International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Study of Cybercrime in Banking and Financial Sectors

S. Balasubramanian
Assistant Professor in Computer Science, Directorate of Distance Education, Alagappa University, Karaikudi, Tamil Nadu, India

ABSTRACT

New computer technologies create new criminal opportunities. Cybercrime is not in the form of traditional criminal activity, the difference is the use of the digital computer. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy not only personal also financial sectors. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behavior alongside some novel illegal activities. Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a having a large volume of numbers and identifiers in multiple computer databases owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.

Keywords : Cyber, Skimming, Cyber Terrorism

I. INTRODUCTION

Cyber Crime may be defined in a general way as an unlawful act wherein the computer is either a tool or a target or both.

Cyber Crime can be categorized as:-

Unauthorized access, Email bombing, Data diddling, Salami attack, Internet time theft, Logic bomb, Virus / worm attack, Trojan attack, Distributed denial of service attack, Denial of Service attack, Email spoofing, Cyber pornography, Intellectual Property Crime, Cyber Stalking

Unauthorized access

Unauthorized access to computer systems or networks means any person who secures access or attempts to secure access to a protected system.

Email bombing

Email bombing refers to sending a large amount of emails to the victim resulting in the victim's email account (in case of an individual) or mail server (in case of a company or an email service provider) crashing.

Data diddling

This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.

Salami attack

This attack is 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 single account holder will probably notice this unauthorized debit, but

CSEIT1831325 | Received : 10 Feb 2018 | Accepted : 18 Feb 2018 | January-February-2018 [(3) 1 : 1205-1212]

the bank employee will make a sizable amount of money every month.

Internet time theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person.

Logic bomb

This is event dependent program. This implies that this program is created to do something only when a certain event (known as a trigger event) occurs, e.g. some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Virus / worm attack

Virus is a program that attach itselves to a computer or a file and then circulate itselves 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.

Trojan attack

A Trojan, the program is aptly called an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

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.

Distributed denial of Service attack

This is a denial of service attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks.

Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc.)

Email spoofing

A spoofed email is one that appears to originate from one source but actually has been sent from another source.

Intellectual Property Crime

This includes software piracy, copyright. Infringement, trademarks violations etc.

Cyber Stalking

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

Cyber crime challenges in Financial Institutions

Financial Crimes are defined as a crime against property, involving the unlawful conversion of the ownership of property (belonging to one person) to one’s own personal use and benefit. Financial crimes often involve fraud.

Financial crimes are carried out via check and credit card fraud, mortgage fraud, medical fraud, corporate fraud, bank account fraud, payment (point of sale) fraud, currency fraud, and healthcare fraud, and they involve acts such as insider trading, tax violations, kickbacks, embezzlement, identity theft, cyber attacks, money laundering, social engineering, and Securities fraud. Financial crimes sometimes, but not always, involve additional criminal acts such as elder abuse, armed robbery, burglary, and even murder. Victims range from individuals to institutions, corporations, governments, and entire economies.

1. Currency counterfeiting

Counterfeit is currency that is produced without the legal sanction of the state or government to resemble some official form of currency closely enough that it may be confused for genuine currency. Producing or using counterfeit money is a form of fraud.

Effect on society

Some of the ill-effects that counterfeit money has on society are: reduction in the value of real money, Increase in prices(inflation) due to more money getting circulated in the economy – an unauthorized artificial increase in the money supply, Decrease in the acceptability(satisfactoriness) of money – payees may demand electronic transfers of real money or payment in another currency(or even payment in a precious metal such as gold), Companies are not reimbursed for counterfeits. This forces them to increase prices of commodities.

2. Money laundering (funds derived from criminal activities)

Money laundering is the process of creating the appearance that large amounts of money obtained from serious crimes, such as drug trafficking or terrorist activity, originated from a legitimate source. The term money laundering was applied only to financial transactions related to organized crime. It was committed by private individuals, drug dealers, Business, corrupt officials, members of criminal organizations such as the Mafia, and even states.

Fighting money laundering

The first defence against money laundering is the requirement on financial intermediaries to know their customers – often termed KYC (know your customer requirements. Knowing one's customers, financial intermediaries will often be able to identify unusual or suspicious behavior, including false identities, unusual transactions, changing behaviour, or other indicators of laundering. But for institutions with millions of customers and thousands of customer-contact employees, traditional ways of knowing their customers must be supplemented by technology. Many Companies provide software and databases to help perform these processes. Bank and corporate security directors can also play an important role in fighting money laundering.

