Types of Threats [4]

One way to analyze harm is to consider the cause or source. We call a potential cause of harm a threat. Harm can be caused by either nonhuman events or humans. Examples of nonhuman threats include natural disasters like fires or floods; loss of electrical power; failure of a component such as a communications cable, processor chip, or disk drive; or attack by a wild boar. Figure 7 illustrated some of threats kinds.

Human threats can be either benign (nonmalicious) or malicious. **Nonmalicious** kinds of harm include someone accidentally spilling a soft drink on a laptop, unintentionally deleting text, inadvertently sending an email message to the wrong person, and carelessly typing 12” instead of “21” when entering a phone number or clicking “yes” instead of “no” to overwrite a file. These inadvertent, human errors happen to most people; we just hope that the seriousness of harm is not too great, or if it is, that we will not repeat the mistake.

Most computer security activity relates to **malicious**, **human-caused harm**: A malicious person actually wants to cause harm, and so we often use the term *attack* for a malicious computer security event. Malicious attacks can be random or directed. In a **random attack** the attacker wants to harm any computer or user; such an attack is analogous to accosting the next pedestrian who walks down the street. An example of a random attack is malicious code posted on a website that could be visited by anybody.

In a **directed attack**, the attacker intends harm to specific computers, perhaps at one organization (think of attacks against a political organization) or belonging to a specific individual (think of trying to drain a specific person’ s bank account, for example, by impersonation). Another class of directed attack is against a particular product, such as any computer running a particular browser. The range of possible directed attacks is practically unlimited.

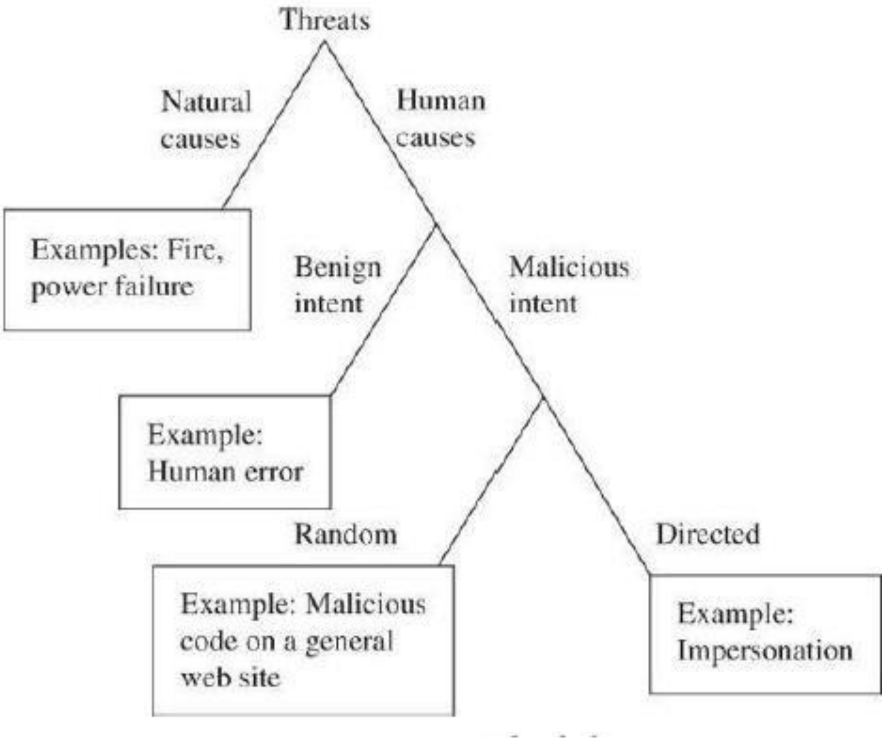

Figure 7: Kinds of Threats

Types of Attackers [4]

Who are attackers? Putting aside attacks from natural and benign causes, we can explore who the attackers are and what motivates them. Most studies of attackers actually analyze computer criminals, that is, people who have actually been convicted of a crime, primarily because that group is easy to identify and study. Some computer criminals are mean types. But many more wear business suits, have university degrees, and appear to be pillars of their communities. Some are high school or university students. Others are middle-aged business executives. Some are mentally deranged, overtly hostile, or extremely committed to a cause, and they attack computers as a symbol. Others are ordinary people tempted by personal profit, revenge, challenge, advancement, or job security—like perpetrators of any crime, using a computer or not. As shown in Figure 8, attackers look just like anybody in a crowd.

