# A Survey of Cybercrime

**Zhicheng Yang**, yangzhicheng@wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 

## Abstract:

Cybercrime is a kind of crime that happens in "cyberspace", that is, happens in the world of computer and the Internet. Although many people have a limited knowledge of "cybercrime", this kind of crime has the serious potential for severe impact on our lives and society, because our society is becoming an information society, full of information exchange happening in "cyberspace". Thus, it is necessary to introduce cybercrime detailedly. While there are several textbooks talking about cybercrime, but focusing on the statutes and laws relevant this new breed of crime, few papers or textbooks focus on the "computer science" itself. In other words, most of materials talk about the "crime" of "cybercrime", but this paper will talk more about "cyber". In this paper, first, we will introduce the definition, origins and evolution of cybercrime. Second, the three categories of cybercrime, which are target cybercrime, tool cybercrime, computer incidental, are presented in each section respectively, where some latest cases will be studied. Finally, the summary will be given. **Keywords:** Survey, Cybercrime, Cyber, Crime, Cyber-crime, Cyber crime, Computer crime

## Table of Contents



## 1. Introduction

A lot of us have a limited knowledge of crime occurring in "cyberspace", known as cybercrime, which happens on computer and the Internet, however, cybercrime has a severe potential for remarkable impact on the lives of individuals and our society. Therefore, a detailed introduction of cybercrime needs to be presented. There are many terms used to describe cybercrime. The former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Also, Internet brought other new terms, like "cybercrime" and "net" crime. Other forms include "digital", "electronic", "virtual" , "IT", "high-tech" and technology-enabled" crime [Clough10]. However, on the one hand, each of them didn't cover the whole meaning of cybercrime, because there is no incorporation of networks. On the other hand, terms such as "high-tech" or "electronic" crime might be too broad to specify that the crime is the exact cybercrime, since other fields also have "hi-tech" developments like nanotechnology and bioengineering. Currently, although no one term has become totally dominant in use, "cybercrime" is the term used most pervasively. In general, cybercrime has three categories [Brenner10]:

1. target cybercrime: the crime in which a computer is the target of the offense.
2. tool cybercrime: the crime in which a computer is used as a tool in committing the offense.
3. computer incidental: the crime in which a computer plays a minor role in committing the offense.

The boundaries of these categories, actually, are not so clear. For example, if someone uses high-tech hacking into a computer or server, getting something valuable, it's hard to say it must be a "theft" in tool cybercrime or a "hacking" in target cybercrime. So why do we still categorize cybercrime? I think we can analyze cybercrime better and more efficiently by this way. Although there are some intersection, with categorization, we will focus on each part of cybercrime respectively and then have a comprehensive concept finally.

The history of cybercrime is short compared with traditional crimes. The first published report of cybercrime occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment allowed them to access into mainframe computers. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because of no Internet in that era [Brenner10]. In following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. Since Internet was invented, people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental. This process is similar to the process of learning one language. In childhood, we learn language itself; then, when we grow up and are good at it, we will use it to communicate with each other but itself is not a prime element. In general, current consensus on the classification of cybercrime is to divide it into three categories that are said in the first paragraph above. We can set another analogy: target cybercrime is like crossword, which focuses on the magic of language itself; tool cybercrime is similar to fraud or harassment on street or in other face-to-face ways, but the place in which tool cybercrime happens is not physical environment but cyberspace; computer incidental including some electronic proof is saved in computer or the camera captures the criminal withdrawing money in a bank. Generally, these three categories are elaborated in the three following sections and in each section some latest cases will be studied.

# 2. Target Cybercrime

When a computer is the target of offense, the perpetrator attacks the computer by breaking into it or attacking it from outside. This kind of cybercrime may be the most "professional" in three cybercrime categories, because the criminal does programming and makes use of some exploits on computer, who always has pretty strong professional background of computer science. In this chapter, the two main types of target cybercrimes will be introduced, which are hacking and malware. Before moving the next chapter, another common target cybercrime, DDoS attacks will be also examined.

## 2.1 Hacking

Almost everyone has heard "hacker", the one who does hacking. But what's the meaning of hacking on earth? For a simpler perception, hacking is similar to trespassing [Brenner10]. Trespass has been a kind of crime for a long history. The statutes of criminal trespass are designed to protect the sanctity and privacy of real estate, including land and building on land, by preventing people from going where they have no right to enter. Since computer is a kind of property, hacking is analogous to trespassing on one's real estate. In trespass, the person(s) is(are) seriously restricted, who can legally enter onto or into real property, such as land, building and so on; while in hacking, the person(s) is(are) seriously restricted, who can legally use computer technology. The following content includes two latest researches on hacking. Notice that the purpose of these researches is to find existing issues or exploits in cyberspace rather than to commit crimes, so they may be potentially used by professional criminals if the issues these researches have revealed are not still solved in the future.

