CHAPTER 3
COMPUTER AND INTERNET CRIME

ETHICS IN INFORMATION TECHNOLOGY
2ND Edition 2007 by George Reynolds

OBJECTIVES

1. Identify key trade-offs and ethical issues associated with safeguarding of data and information systems.
2. Enumerate some causes concerning the rapid growth of Internet-related security incidents in recent years.
3. Describe the most common types of computer security attacks.
4. Outline the characteristics of common perpetrators including their objectives, available resources, willingness to accept risk, and frequency of attack.
5. Describe a multi-level process for managing Internet vulnerabilities based on the concept of reasonable assurance.
6. Discuss some actions that must be taken in response to a security incident.

WHAT IS A CRIME?

CRIME is the breach of rules or laws for which some governing authority (via mechanisms such as legal systems) can ultimately prescribe a conviction. Individual human societies may each define crime and crimes differently.

While every crime violates the law, not every violation of the law counts as a crime; for example: breaches of contract and of other civil law may rank as "offences" or as "infractions". Modern societies generally regard crimes as offenses against the public or the state, distinguished from torts (offenses against private parties that can give rise to a civil cause of action).

ATTY. SAMUEL R. MATUNOG
Matunog & Associates

CEO, Segworks Technologies Corp.
President, Davao Software Industries Association

“Crime is an act that needs to be controlled because they are destructive to public order”

IT SECURITY INCIDENTS

Year	Mail Messages Processed	Hotline Calls Received	Incidents Report Received
1997	39,626	1,058	2,134
1996	31,268	2,062	2,573
1995	32,084	3,428	2,412
1994	29,580	3,665	2,340
1993	21,267	2,282	1,334
1992	14,463	1,995	773
1991	9,629	-	406
1990	4,448	-	252
1989	2,869	-	132
1988	539	-	6

IT SECURITY INCIDENTS

Year	Mail Messages Processed	Hotline Calls Received	Incidents Report Received
2006	674,235	977	-
2005	624,634	591	-
2004	717,863	795	-
2003	542,754	934	137,529
2002	204,841	880	82,094
2001	118,907	1,417	52,658
2000	56,365	1,280	21,756
1999	34,612	2,099	9,859
1998	41,871	1,001	3,734

INCREASE INTERNET SECURITY INCIDENTS

- Increasing complexity increases vulnerability.
- Higher computer user error and access to information.
- Expanding and changing environment introduces new risks.
- Increased reliance on commercial software with known vulnerabilities.

TYPES OF ATTACKS

VIRUS

is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event.

HISTORY (Virus)

ACADEMIC WORK

- **1949** - John von Neumann's "Theory & Organization of Complicated Automata"
- **1972** -Veith Risak article "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Self-reproducing automata with minimal information exchange)
- **1980** - Jürgen Kraus' thesis "Selbstreproduktion bei Programmen" (Self-reproduction of programs) at the University of Dortmund.

HISTORY (Virus)

VIRUS PROGRAMS

1970's - CREEPER VIRUS by Bob Thomas

1981 - ELK CLONER by Richard Skrenta

1986 - ©BRAIN by Farooq Alvi Brothers, Lahore Pakistan

TYPES OF ATTACKS

WORM

is also a harmful computer program and has the ability to propagate without human intervention unlike virus.

HISTORY (Worm)

The actual term 'worm' was first used in John Brunner's 1975 novel, The Shockwave Rider. In that novel, Nichlas Haflinger designs and sets off a data-gathering worm in an act of revenge against the powerful men who run a national electronic information web that induces mass conformity. "You have the biggest-ever worm loose in the net, and it automatically sabotages any attempt to monitor it... There's never been a worm with that tough a head or that long a tail!

On November 2, 1988, Robert Tappan Morris, a Cornell University computer science graduate student, unleashed what became known as the Morris worm, disrupting perhaps 10% of the computers then on the Internet and prompting the formation of the CERT Coordination Center and Phage mailing list. Morris himself became the first person tried and convicted under the 1986 Computer Fraud and Abuse Act

TYPES OF ATTACKS

TROJAN HORSE

Is a program that gets secretly installed on a computer, planting a harmful payload that can allow the hacker who planted it to do such things as steal passwords or spy on users by recording keystrokes and transmitting them to a third party.

