General Idea

Many crimes involving computers are no different from crimes without computers, the computer is only a tool that a criminal uses to commit a crime. For example:

- Using a computer, a scanner, graphics software, and a high-quality color laser or ink jet printer for forgery or counterfeiting is the same crime as using an old-fashioned printing press with ink.
General Idea

- Stealing a laptop computer with proprietary information stored on the hard disk inside the computer is the same crime as stealing a briefcase that contains papers with proprietary information.

- Using computers can be another way to commit either larceny or fraud.

General Idea

- After about 1975, it became common to enter programs and data from remote terminals (a keyboard and monitor) using a modem and a telephone line. This same technology allowed banks to retrieve a customer's current balance from the bank's central computer, and merchants to process credit card billing without sending paper forms.

General Idea

- But this change in technology also meant that a criminal could alter data and programs from his home, without physical entry into the victim's building. The traditional laws were no longer adequate to punish criminals who used computer modems.
Introduction

- There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to calculate.

Introduction

- Nevertheless, there is a consensus among both law enforcement personnel and computer scientists who specialize in security that both the number of computer crime incidents and the sophistication of computer criminals is increasing rapidly.

Introduction

- Estimates are that computer crime costs victims in the USA at least US$ $5\times10^8$/year, and the true value of such crime might be substantially higher. Experts in computer security, who are not attorneys, speak of "information warfare".
new crimes in cyberspace

There are three major classes of criminal activity with computers:

1- unauthorized use of a computer, which might involve stealing a username and password, or might involve accessing the victim’s computer via the Internet through a backdoor operated by a Trojan Horse program.

2- Creating or releasing a malicious computer program (e.g., computer virus, worm, Trojan Horse).

3- Harassment and stalking in cyberspace.

False origin

There are many instances of messages sent in the name of someone who neither wrote the content nor authorized the sending of the message. For example:

1- E-mails with bogus From: addresses were sent automatically by malicious programs (e.g., the Melissa virus in 1999, the BadTrans worm in 2001, the Klez program in 2002).

2- Posting messages in an Internet newsgroup or online bulletin board with a false author’s name that is intended to harm the reputation of the real person of that name.

The major classes of criminal activities with computers
1. Unauthorized Use

Unauthorized use of computers tends generally takes the following forms:

1. **Computer voyeur.** The criminal reads (or copies) confidential or proprietary information, but data is neither deleted nor changed.

In 1999, the Melissa virus infected a [possibly confidential] document on a victim's computer, then automatically sent that document and copy of the virus via e-mail to other people. Subsequently, the SirCam and Klez malicious programs made a similar release of [possibly confidential] documents from a victim's computer.

These malicious programs are a new way to release confidential information from a victim's computer, with the confidential information going *not* to the author of the malicious program, but to some person unknown to the author of the malicious program.
2- **Changing data.** For example, change a grade on a school transcript, add "money" to a checking account, etc. Unauthorized changing of data is generally a fraudulent act.

3- **Deleting data.** Deleting entire files could be an act of vandalism or sabotage.

4- **Denying service to authorized users.** On a modern time-sharing computer, *any* user takes some time and disk space, which is then not available to other users. By "denying service to authorized users", for example:

   a- by sending large amounts of junk e-mail in one day, a so-called "mail bomb",
   b- by having the computer execute a malicious program that puts the processing unit into an infinite loop, or,
   c- by flooding an Internet server with bogus requests for webpages, thereby denying legitimate users an opportunity to download a page and also possibly crashing the server. This is called a denial of service (DoS) attack.
To successfully use a remote computer, any user (including criminals) must have both a valid user name and valid password. There are several basic ways to get these data:

1. Call up a legitimate user, pretend to be a system administrator, and ask for the user name and password. This sounds ridiculous, but many people will give out such valuable information to anyone who pretends to have a good reason.

2. Search user's offices for such data, as many people post their user name and password on the side of their monitor or filing cabinet, where these data can be conveniently seen.

3. Write a program that tries different combinations of user names and passwords until one is accepted.

4. Use a packet "sniffer" program to find user names and passwords as they travel through networks.

5. Search through a garbage bin behind the computer building in a university or corporate campus, find trash paper that lists user names and passwords.
Attack Scenario

- In recent years, there have been a large number of attacks on websites by hackers.
- In a typical attack, the hacker will delete some pages or graphics, then upload new pages with the same name as the old file, so that the hacker controls the message conveyed by the site.

Cont.

- This is not the worst kind of computer crime. The proper owner of the site can always close the website temporarily, restore all of the files from backup media, improve the security at the site, and then re-open the site.
- Nonetheless, the perpetrator has committed a computer crime by making an unauthorized use of someone else's computer or computer account.