### 2.1.1 Hack Faces to Find Social Security Numbers (SSN) [Networkworld11, Techworld11]

It is possible to take someone's photo from public online social-network database and within minutes acquire his/her SSN and other private data like personal interests and credit status.

The technique calls for linking faces of random individuals to images in public online social-network databases that contain other information about them and using face-recognition software and an algorithm to project Social Security numbers, says Alessandro Acquisti, a professor at Carnegie Mellon University, who presented the research at the Black Hat and Defcon conference. He pointed that the digital surveillance framework that can go from a person's image to personal data is very dangerous. To resolve this issue, better technologies need to be improved, privacy needs more scarce and surveillance needs readily available to the masses. Prof. Acquisti says, "This, I believe and fear, is the future we are walking into." He admits though this method is far from very effective, this technology will be developed very quickly and it is absolutely possible to be used in the future. On the conference, there are three pieces of this research showed as follows:

1. Find out one person's photo on Facebook, and then input it into the face-recognition software, called "PittPatt", to identify this person's other photos in other databases, which hold dating services and where users always register with phony names. As researchers consider just PittPatt's best guess for each photo, the accuracy rate is 1/10 , which is a great result since only one photo is used, the Facebook profile photo.
2. Randomly take photos for some students and ask them to fill out a questionnaire, and then compare their photos with the photos of online databases so that identify their names, ages and collect other photos of those students. Finally, students check if those photos are themselves and the accuracy rate is 1/3.
3. Based on the subjects' Facebook profiles, predict the first five digits of their SSN, personal interests and personal activities.

### 2.1.2 Hack On Universal Serial Bus (USB) Cable [Zdnet11, Wang10]

Angelos Stavrou, an assistant professor of computer science at United States-based George Mason University, and student Zhaohui Wang find a kind of attack to laptops and smartphones via USB cable. By programming a software to change the function of USB driver, they can make a secret attack during charging a smartphone or syncing data between a smartphone and a computer. This attack works by adding the function of keyboard and mouse into the USB driver. Thus, when the connection is built, attacker can steal files, upload Trojan horse (the definition of "Trojan horse" will be introduced in the Section 2.2) or something else. In general, the attacker can manipulate this computer. The reason for that is USB protocol can be used to connect any device to a computing platform without any authentication.

The software can recognize the operation system automatically. Detailedly, on Macintosh and Windows machines, a message pops up, informing a new human interface device has been detected, however, it is difficult to stop this process, while the pop-up message is disappeared swiftly. Even on Linux, there is no message popping up, so users have totally no idea about what happening.

Stavrou said this attacking software can be written in Android and Iphone OS, and it can work between two smartphones connected via a USB cable. Also, this software can be made into a virus program. If a smartphone is

contaminated, when it is connected with any computer, this computer will be also contaminated and then this computer will spread this virus to other smartphone connected via USB cable.

The current antivirus software have no effect, because the attacker controls computer just based on the common driver. "It's hard to separate good behaviour from bad behaviour when it comes from the keyboard" Prof. Stavrou said.

## 2.2 Malware

We always hear "computer virus", "computer worm" and "Trojan horse", however, what are they on earth? To answer this question, the best way is to explain separately each of them. In those terms above, the strict definition of "computer virus" is a computer program which can reproduce itself and spread from one computer to another [Wikipedia11a]. Computer worm uses a computer network to send copies of itself to other computer on the network [Wikipedia11b]. Trojan horse can perform a desirable function for the user prior to run or install, steal information and harm the system [Wikipedia11e]. Generally, malware, short for malicious software, includes computer viruses, computer worms, Trojan horses and other malicious and unwanted software [Wikipedia11a]. For a easier perception, like hacking, malware can also be analogized to a traditional crime in our real world, which is vandalism [Brenner10]. The crime of vandalism means someone damages, even destroys, the property of others without their permission. Notice that the "property" means the real or personal property. While computer system and data saved in computer are also personal property and computer viruses and worms can be used to damage or destroy them, though computer viruses and worms couldn't make the physical property damage, which may be caused by traditional vandalism, they are still regarded as a kind of vandalism, known as "malware". Let's set an extreme example. Suppose someone uses ax to destroy your laptop, which is your personal property, and this behavior is definitely vandalism because your laptop is damaged. However, if he/she uses viruses or worms to destroy your computer system, like you failing to log in Windows XP at all, or your electronic data, like there becoming no files in each of your local disk, this behavior is a cybercrime by malware. In addition, another condition we have to consider: perhaps a virus or worm is implanted in one's computer, however, this computer don't be damaged or destroyed, but is a medium, which will be potential to transmit those malware to other computer on Internet or local area network (LAN). We can call this computer is "harmed", like contamination or infection. The "harm" doesn't mean an existing damage or destroy but a potential [Brenner10], which is not covered by the definition of traditional vandalism but is absolutely a kind of malware. Since those malware, viruses and worms, also make use of exploits on computer or Internet, it is very important to keep the latest trend of malware in order to make up those exploits they have taken or intend to take use of . For preventing malware, many antivirus companies provide malware journals every month or every week. Especially, the leader company of antivirus, Kaspersky Lab, produces malware report every month. Therefore, the following content includes two latest parts on the malware report for October 2011 released by Kaspersky Lab on November 2011.