HISTORY (Trojan Horse)

- **1200 BC**, the Greek army, seeking entrance into the city of Troy, built a large wooden horse, hid its army inside of it and left it at the gates of Troy. The Trojans, thinking that victory has been achieved, rolled the horse into their city. That night Troy fell.
- **1975**, John Walker wrote a program called Pervade to help distribute the then popular animal game. Every time the user would launch the game it would copy itself into the directory of other users. The program wasn't malicious.
- **2000**, Written by Onel de Guzman, the ILOVEYOU Trojan disguised itself in the form of an “I Love You” email letter and overtook the computer. This has been the most costly virus to businesses causing over $5 billion in damages.
- **2002**, Beast was released and written by Tataye; it is a back-door trojan that allows remote, administrative access to a victim's computer
- 2006, The first trojan to strike a Mac appeared in 2006, it was called Leap-A and was distributed via iChat.

LOGIC BOMB (Trojan Horse)

- A logic bomb is a type of Trojan horse that executes when a specific condition occurs

- Logic bombs can be triggered by a change in a particular file, typing a specific series of key strokes, or by a specific time or date.

- Many viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs"

TYPES OF ATTACKS

DENIAL-OF-SERVICE

is an attempt to make a computer resource unavailable to its intended users. It generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

Examples include :

- ✓attempts to "flood" a network, thereby preventing legitimate network traffic
- ✓attempts to disrupt connections between two machines, thereby preventing access to a service
- ✓attempts to prevent a particular individual from accessing a service
- ✓attempts to disrupt service to a specific system or person

Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack.

CLASSIFICATION OF PERPETRATORS OF COMPUTER CRIME

Type of Perpetrator	Objective	Resources available to perpetrator	Level of risk taking acceptable to perpetrator	Frequency of Attack
Hacker	Test limits of system, gain publicity	Limited	Minimal	High
Cracker	Cause problems, steal data, corrupt systems	Limited	Moderate	Medium
Insider	Financial gain or disrupt company's information systems	Knowledge of systems and passwords	Moderate	Low
Industrial Spy	Capture trade secrets or gain competitive advantage	Well funded, well trained	Minimal	Low
Cybercriminal	Financial gain	Well funded, well trained	Moderate	Low
Cyber Terrorist	Cause destruction to key infrastructure components	Not necessarily well funded nor well trained	Very High	Low

TYPES OF PERPETRATOR

HACKER

an individual who tests the limitations of systems out of intellectual curiosity.

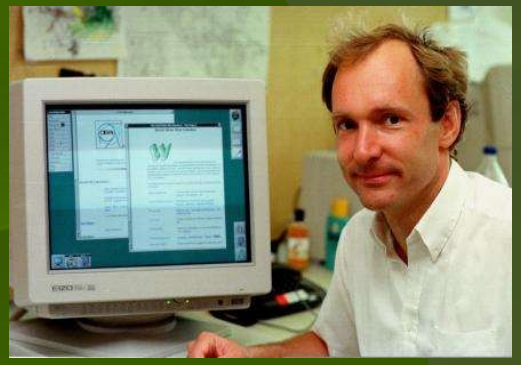
WHITE HAT HACKERS

- These are hackers that use their skills for good.
- These hackers are mostly hired by companies to test the integrity of their systems.
- Others, operate without company permission by bending but not breaking laws and in the process have created some really cool stuff.

