Computer Crime

- Computers and the Internet make many activities easier for us.
- They also make many illegal activities easier for criminals such as

o Distribution of child pornography
o Copyright infringement
o Stock manipulation and
o Other scams

Computer Crime

- Computers and the Web provide a new environment for
  - Fraud
  - Embezzlement
  - Theft
  - Forgery and
  - Industrial espionage

Computer Crime

- Hacking or intentional unauthorized access to computer systems is a whole a new category that includes a wide range of illegal activities

i) From harmless pranks to huge thefts

ii) Shutdown of important services on which lives and livelihoods depend

- Internet initially used for research, collaboration and science but people were shocked when it was invaded by criminals

Computer Crime

- Crimes committed with computers and on the Web are more devastating and harder to detect than similar crimes committed without computers.
- A robber who enters a bank and uses a gun gets USD2500 to USD5000 on average
- The average loss from a computer fraud is more that USD100000

Computer Crime

- A thief who steals a credit card gains access to a much larger amount of money than the thief who stole a wallet in the past with only cash
- A hacker who breaks into an e-commerce Web site might steal not one or a dozen, but hundreds or thousands of credit card numbers
- Terrorists could sabotage power and communications systems and other critical infrastructures

Computer Crime

- Criminals can steal, commit fraud or destroy data from miles away or from another country by modem
- Global business networks and the Web extend the criminal's reach
- Detecting and protecting against the large number of hacking attacks is expensive
- Deciding on punishments appropriate for young hackers is difficult

Computer Crime

- Computers present new challenges for prevention, detection and prosecution of crimes
- We are concerned how computers are used in a variety of crimes and consider some steps taken to reduce the problem

Computer Crime

- Hacking
- Hackers are irresponsible, destructive criminals. They intentionally release computer viruses, steal sensitive personal, business and government information, steal money, crash Web sites, destroy files and disrupt businesses.
- To organize the discussion we describe three phases of hacking:

Computer Crime

- Phase 1: The joy of programming (the early years between 1960s and 1970s, when hacking was a positive term):
- In the early days of computing a hacker was a creative programmer who wrote very elegant or clever programs
- A "good hack" was an especially clever piece of code
- Hackers were called "computer virtuosos"
- They created many of the first computer games, operating systems and many other programs

Computer Crime

- The New Hacker's Dictionary describes a hacker as a person "who enjoys exploring the details of programmable systems and how to stretch their capabilities, one who programs enthusiastically
- Jude Milhon, one of the relatively few women hackers, described hacking as "clever circumvention of imposed limits".

Computer Crime

- The limits can be
- -technical limits of the system one is using
- - limits imposed by someone else's security system
- -legal limits
- -the limits of one's own skills
- Steven Levy captured some of the spirit of the early hackers in his book ***Hackers:***
- *Heroes of the Computer Revolution*, when he said "Art, science and play had merged into the magical activity of programming."

Computer Crime

- Phase 2- The period from the 1970s to the 1990s (when hacking took on its more negative meanings)
- The meaning and especially the connotation s of the word "hacker" changed as more people began using computers and more people began abuse them
- The word "hacking" took on its most common meaning today: breaking into computers on which the hacker does not have authorized access.

Computer Crime

- By the 1980s, hacking also included spreading computer viruses, mostly in software traded on floppy disks
- Hacking behavior includes:
- - pranks
- - Thefts (information, software and sometimes money etc.)
- - manipulating the telephone system
- In 1986, one hacker broke into
- - at least 30-60 computers on the Stanford University campus

Computer Crime

- - Several other universities
- - 15 Silicon Valley Companies
- - Three government laboratories and
- - Several other sites
- It appeared that his goal was simply to get into as many computers as he could

Computer Crime

- In 1980s a German hacker broke into dozens of U.S. Computers, including military systems, looking for information to sell to the Soviet Union (USSR)
- Hackers spoofed email from the premier of Ontario, Canada, sending out unflattering comments about Ontario's parliament
- The secret service reported that a 15-year-old hacked a credit-reporting service and the telephone system in a scheme to get Western Union to wire money to him from other people's account

Computer Crime

- Hackers became a serious threat to security and privacy
- They use programs called "sniffers" to read information traveling over the Internet and extracted passwords
- Adult criminals began to recognize the possibilities of hacking; thus business espionage and significant thefts and frauds joined the list of hacking activities in the 1980s and 1990s

Computer Crime

- A Russian man with accomplices in several countries, used stolen passwords to steal USD 400000 from Citicorp
- Under computer surveillance by authorities, he transferred another $11 million to bank accounts in other countries