### 2.2.1 Duqu Trojan horse [Securelist11a, Arstechnica11]

The highlight in October was the detection of the Duqu Trojan horse, which is very similar to Stuxnet, the first cyber-weapon. Because these two malwares have tremendous similarities in the coding, it indicates that Duqu and Stuxnet are programmed by the same team, or Duqu is modified based on the source code of Stuxnet.

However, except the similarities, unlink Stuxnet, Duqu has no ability of attacking industrial systems. While Duqu files are found to contain a main module that makes sure the Trojan horse functions properly and establishes communication with the command server, it also contains an extra Trojan-Spy module, which is able to intercept data entered via a keyboard, capture screenshots and collect information of the system. Thus, all of these clues above show the main purpose of Duqu is to make industrial espionage rather than industrial sabotage.

After making a deeply investigation, the experts at Kaspersky Lab confirmed that the victim suffering from the recent Duqu attack is located primarily in Iran (once again echoing the parallels with Stuxnet). This finding indicated the close relationship of Duqu and Stuxnet. Since the experts also found the latest and old version of Duqu files, the people behind Duqu are continuing their activity. However, unlike the huge infection of Stuxnet,

Duqu can select carefully and attack the specific target. Moreover, a unique set of files is used in every attack. It is also possible that not only a Trojan-Spy module but also other modules set in Duqu files.

At the same time, in the security report released by Microsoft in November, Microsoft fails to patch Duqu, but fixes a critical exploit in Windows TCP/IP stack which seems a temporary solution. Actually, for patching Duqu, to find a possible solution still needs more time.

### 2.2.2 Malware on Android [Securelist11a]

For the mobile threats, October is a turning point. The statistics of Kaspersky Lab indicated this is the first time for the total number of malicious programs for Android exceeding that for Java 2 Micro Edition (J2ME). Notice that over the last two years, the most prevalent platform for malware has been J2ME among mobile threats. However, this dramatic change indicates that virus writers tend to concentrate on Android malware, which is a promising mobile platform.

At the end of October, the experts in Kaspersky Lab had detected 1,916 malware for Android belonging to 92 malware families, at the same time, 1,610 variations from 60 families were detected for J2ME. In all, the total number of mobile threats detected in October is 4,053 from 289 families. Figure 1 shows the details of malicious programs for all mobile platforms.

Particularly, let's use Antammi as an example, which is a malicious program appearing the official Android store from September. This malicious application acts as a normal ringtone downloading application, by which user has to send text messages to a paid service to receive tunes. This application can run in the background, stealing contacts, short message service (SMS) archives and global positioning system (GPS) coordinates and so on. This malicious program then sends the information about its activity to a Gmail address and the stolen information to a server. After informed by Kaspersky Lab in October, the Android online store removed another malicious application which included Trojan-Spy.AndroidOS.Antammi.b, designed for users in Russia.

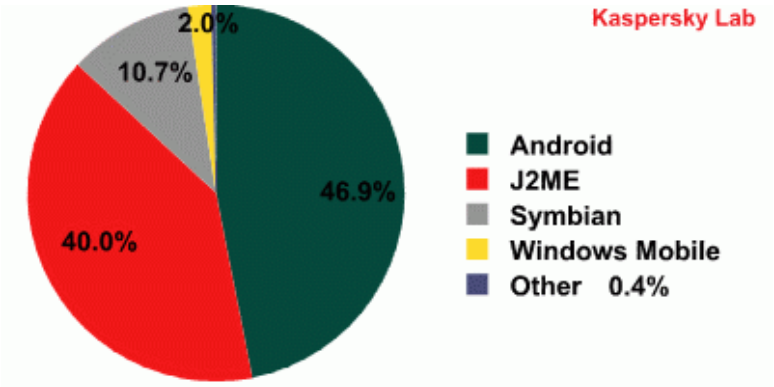


**Figure 1: Breakdown of malicious programs for all mobile platforms [Securelist11b]**

## 2.3 Distributed Denial of Service (DDoS)

A typical DDoS attack is an malicious behavior to make a computer resource unavailable to its intended users. Perpetrator of DDoS attacks typically focus on sites or services on high-profile web servers such as banks and credit card payment gateways [Wikipedia11c]. In a DDoS attack, the perpetrator uses a network of compromised computers, known as "zombies", to send tremendous data to the target(s) of the attack [Brenner10]. So what's the "zombie"? To explain it, the term "bot" should be explained at first. "Bots" is a kind of software that invisibly infiltrates a computer without the owner's awareness. "Zombie" are the computers that have been contaminated by "bots", who can take over "zombie" computers secretly. Therefore, the owners of "zombies" have no idea that their computers have already become minions of the moon for a malicious force. The only indication of "zombies" for the owner might be just that the running speed is a little slower than usual, but for a common user, not a master of computer science, it's difficult to smell some big serious problem based on this kind of tiny difference.