TOP 5 WHITE HAT HACKERS

1. Stephen Wozniak

3. Linus Torvalds



2. Tim Berners-Lee

4. Richard Stallman

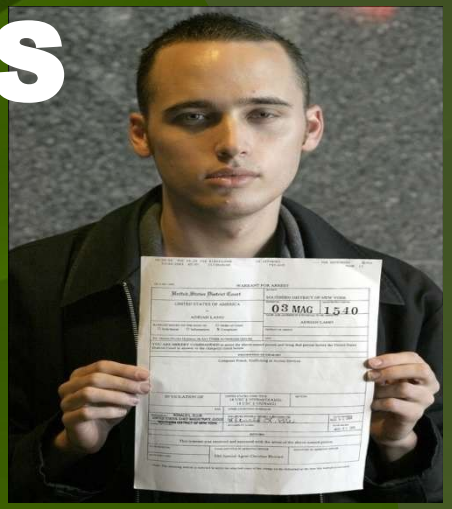
5. Tsutomu Shimomura

BLACK HAT HACKER (Cracker)

- These are hackers who work to exploit computer systems.
- They are the ones you've seen on the news being hauled away for cybercrimes.
- Some of them do it for fun and curiosity, while others are looking for personal gain.

TOP 5 BLACK HAT CRACKERS

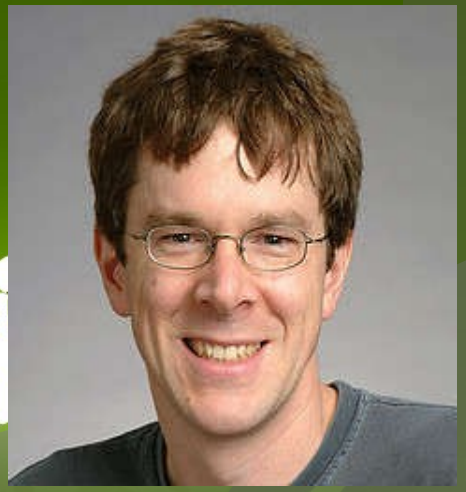
1. Jonathan James



2. Adrian Lamo

3. Kevin Mitnick

4. Kevin Poulsen



5. Robert Tappan Morris

FORMS OF COMPUTER CRIMINALS

- MALICIOUS INSIDERS are the number one security concern for companies.
- INDUSTRIAL SPIES use illegal means to obtain trade secrets from the competitors of firms for which they are hired.
- CYBERCRIMINALS are criminals who hack into computers and steal money.
- CYBERTERRORISTS are people who intimidate or coerce a government to advance their political or social objectives by launching attacks against computers and networks.

LEGAL OVERVIEW

- FRAUD is obtaining title to property through deception or trickery.

- To prove fraud four elements must be shown:
  - ✓ The wrongdoer made a false representation of the material fact.
  - ✓ The wrongdoer intended to deceive the innocent party.
  - ✓ The innocent party justifiably relied on the misrepresentation.
  - ✓ The innocent party was injured.

REDUCING INTERNET VULNERABILITIES

- Risk assessment is an organization's review of the potential threats to its computer and network and the probability of those threats occurring.
- Establish a security policy that defines the security requirements of an organization and describes the controls and sanctions to be used to meet those requirements.
- Educate employees, contractors, and part-time workers in the importance of security so that they will be motivated to understand and follow security policy.

PREVENTION

- Install a corporate firewall.
- Install anti-virus software on personal computers
- Implement safeguards against attacks by malicious insiders.
- Address the ten most critical Internet security threats.
- Verify backup processes for critical software and databases.
- Conduct periodic IT security audits.

DETECTION

- INTRUSION DETECTION SYSTEMS monitor system and network resources and activities and, using information gathered from theses sources, they notify authorities when they identify a possible intrusion.
- HONEYPOT is a computer on your network that contains no data or applications critical to the company but has enough interesting data to lure intruders so that they can be observed in action.

REFERENCES

http://www.docstoc.com

http://www.itsecurity.com/features/top-10-famous-hackers-042407/

http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1517422,00.html

http://www.merriam-webster.com

http://gcn.com/articles/2010/07/27/wifi-hole-puts-networks-at-risk.aspx

http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1517422,00.html

http://en.wikipedia.org/wiki/Crime

www.cert.org/stats

http://en.wikipedia.org/wiki/Computer_virus

http://en.wikipedia.org/wiki/Computer_worm

http://www.ehow.com/facts_6771981_history-trojan-horse-viruses.html