Using Information technology

Information technology can never be a replacement for a well-trained investigator, but as money laundering techniques become more sophisticated, so too does the technology used to fight it. Before anti-money laundering programs became commonplace.

The various software packages are capable of name analysis, rule-based systems, statistical and profiling engines, neural networks, link analysis, peer group analysis, and time sequence matching. Also, there are specific KYC solutions that offer case-based account documentation acceptance and rectification, as well as automatic risk scoring of the customer taking account of country, business, entity, product, transaction risks that can be reviewed intelligently. Other elements of AML technology include portals to share knowledge and e-learning for training and awareness.

This software is not used exclusively to track money laundering, but more often the common theft of credit cards or bank details. Unusual activity on an account may trigger a call from the card issuer to make sure it has not been misused.

3. Intellectual property (IP) crime

Intellectual property crime is a generic term used to describe a wide range of counterfeiting and piracy offences.

Trademark counterfeiting and copyright piracy are serious intellectual property crimes that defraud consumers, threaten the health of patients, cost society billions of dollars in lost government revenues, foreign investments or business profits and violate the rights of trademark, patent, and copyright owners. Imitation products pose a significant safety threat to consumers worldwide. Unsuspecting customers and severely sick patients put their health, and even life, in jeopardy each time they use counterfeit medication, alcoholic beverages, food products or travel in automobiles and aircrafts maintained with substandard counterfeit parts.

Payment card fraud

Payment card fraud is a generic term used to describe a range of offences involving theft and fraudulent use of payment card account data. Frequent types of payment card fraud include

Application fraud is a type of ID theft crime in which payment card are obtained through a fraudulent application process using stolen or counterfeit documents.

Account takeover is a another type of ID theft crime, this usually involves deception of a financial institution, re-issue of a payment card and its redirection to a different address.

Lost / stolen card as the name suggests, this type of fraud involves misuse of actual cards that are either lost or stolen from the genuine cardholder.

Counterfeit card is a fraud undertaken using plastic card that have been specifically produced or existing cards that have been altered. These cards are encoded with illegally obtained payment card account data in order to pay for goods and services or to withdraw cash.

Card not present, fraud committed using payment card account data to undertake transactions where there is no face-to-face contact between the seller and purchaser. Typically, this type of fraud is committed by internet, mail order or telephone. Card not present fraud is currently the fastest growing payment card related type of fraud in many areas of the world.

We have three solutions to authenticate such transactions:

Card Verification Value 2 (CVV2)

Often referred to as the 'card security code'. This is the three-digit security code on the reverse of every Visa card – either on, or to the right of, the signature panel.

Verified by Visa

This is our e-commerce security solution. It is a password-protected identity checking system that has been designed to counter online fraud.

Address Verification Service (AVS)

This system verifies a cardholder's billing address. It is currently only used by merchants in the UK.

1) Skimming

2) Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant. The thief can procure a victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store hundreds of victims' credit card numbers.

3) Carding

4) Carding is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product; a Web site subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the card issuer's attention.

5) Computer virus attacks

6) Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, and file sharing network spam.

7) People who create electronic spam are called *spammers*

8) E-mail spam, known as unsolicited bulk Email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

9) Mobile phone spam

Mobile phone spam is directed at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience but also because of the fee they may be charged per text message received in some markets. The term "SpaSMS" was coined at the adnews website Adland in 2000 to describe spam SMS.

10) Web search engine spam (Spamdexing)

11) Spamdexing refers to a practice on the World Wide Web of modifying HTML pages to increase the chances of them being placed high on search engine relevancy lists. These sites use "black hat search engine optimization techniques" to unfairly increase their rank in search engines. Many modern search engines modified their search algorithms to try to exclude web pages utilizing spamdexing tactics.

Malware

A short for *malicious software*, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses.

Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most root kits, spy ware, dishonest adware, crimeware and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of several U. S. states.

Malware is not the same as defective software, that is, software that has a legitimate purpose but contains harmful bugs.

Cyberterrorism

Cyberterrorism 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.

Cyberterrorism is defined as “The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.”

Cyberterrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries' economy greatly, thereby stripping it of its resources and making it more vulnerable to military attack.

Cyberterror can also affect internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals.

As internet-businesses have increasing economic importance to countries, what is normally cyber crime becomes more political and therefore "terror" related.

New Technologies

The high-tech crimes are happening through,

1. Wireless technology
2. 3G mobile phones
3. Multimedia messaging
4. Virtual money
5. Archives

Wireless Technology

Wireless local area network (WLAN) is one to which a computer can be connected without wires by means of so-called 'access points' or radio stations distributed throughout a building. Each access point has a particular range and serves a maximum number of clients.

A significant characteristic of WLAN is that a user has to share an access point with several other clients. This is known as 'shared media'. Multiple computer users use the same bandwidth and can listen in on all messages which are sent to and from the access point.

Monitoring communication

An unauthorized person could monitor communication within a wireless network and possibly elsewhere within the same company's network.

Data theft

The fact that an unauthorized user could access a network from inside means that he or she will very likely be able to read data within the network which could not otherwise be accessed from outside.

12) Data manipulation

An unauthorized user could change data which has already been saved or is being transmitted.

In addition to these illicit uses of a private WLAN, a client who uses a hotspot to transmit unencrypted data opens up the possibility for criminals to monitor - and possibly even modify - that data. There are also possibilities for criminals to piggy-back on communications to get inside corporate networks.

3G mobile phones

13) Telecommunication providers are introducing a new generation of mobile telephone technology, (third generation, or 3G), which will enable increased data-handling rates. This will allow mobile telephones to offer new features such as video streaming, video conference calling, transmission of video calls, and enhanced e-mail and web-browsing capabilities. There is considerable variety in the uptake across European countries: for example, in Italy, nearly 50% of mobile telephones are 3G units.

- There is a potential criminal market in stolen units given their high unit value. 'Chipping and pinning', the reprogramming of phones and personal identification numbers, is already widely available at the street level for pre-3G phones. If this becomes possible with 3G units, it could lead to a rise in related thefts.
- When units are stolen, there are issues related to the security of any sensitive data held on the units. This is a serious problem with 3G phones as they are in effect a crossover between telephones and portable computers. Data held on the units such as card or account numbers could be used to commit further fraud or theft.
- The streaming video and digital-imaging capabilities of the units hold the potential for misuse by online child abusers and voyeurs as surveillance/anti-surveillance devices by criminals. There is also the potential for use in extortion and blackmail. There have already been reports of use in election fraud, i.e. transmitting a live picture from within the election booth.
- Units may fall prey to Trojan-style attacks in an attempt to capture sensitive data either stored on the phone or transmitted via the unit, e.g. bank or card details. Such attacks have already been observed in the mobile and PDA markets over the past two years.
- The increased e-mail and video-conferencing capabilities open up the possibility that criminals will use such units as secure communication tools. This is likely to rise if instant messaging services become available on 3G phones.
- If such units are used to carry out voting in public elections, there is a danger that cloned or misappropriated phones could be used to skew results. This has already been a concern in Italy and Taiwan, and many countries are considering mobile-telephone-based voting systems.
- There is a possibility that re-dialer programs loaded onto the phone during web surfing could redirect web access or dial premium rate lines without the user’s knowledge, resulting in large telephone bills. The UK computer trade press has reported a rise in malicious re-dialer programs being disseminated, primarily by offshore premium line service pornography providers.
- The use of 3G phones to access the Internet and other web services may in itself encourage a new wave of virus writing and dissemination activity, increasing resource demands on both anti-virus providers and law enforcement.

14) Multimedia messaging

Multimedia messaging service (MMS) via mobile phones is a recent development which is slowly replacing short message service (SMS). The system aims at not only the exchange of messages between mobile phones but also between mobile phones and e-mail (and vice versa).

The content is not limited to text; it also comprises sound, images and other rich content. In other words, MMS enriches communication with 'real and live content'. Images or audio or video files are not attachments but appear within the body of the message as multimedia content.

The criminal risks related to the use of MMS are quite clear. The possibility of exchanging files in diverse forms represents a real threat to society if the content is illegal. It is easy to see how child sexual abuse images could be transmitted this way. The criminal use of this system could be very wide, e.g. the spread of viruses.