Computer Crime

- Phase 3: The Web Era (Beginning in the mid-1990s with the growth of the Web and of e-commerce and the participation of a large portion of the general public online
- In the era of the Web, hacking includes ***all the above*** discussed in Phase 2 plus a variety of new threats

Computer Crime

- Beginning in the mid-1990s:
  - the intricate interconnectedness of the web
  - the increased use of the Internet for e-mail and
  - other communications
- sensitive information and
- economic transactions

Computer Crime

- made hacking more dangerous and damaging and more attractive to criminals gangs and military organizations.
- Hacking now affects almost everyone
- Risk is increased with hacking for basic infrastructure systems in addition to telephone system such as:

o water and power
o hospitals
o transportation
o emergency services

Computer Crime

- Some examples ranging from new pranks to serious disruptions
  - When businesses and government agencies began to set up Web sites:
- Internet security expert ***Dan Farmer*** ran a program to probe 1700 sites of banks, newspapers, government agencies and pornography sellers for software loopholes that made it easy for hackers to invade and disable or damage the sites

Computer Crime

- Dan Farmer found out of 1700 sites,
- about two-thirds of the sites such security weakness and
- only four sites apparently noticed that someone was probing their security
- By mid-2001, ***attrition.ogr***'s online archive had copies of more than 15000 defaced Web pages
- In the USA, hackers modified or defaced the Web pages of the:
  - White House
  - the Bureau of Labor Statistics and
  - the FBI

Computer Crime

- Some examples ranging from new pranks to serious disruptions
  - When businesses and government agencies began to set up Web sites:
- Internet security expert ***Dan Farmer*** ran a program to probe 1700 sites of banks, newspapers, government agencies and pornography sellers for software loopholes that made it easy for hackers to invade and disable or damage the sites

Computer Crime

- Hackers revised the Department of Justice page to read "Department of Injustice" in protest of the Communications Decency Act.
- Hackers changed the CIA's site to read "Central Stupidity Agency" and adds links to inappropriate sites
- A member of the **Global Hell** hacker group hacked the U.S. Army's Web sites and tried to make it look like the work of the Chinese government.

Computer Crime

- When FBI investigated, questioned and searched the homes of members of Global Hell in 1999, hackers responded by defacing numerous government Web sites and taunting the FBI
- Hackers obtain information that can threaten other people's financial assets or privacy
- According to the FBI report, hackers group in Russia and Ukraine broke into more than 40 online businesses and stole more than a million credit-card numbers.

Computer Crime

- In some cases they demanded extortion payments for example from ***CDUniverse*** and ***Creditcards.com***
- When Creditcards.com refused to pay for 55000 stolen card numbers, hackers posted the numbers on Web sites in three countries
- Some hackers who steal credit-card numbers are members of organized-crime group
- Others sell the numbers to organized-crime groups
- In several hacking incidents, medical records were copied

Computer Crime

- A teenager crippled a compute system that handled communications between the airport tower and incoming planes at a small airport.
- He obtained confidential patient information from a drugstore database and shut down telephone services to several hundred homes
- **Hackers in England** impersonated air-traffic controllers and gave false instructions to pilots

Computer Crime

- In 1998, **the U.S. Deputy Defense Secretary** described a series of attacks on numerous U.S. military computers
- Two boys, aged 16 and 17, were hacked computers at top **universities, national laboratories** and two sites in **Mexico**. The were caught and pleaded guilty
- The **Melissa virus** of 1999 mailed copies of itself to the first 50 people in a computer's e-mail address book on system using popular Microsoft software.

Computer Crime

- Each new copy sent 50 more copies and the virus quickly infected approximately a million computers worldwide including those individuals, government and military agencies and hundreds of businesses.
- In 2000, the **"Love Bug" or "ILOVEYOU"** virus, spread around the world in a few hours.
- It destroyed **digital image** and **music files**, **modified the computer's operating system** and **Internet browser** and collected **passwords**

Computer Crime

- The virus infected major corporations like **Ford and Siemens** and **80% of U.S. federal agencies** including the State Department, the Pentagon and NASA along with member of British Parliament and the U.S. Congress
- Many businesses and government agencies had to shut down their e-mail servers.
- The **virus hit tens of millions of computers** worldwide and did an **estimated USD 10 billion damage**.

Computer Crime

- In 2000, within about a week, almost **a dozen major Web sites** were shut down for several hours by ***denial-of-service attacks***
- Yahoo!, eBay, Amazon, E*Trade, Buy.com, CNN and many others were victims
- In this kind of attacks, hackers overload the target site with hundreds of thousands of request for Web pages and other information

Computer Crime

- The request were generated by programs planted on numerous other systems to disguise their origin; thus it is also called ***distributed denial-of-service attack***
- Denial-of -service attacks against individual Web sites are frequently. They are difficult to avoid.