Zombie computers are integrated into a "botnet", a network controlled by a cyber criminal, known as the "botherder". A botnet is a huge digital army, including even two million zombie computers. The leader of this army, botherder, often order them to do some cyber criminals, such as shutting down websites and extorting money from their owners, sending spam emails and tricking users into online fraud, and installing adware [Brenner10]. However, it is difficult to find a good analogy to understand its concept, but the process of this attack is quite simple as Figure 2 shows. In Figure 2, the attacker, as the botherder, orders these compromised computer through handler to attack the target server via Internet Generally, For the use of DDoS attack, attackers may tell you they use this attack as a primarily tool to commit a traditional crime. The crime that DDoS attacks generally are used to commit is extortion [Brenner10]. The following content will focus on (1) a detailed introduction on how to make a successful extortion by using DDoS and (2) the issue of preventing DDoS attacks and the possible solution of these attacks.

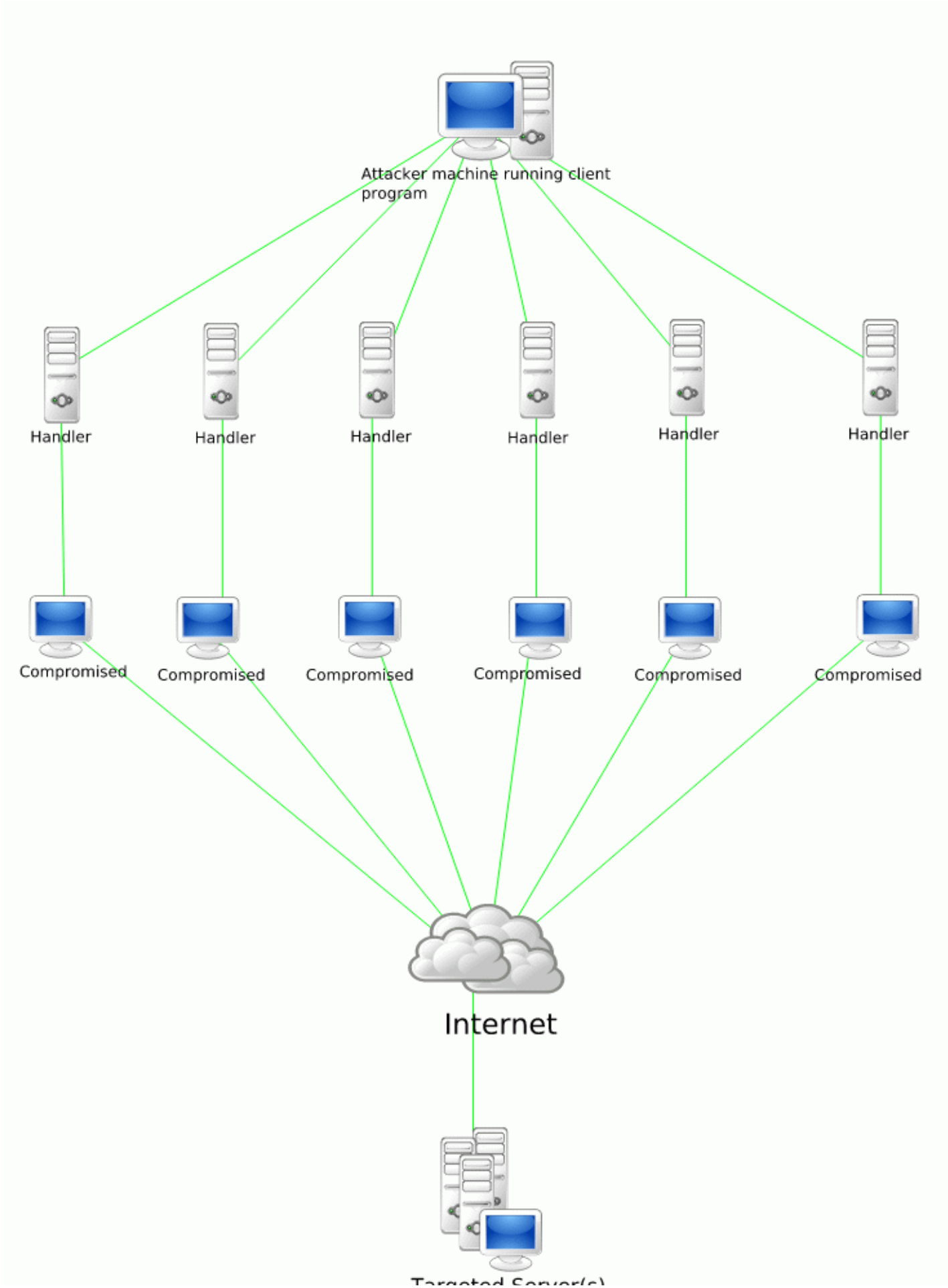
Attacker machine running client program
Handler
Handler
Handler
Handler
Handler
Handler
Compromised
Compromised
Compromised
Compromised
Compromised
Compromised
Internet