The main problem for law enforcement is the ease with which criminals could use the technology to upload, download and disseminate files with illegal content.

Another risk is anonymity: criminals can use virtually untraceable pre-paid cards for moving files and then discard them immediately after use.

Finally, the use of smart phones (as explained above) equipped with cameras may be an additional tool for criminals to disseminate illegal material.

Virtual money

Virtual money is defined as money value as represented by a claim on the issuer which is stored on an electronic device and accepted as a means of payment by persons other than the issuer.

Virtual money is an encrypted code representing money, in the same way that paper money is only paper bearing certain characteristics such as graphics and serial numbers. Virtual money is money in the real sense since it can be converted into other forms of money. Although historically it was a slow process, people have come to accept paper money as payment, and virtual money may become dominant as electronic transactions become more common.

Like conventional paper money, virtual money can function as a medium of exchange, a unit of account and a store of value. It is intended for use in place of coins and banknotes for the purpose of making electronic payments of small amounts. Like notes and coins, electronic cash represents ready money; it is not a credit instrument and there is no need for authorization from a bank or credit institution. Virtual money can be carried on a number of electronic devices and may be downloaded from an automatic cash machine, a shop-based terminal or the Internet. It can be used in the physical world by inserting a card into a terminal or through the use of wireless technology, and in the virtual world over the Internet from a PC or mobile phone or over telephone and television networks.

Many transactions over the Internet already take place with debit and credit cards. However, one of the advantages and purposes of virtual money is that it allows those individuals normally excluded from e-commerce, by reason of their economic status, for example, to participate. The cash-like nature of virtual money means that a good credit history or established banking relationship is not required. Another advantage of virtual money will be that small and new merchants can receive payment conveniently without the associated credit risks.

There are two kinds of virtual money:

- ***Identified virtual money*** - contains information revealing the identity of the person who originally withdrew the money from the bank. This can be traced through the economy, by the bank or law enforcement personnel, in much the same way as credit cards.
- ***Anonymous virtual money*** (also known as digital cash) - once it is withdrawn from an account, it can be spent or given away without leaving a transaction trail. Using blind signatures rather than non-blind signatures creates anonymous e-money.

Criminal possibilities

The main areas of criminal risk for virtual money are believed to be:

- Unauthorized creation, transfer or redemption of virtual money.
- Criminal access to computer systems being used to change illicitly the attribution of funds within the system.
- Criminal attacks on virtual money systems, leading to loss of virtual money value or loss of function of the virtual money system.

- Criminal misuse of virtual money systems for financial crimes or as a tool to subvert or misuse other financial systems.
- Criminals may use virtual money to reduce the likelihood of capture, for example, in cases of blackmail, kidnapping or extortion, where, in the past, the collection of money has been problematic for perpetrators. This is particularly significant for anonymous virtual money.

Online games now have their own foreign exchange which lets players buy and sell different virtual currencies, just as in the real world. Criminals will undoubtedly take advantage of this.

While it is accepted within the industry that non-face-to-face transactions may give rise to new risks of money laundering, at present there is no evidence that this is a bigger concern for Internet-based companies, particularly with respect to the regulated e-money sector.

II. Conclusions

Computer crime threatens our commercial and personal safety. Computer forensics has developed as an indispensable tool for law enforcement. But in the digital world, as in the physical world, the goals of law enforcement are balanced with the goals of maintaining personal liberty and privacy. Forensic computing is a complex area which involves a range of disciplines such as software engineering, cryptography, electronic engineering and data communications.

Jurisdiction over cyber crimes should be standardized around the globe to make swift action possible against terrorists whose activities are endangering security worldwide. Differences in the laws among countries prevented effective investigation against cyber terrorism, which is not bound by national boundaries, and each investigation could involve several countries. Finally prevention is better than cure. We can protect ourselves from cyber attack from the following, use antivirus software, insert firewalls, maintain backup, uninstall unnecessary software, and check security settings.

III. REFERENCES

[1]. Reserve Bank of India Mumbai, Report of the Working Group on Electronic Banking”, January 2011

[2]. Social Impacts of Cyber Crime Research Paper Starter - eNotes.com

[3]. http://www.interpol.int

[4]. http://www.wikepedia.org

[5]. http://www.cybercrime.com.au

[6]. http://www.oppapers.com