DoS Attack

Denial of Service (DoS) Attacks

- A denial of service attack occurs when an Internet server is flooded with a nearly continuous stream of bogus requests for webpages, thereby denying legitimate users an opportunity to download a page and also possibly crashing the webserver.
- Criminals have developed a simple technique for executing a distributed DoS attack:
1- The criminal first plants remote-control programs on dozens of computers that have broadband access to the Internet. The remote-control program will, at the command of the criminal, issue a nearly continuous series of pings to a specified victim's website.

2- When the criminal is ready to attack, he instructs the programs to begin pinging a specific target address. The computers containing the remote-control programs act as "zombies".

3- The victim computer responds to each ping, but because the zombie computers gave false source addresses for their pings, the victim computer is unable to establish a connection with the zombie computers. Because the victim computer waits for a response to its return ping, and because there are more zombie computers than victims, the victim computer becomes overwhelmed and either (a) does nothing except respond to bogus pings or (b) crashes.

4- Typically, after one or two hours, the criminal instructs his programs to stop pinging the victim. This brief duration is not because the criminal is a nice person, but because long-duration attacks make it easier for engineers at the victim's website to promptly trace the source of the attacks.
Examples of DoS Attacks

The following is one case involving a famous series of DoS attacks:

1- The Yahoo website was attacked at 10:30 PST on Monday, 7 Feb 2000. The attack lasted three hours. Yahoo was pinged at the rate of one gigabyte/second.

2- The websites of amazon.com, buy.com, cnn.com, eBay.com were attacked on Tuesday, 8 Feb 2000. Each attack lasted between one and four hours. CNN reported that the attack on its website was the first major attack since its website went online in August 1995.

Cont.

3- The websites of E*Trade, a stock broker, and ZDNet, a computer information company, were attacked on Wednesday, 9 Feb 2000.

4- About fifty computers at Stanford University, and also computers at the University of California at Santa Barbara, were amongst the zombie computers sending pings in these DoS attacks.

2- Malicious Computer Programs

The following are general terms for any computer program that is designed to harm its victim(s):

- malicious code
- malicious program
- malware (by analogy with "software")
- rogue program
Classes of Malicious programs

- Malicious computer programs are divided into the following classes:

1- A **virus** is a program that "infects" an executable file. After infection, the executable file functions in a different way than before: maybe only displaying a benign message on the monitor, maybe deleting some or all files on the user's hard drive, maybe altering data files.

Cont.

2- A **worm** is a program that copies itself. The distinction between a virus and worm, is that a virus never copies itself – a virus is copied only when the infected executable file is run.

Cont.

3- A **Trojan Horse** is a deceptively labeled program that contains at least one function that is unknown to the user and that harms the user. A Trojan Horse does *not* replicate, which distinguishes it from viruses and worms.
4- A logic bomb is a program that "detonates" when some event occurs. The detonated program might stop working (e.g., go into an infinite loop), crash the computer, release a virus, delete data files, or any of many other harmful possibilities.

5- A time bomb is a type of logic bomb, in which the program detonates when the computer's clock reaches some target date.

6- A hoax is a warning about a nonexistent malicious program.

"Justification" for malicious programs

- Designing and releasing malicious computer programs is not only unethical, but also unlawful. However, some people defend the authors of malicious code by offering one or more of the following justifications:
  1- The malicious code exposes security flaws in operating systems and applications software.
2- It is the victim's fault if they are infected by a worm or virus that exploits a known security flaw, for which a patch is available.
3- It is ok if the author of the malicious code does not alter or delete any of the victim's data files.

Cont.
4- The virus/worm was a laboratory experiment gone awry.
5- The virus/worm was "accidentally" released.
6- The author of the virus/worm did not know how rapidly the virus/worm would propagate.

Cont.

3. Harassment & Stalking
- In general, the harasser intends to cause emotional distress and has no legitimate purpose to his communications. Harassment can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender.
Cont.

- It is often difficult to get law enforcement personnel and prosecutors interested in harassment, unless threats of death or serious bodily harm are made, simply because the resources of the criminal justice system are strained by "more serious" criminal activities.

Conclusion

- The fundamental issue in most computer crime is the criminals' lack of respect for the property or privacy of other people. I hope that society will recognize the seriousness of computer crime and demand more severe punishment for such criminals.

References

- Copyright 1999, 2002 by Ronald B. Standler
- [http://www.rbs2.com/ccrime.htm](http://www.rbs2.com/ccrime.htm)