**Figure 2: Structure of DDoS [Wikimedia11]**

### 2.3.1 DDoS Extortion

As the above paragraph said, the crime that DDoS attacks are commonly used to commit is extortion. In particular, the best of example is attacking online casinos. In order to earn money, casinos should be online and available to gamblers, if they fail to do that, they will lose money. Meantime, the DDoS attack is a effective way to make a casino offline. The common way to make an extortion is that the attacker might send one email to the owner of an online casino, telling him/her here will be a big potential attack to his/her casino website, which can let him/her lose lots of money in a short time. The only way to solve it is to pay a certain amount of money to the attacker so that the attacker will cancel this DDoS attack. Actually, online casinos have no choice but pay off, since if their website are offline, they will lose an incomparable amount of money. As one observer noted, when a casino in offline for only several hours, it may lose "$500,000 to $1 million of action" in lost wagers [Brenner10]. Besides making DDoS attacks on online casinos, there are also DDoS attacks on portal sites and other great websites. Table 1 [Scribd11, Thenextweb10, Cnet11, Torrentfreak09] shows some representative DDoS attacks in 2000, 2009, 2010 and 2011. The reason why the attacks in 2000 are presented is in this year, the first DDoS attack was publicized, so many portal sites suffered from the first time of DDoS attack in 2000. Additionally, the purpose of DDoS attacks might also include a showing off the attacker's hacking ability, not only for money.

**Table 1: Some representative DDoS attacks in 2000, 2009, 2010 and 2011**

| Website suffering from DDoS attack | Date |
|---|---|
| Yahoo! | February 7, 2000 |
| Amazon | February 8, 2000 |
| Buy.com | February 8, 2000 |
| CNN | February 8, 2000 |
| eBay | February 8, 2000 |
| E*Trade | February 9, 2000 |
| ZDNet | February 9, 2000 |
| Mininova | March, 2009 |
| Visa | December, 2010 |
| MasterCard | December, 2010 |
| Paypal | December, 2010 |
| Wordpress | March 4, 2011 |

### 2.3.2 Difficulty of Prevention and Content Distribution Network (CDN) [Trendmicro09, Wikipedia11f]

In fact, DDoS attacks are difficult to defense. There is an article, written by Todd Thiemann, the senior director of security vendor Trend Micro Inc, illustrating the reason. Most network countermeasures fail to protect against DDoS attacks, since they cannot stop the deluge of traffic and cannot tell a good content from a bad one. Although intrusion prevention systems (IPS) are effective on the attacks having pre-existing signatures but are not effective if the content is legal with malicious intentions. Analogously, firewalls use some simple rules to allow or deny protocols, ports or IP addresses. DDoS attacks can bypass IPS devices and firewalls easily because their traffic is legitimate, like HTTP requests to a web server. Moreover, these attacks generate tremendous traffic from many distinct hosts so that the internet connection cannot deal with these traffic.

The possible way to relieve the harm of DDoS attacks is to use CDN. A CDN is a computer system, including data copies placed at various nodes in a network. A CDN can improve access to the data it caches by increasing access bandwidth and reducing access latency. Technically, it can solve the issues that the bandwidth of network is

narrow, the traffic is huge and the density of nodes in a network is uneven. Since portal sites use CDN now, they are rarely influenced by DDoS attack.

In this section, the three main types of target cybercrime, which means a computer is the target of the offense in this crime, are introduced, including hacking, malware and DDoS attack. In next section, the second category of cybercrime, tool cybercrime will be presented.

# 3. Tool Cybercrime

Tool cybercrime means crimes in which a computer is used as a tool in committing the offense. Hence for the tool cybercrimes, the role of computer is similar to the role telephone plays in telephone fraud [Brenner10]. Therefore, in this section, the ways computer is used to commit traditional crimes against property will be introduced, including theft, fraud and extortion. Also, the ways computer is used to commit traditional crimes against persons will be introduced, including two classes: psychological harm and physical harm.

