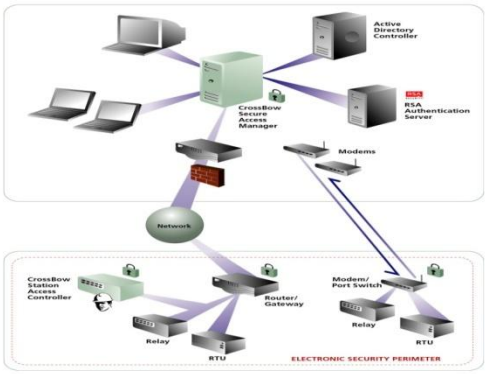
The Access and security trade-off:

Today, extending access to applications for the users who need them is no longer a "nice to have" - but a key determinant of who will win and who will lose. Legacy applications and databases, for example, contain invaluable customer information and provide a great resource for partners and other trusted third parties; email and other

messaging applications are indispensable for seemingly instantaneous communication; and 'emerging' applications, such as audio and video conferencing, are now the critical enabler of 'real-time business,' resulting in huge gains in both productivity and profitability. Facilitating the rollout and accessibility of these applications, IP networks - both private and public, wired and wireless - make access to applications possible for any user from any corner of the globe. Why, then, are CIOs constantly refereeing a tug-of-war between the lines of business who want to realize the value of their applications by extending them to the users who need them and the network administrators who want to insulate their network from attack by increasingly limiting access for untrusted third parties.

CYBER SECURITY AND STANDARDS:

CrossBow was formally known as IED Anywhere 2,it was designed specifically for the cyber security. CrossBow is an interface which has RSA authentication server, active directory control and CrossBow secure access
manager.



Benefits:

- Remote, transparent access to IEDs, from any software application
- Preserves investment in legacy gateway devices and communication infrastructure
- Meets NERC CIP-002-1 through CIP-009-1 requirements for security:
- Strong (2-factor) authentication
- Active Directory support
- Individual user accounts
- Comprehensive NERC CIP compliance reports
- Audit log
- WAN or Dial-up access
- Administration interface allows management of thousands of IEDs and hundreds of users

CHALLENGES TO CYBERLAW ENFORCERS:

- Technological Challenges

-Technological Challenges • Technology allows for near absolute
Technology allows for near absolute anonymity of culprits.

- Legal Challenges

-Laws lag behind the changes in technology
Laws lag behind the changes in technology

- Resource Challenges

-Lack of sufficient experts/budget

SECURITY TIPS:

Desktop and Laptops:

Require a user account password to login to your system:
By enabling password based authentication you make it harder for someone to get into your system.

Don't insert untrusted media into your system:
CDs, DVDs and USB drives can contain malicious code like viruses, worms and trojans. Simply inserting a contaminated piece of media can cause this code to run and infect or disable your entire system.

Supervise others you allow to use your system:
People all have their own agendas. Keep this in mind. Don't let anyone you can't fully trust use your system. Never give strangers access to your system. Dangerous activity can occur quickly and easily.

Use a cable lock to secure your laptop: Leaving your laptop unsecured when unattended can result in theft. A simple cable lock makes it much more difficult to steal.

Apply latest software updates: Keeping the system hardware and software code updated is always a good practice since security functionality is usually updated as well.

Advanced BIOS password protection: Enable a BIOS password when your computer first starts up. This makes it much more difficult for intruders to change your system settings, boot order, and such. But remember, if you forget the password, you won't be able to start your computer.

Portable Media:

USB flash drives, CD/DVD discs and external hard drives:

Use password protection if available: Many new storage devices have password protection available. Use it to deter unauthorized access to your data.

Encrypt sensitive data:
When you cannot afford to let an unauthorized person access your data, protect that data with reputable encryption software.

Secure your CDs, DVDs, USB and other external data drives:
Protect your electronic data storage devices from theft or tampering. Portable media are attractive means of transmitting malicious programs like viruses and are goldmines for data thieves.

Install anti-virus & spyware software:
Digital bugs and spies are the most common and damaging threat to business computers, and they require solid defenses. Set the software to update virus/spyware definitions regularly and automatically.

Get a spam blocker:
Spam doesn't just mean annoying ads anymore—it introduces all kinds of new threats, such as phishing scams.

Build a firewall:
The digital barrier keeps hackers out and luckily it exists on most operating systems. Make sure yours is turned on. If you don't have a firewall, you can download one.

Setup effective encryption network access keys:
Always use long, automatically-created network encryption keys and rotate them regularly.

Install security patches:
New vulnerabilities are regularly exploited in many software platforms. You should check for and install updates on all software you use.

Backup important files:
No amount of protection is a guarantee, so take preventative steps to save your data before it can be damaged.

CONCLUSION:

Security threats to information systems have increased 65 percent over the past two years, and the number of network intrusions has quadrupled. Any small business with a broadband Internet connection needs to guard against becoming a cyber-crime victim.

Security is everybody's business, and only with everyone's co-operation, an intelligent policy, and consistent practices, will it be achievable.

BIBLIOGRAPHY:

1. **"**UNDERSTANDING AND MANAGING CYBERCRIME**"** Sam C. McQuade

2. "CYBER WAR,CYBER TERROR,CYBER CRIME",
Dr. julie Mehan

3. "COMPUTER SECURITY THREAT MONITORINGAND SURVEILLANCE",
James P. Anderson,

REFERENCES:

- **www.capricornian.com**
- **www.eweek.com**
- **www.amazon.com**