## 3.1 Crimes Against Property

In this discussion, how computers can be used to commit traditional crime against property will be presented, such as fraud, theft and extortion.

### 3.1.1 Theft

Actually, as the introduction said above, cybercrime is hard to be very strictly classified into several categories. Therefore, if someone use high-tech method to hack the target computer or server in order to steal something valuable, it might be difficult to classify this behavior into either "hacking" in target cybercrime or "theft" in tool cybercrime. Let us set a sort of extreme example to classify them. Suppose you have a set of username and password of a private webpage, which includes other members' profiles. Actually, those profiles are public for the members of this network. You can copy them on your local dictionary, but this behavior is not good. If you do that, you are suspected to commit the crime of information theft. The fact that other members' profiles are on the webpage is weird, so might be an exploit, but you made use of it. However, you got those profiles very easily, without programming for hacking this webpage from outside. Instead, you just made use of the possible existing exploit to gather those profiles, even unintentionally. I guess this is the tiny difference between hacking for profit and theft by computer, based on the difficulty to obtain things or the technology you use.

### 3.1.2 Fraud

Fraud, which has exploded in cyberspace, means enticing someone into giving his/her property [Brenner10]. Generally, there are 12 different kinds of online fraud. However, we are very sure that new patterns are always emerging, as the development of the utilization of cyberspace. The current 12 different kinds consist of identity theft; purchase scams; money transfers fraud; dating scams; click fraud; international modem dialing; Internet marketing and retail fraud; Internet marketing and SEO fraud; phishing; e-mail spoofing; pharming; and stock market manipulation schemes [Wikipedia11d]. Actually, fraud will hardly happen if everybody don't be so greedy. This crime is a kind of "passive" crime for perpetrator, as the victims always have a greedy appetite. Perhaps they are obsessed by a huge bunch of money, a gorgeous girl or a big deal for saving a lot of money. The criminals make great use of the avaricious mind of those victims so that they can succeed.

### 3.1.3 Extortion

The DDoS attack in the section of target cybercrime showed a common way of extortion in cyberspace. However, the content of extortion is far more than this example. Actually, as long as one gets some of critical or private materials, no matter paper-based or electronic, he/she can definitely make an extortion in cyberspace, just like an

extortion by phone during the common scene of kidnap we always see on TV. But here, the extortion is restricted to happen in cyberspace, in particular, on computer or Internet. Notice here is a subset of extortion, known as "blackmail" [Brenner10]. Blackmail means using a threat to force someone to give money or property to the blackmailer. Usually, blackmail could expose a secret that can destroy the victim's public reputation. However, to send a blackmail, the perpetrator must achieve access to secret information about the victim's private life. Thus, that's why blackmail is far less common than extortion, which can be easily to commit.

## 3.2 Crimes Against Persons

People can use cyberspace to harm each other in many ways. As the online crimes against persons are common, this discussion is divided into two classes: physical harm and psychological harm.

### 3.2.1 Physical Harm

There are only few types in which computer is used to make physical injury or death. The possible use of cyberspace for physical injury might be to commit rape. As far as I know, here are some cases in the world in which male criminals entice their female net friends to have a face-to-face appointment , based on online chatting tools, like MSN or Gtalk, and then rape them. For instance, at the beginning, a criminal acts as a considerate and warm-hearted net friend of the victim to obtain her trust. As the relationship between criminals and victims is becoming closer, the criminal may ask for an appointment by face-to-face. After meeting the victim, the criminal might force or trick the victim to have a sexual behavior. When it comes to physical death, there might be two methods cyberspace can be used to kill someone's life: suicide and murder [Brenner10]. First, in suicide case, a victim always has psychological problem in some degree, thus, when someone may tell him/her some malicious comment on himself/herself from others, he/she may go desperate and take his/her own life. The Meier case [Brenner10] is a good example for this. While, secondly, in murder case, a good example is that someone gets access to the hospital database to modify the prescription of patients so that nurses and doctors caring about those patients would take a totally wrong treatment on them based on the revised prescription.

### 3.2.2 Psychological Harm

If we say physical harm as "hard" harm, psychological harm can be regarded as "soft" harm, since they are hard to be tangible. Also, this kind of soft harm is hard to be categorized and targeted by criminal law [Brenner10]. There are two main types of soft harm crimes: threat and harassment. First, threat is always believed as an incomplete crime, because it doesn't indicate the actual fact of a crime. For example, someone just, maybe via emails, makes a threat against you that you will be killed if you won't do what he/she want you to do, however, he don't have any opportunity and ability to kill you at all. His threat just causes your psychological harm. However, modern criminal law criminalize attempts on the theory that it protects public safety [Brenner10]. Thus, the threat in the example above or the potential intention of rob or vandalism will break the law. Secondly, harassment, sometimes accompanied with stalking, is a new type of crime. In this case, someone may use computer to send "vulgar, profane, obscene or indecent language" to the victim, which can cause substantial emotional distress to the victim [Brenner10].

In this section, the main two types of tool cybercrime, which means a computer is used as a tool in committing the offense in this crime, are introduced, including crimes against property and persons. For each type, several typical ways to commit a crime are presented, such as fraud, theft, extortion in crimes against property and psychological harm, physical harm in crimes against persons. In next section, the last category of cybercrime will be presented

# 4. Computer Incidental

Computer incidental means crimes in which a computer plays a minor role in committing the offense. Students in law school might be more familiar with this part, compare with ones whose major is computer science. Hence in this part, topics which are really related to computer science will be less. Actually, since the computer is a source

of evidence in these crimes, the challenges of obtaining evidence from cyberspace should be focused on. The challenges fall into two categories: digital evidentiary challenge and privacy [Brenner10].

In the first place, since electronic evidence is different from traditional paper evidence, prosecutors has to face several of evidentiary challenges in cybercrime prosecutions, including Trojan horse defense, authenticity of evidence and inadmissible hearsay [Brenner10]. As what we talked about in the section of malware, Trojan horse is a kind of malware, which can perform a desirable function for the user prior to run or install, steal information and harm the system [Wikipedia11e]. Trojan horse can contaminate a computer into a "zombie"computer. In the situation of Trojan horse defense, someone, who are claimed to commit DDoS attack on the target computer, might be not the real criminal, because it is possible that his/her computer has become a "zombie" computer in botnet. Therefore, it is also possible that the attacker manipulates this "zombie" computer to do an DDoS attack into the target computer without the aware of the owner of "zombie" computer. In this case, if there is no evidence to prove whether there is a Trojan horse implanted in the defendant's computer or not, the defendant cannot be sentenced as the one committing this crime. Second, the items' authenticity must be proved before they are introduced into evidence at trial, that is, they must be showed they are what the purport to be [Brenner10]. For example, when a police officer finds some chat records and emails, in which there exist the defendant's names, in the defendant's computer, which may become critical evidence. Those items seem incontrovertible, however, the chat records can be possibly modified after the fact from a user's homepage, Also, even though the emails include the defendant's names, it is also possible that someone uses the defendant's account to send those emails. Third, hearsay is also an issue when prosecutor introduces some information into evidence. If an item is regarded as hearsay, it must not be an evidence at trial. Generally, records generated by computer might not be hearsay, as they lack a human declarant, but computer documents generated by a human often are considered hearsay [Brenner10]. For example, if a person introduces an email talking about what he/she heard from the dead's last words. This email is vulnerable, if there is no other evidence to prove the fact of the dead's dying words and there is no other evidence to prove the words the person retails are definitely the same as the dead's dying words. Thus, this example is a situation of hearsay in hearsay, which is absolutely rejected to be introduced into an evidence at trial.

In the second place, privacy is the second main challenge of obtaining evidence from cyberspace. Even though a prosecutor has obtained dominant electronic items, but by an illegal way, like implanting a Trojan horse on defendant's computer or running a brute-force cracker to get a password, which is a method that trying every possible letter and number combination in order to match the target's real password, those items are still not admitted to become an available evidence, because the way the prosecutor used has violated the defendant's privacy.

In this section, the two main challenges of computer incidental, which means crimes in which a computer plays a minor role in committing the offense, are introduced, including digital evidentiary challenge and digital privacy. In next section, the summary of this survey paper will be presented.

# 5. Summary

In this paper, the three main categories of cybercrime are introduced.: (1) target cybercrime: crimes in which a computer is the target of the offense. In this category, three main target cybercrimes are presented, including hacking, malware and DDoS attack. Actually, target cybercrime is the most professional crime on cyberspace. The defense of target cybercrime always has time lag, since we always take actions to patch an exploit after a novel method is revealed. In other words, the active defense is difficult. (2) tool cybercrime: crime in which a computer is used as a tool in committing the offense. In this category, crime against property, including theft, fraud and extortion, and crime against persons, including physical harm and psychological harm are examined. (3) computer incidental: crimes in which a computer plays a minor role in committing the offense. In this category, the challenges for collecting the evidence are presented, which include evidentiary challenge and digital privacy. In all, cybercrime is a new type of crime, compared with traditional crimes, but the harm caused by the former is not less than the latter. Thus, we hope people obtain a general concept of cybercrime so that protect our cyber-security better from now.

# References


1. [Brenner10] Susan W. Brenner, "Cybercrime: Criminal Threats from Cyberspace," Praeger, 2010, ISBN-13: 978-0313365461.
2. [Clough10] Jonathan Clough, "Principles of Cybercrime," Cambridge, 2010, ISBN-13: 978-0521899253.
3. [Networkworld11] "Black Hat: System links your face to your Social Security number and other private things"; http://www.networkworld.com/news/2011/080111-blackhat-facial-recognition.html [A news talking about one hacking method to get people's private data].
4. [Techworld11] "10 scariest hacks from Black Hat and Defcon"; http://www.techworld.com.au/slideshow/397747/10_scariest_hacks_from_black_hat_defcon_/?image=1 [General introduction of 10 scariest hacks from Black Hat and Defcon conference].
5. [Wang10] Zhaohui Wang, Angelos Stavrou, "Exploiting Smart-Phone USB Connectivity For Fun And Profit," In the Proceedings of the 26th Annual Computer Security Applications Conference (ACM ACSAC), December 6-10, 2010, pp. 357-366.
6. [Zdnet11] "Viral USB attack borne from Black Hat"; http://www.zdnet.com.au/viral-usb-attack-borne-from-black-hat-339308710.htm [A new research on USB cable attack in Black Hat DC conference 2011].
7. [Securelist11a] "Monthly Malware Statistics: October 2011"; http://www.securelist.com/en/analysis/204792200/Monthly_Malware_Statistics_October_2011 [The monthly malware report in October 2011 released by Kaspersky Lab].
8. [Arstechnica11] "Microsoft fails to patch Duqu, but fixes critical hole in Windows TCP/IP stack"; http://arstechnica.com/business/news/2011/11/microsoft-fails-to-patch-duqu-but-fixes-critical-hole-in-windows-tcpip-stack.ars [The Microsoft security news in November 2011, introducing the failure of patching the new Trojan horse, Duqu].
9. [Wikipedia11a] "Computer Virus"; http://en.wikipedia.org/wiki/Computer_virus [General introduction of computer virus, including several categories].
10. [Wikipedia11b] "Computer Worm"; http://en.wikipedia.org/wiki/Computer_worm [General introduction of computer worm, including its history].
11. [Wikipedia11c] "Denial-of-service Attack"; http://en.wikipedia.org/wiki/Denial-of-service_attack [General introduction of denial-of-service attack, including its methods].
12. [Wikipedia11d] "Internet fraud"; http://en.wikipedia.org/wiki/Internet_fraud [General introduction of Internet fraud, including its categories].
13. [Wikipedia11e] "Trojan Horse"; http://en.wikipedia.org/wiki/Trojan_horse_(computing) [General introduction of Trojan horse, including its definition].
14. [Scribd11] "Report"; http://www.scribd.com/doc/55333480/Report#open_download [A report released in 2011, including the history of DDoS attack].
15. [Thenextweb10] "How DDoS attacks became the frontline tool of cyber-war"; http://thenextweb.com/media/2010/12/19/how-ddos-attacks-became-the-frontline-tool-of-cyber-war/ [A news in Dec 2010, including the information of DDoS attack to some websites].
16. [Securelist11b] "http://www.securelist.com/en/images/vlill/top20_october2011_pic01_en.png"; http://www.securelist.com/en/images/vlill/top20_october2011_pic01_en.png [A graph shows the breakdown of malicious programs for all mobile platforms in October 2011].
17. [Wikimedia11] "http://upload.wikimedia.org/wikipedia/commons/3/3f/Stachledraht_DDos_Attack.svg"; http://upload.wikimedia.org/wikipedia/commons/3/3f/Stachledraht_DDos_Attack.svg [A graph shows the structure of DDoS attacks].
18. [Cnet11] "WordPress hit by 'extremely large' DDoS attack"; http://news.cnet.com/8301-1009_3-20038874-83.html [A news about a latest DDoS attack to Wordpress].
19. [Torrentfreak09] "Mininova Hit By Massive DDoS Attack"; http://torrentfreak.com/mininova-hit-by-massive-ddos-attack-090307/ [A news about a recent DDoS attack to Mininova].
20. [Trendmicro09] "DDoS and the Cloud: Sad but True"; http://cloudsecurity.trendmicro.com/ddos-and-the-cloud-sad-but-true/ [An article talking about the difficulty of preventing DDoS attacks].
21. [Wikipedia11f] "Content delivery network"; http://en.wikipedia.org/wiki/Content_delivery_network [General introduction of content delivery network, including its definition].

# List of Acronyms

DDoS = Distributed Denial of Service
SSN = Social Security Number
USB = Universal Serial Bus
LAN = Local Area Network
J2ME = Java 2 Micro Edition
CDN = Content Distribution Network
IPS = Intrusion Prevention Systems
SMS = Short message Service
GPS = Global Positioning System

---

Last modified on Nov 27, 2011
This and other papers on latest advances in network security are available on line at http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page