99

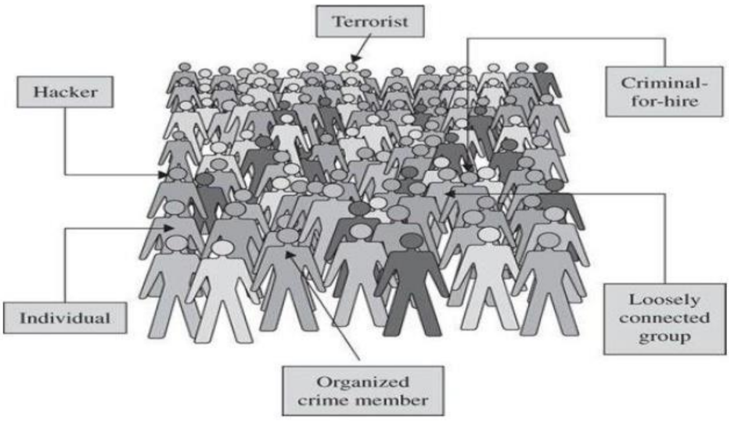

Figure 8: Attackers.

❖ Individuals

Originally, computer attackers were individuals, acting with motives of fun, challenge, or revenge. Early attackers acted alone. Two of the most well known among them are Robert Morris Jr., the Cornell University graduate student who brought down the Internet in 1988, and Kevin Mitnick, the man who broke into and stole data from dozens of computers, including the San Diego Supercomputer Center.

❖ Organized, Worldwide Groups

More recent attacks have involved groups of people. For instance, in October 2004, U.S. and Canadian authorities arrested 28 people from 6 countries involved in an international, organized cybercrime ring to buy and sell credit card information and identities.

❖ Organized Crime

Attackers goals include fraud, extortion, money laundering, and drug trafficking, areas in which organized crime has a well-established presence. Evidence is growing that organized crime groups are engaging in computer crime. In fact, traditional criminals are recruiting hackers to join the lucrative world of cybercrime. For example, Albert Gonzales was sentenced in March 2010 to 20 years in prison for working with a crime ring to steal 40 million credit card numbers from retailer TJMaxx and others, costing over $200 million (Reuters, 26 March 2010).

"Organized crime groups are discovering that computer crime can be lucrative."

❖ Terrorists

The link between computer security and terrorism is quite evident. We see terrorists using computers in four ways:

- Computer as target of attack: Denial-of-service attacks and website defacements are popular activities for any political organization because they attract attention to the cause and bring undesired negative attention to the object of the attack. An example is the massive denial-of-service attack launched against the country of Estonia.

- Computer as method of attack: Launching offensive attacks requires the use of computers. Stuxnet, an example of malicious computer code called a worm, is known to attack automated control systems, specifically a model of control system manufactured by Siemens. Experts say the code is designed to disable machinery used in the control of nuclear reactors in Iran. The persons behind the attack are unknown, but the infection is believed to have spread through USB flash drives brought in by engineers maintaining the computer controllers
- Computer as enabler of attack: Websites, web logs, and email lists are effective, fast, and inexpensive ways to allow many people to coordinate. According to the Council on Foreign Relations, the terrorists responsible for the November 2008 attack that killed over 200 people in Mumbai used GPS systems to guide their boats, Blackberries for their communication, and Google Earth to plot their routes.
- Computer as enhancer of attack: The Internet has proved to be an invaluable means for terrorists to spread propaganda and recruit agents. In October 2009 the FBI arrested Colleen LaRose, also known as JihadJane, after she had spent months using email, YouTube, MySpace, and electronic message boards to recruit radicals in Europe and South Asia to "wage violent jihad", according to a federal indictment.

The Relationship of Vulnerability-Threat-Control Paradigm

The goal of computer security is protecting valuable assets. To study different ways of protection, we use a framework that describes how assets may be harmed and how to counter or mitigate that harm.

A **vulnerability** is a weakness in the system, for example, in procedures, design, or implementation, that might be exploited to cause loss or harm. For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

***A vulnerability is a weakness that could be exploited to cause harm*.**

A **threat** to a computing system is a set of circumstances that has the potential to cause loss or harm. To see the difference between a threat and a vulnerability, consider the illustration in Figure 9. Here, a wall is holding water back. The water to the left of the wall is a threat to the man on the right of the wall: The water could rise, overflowing onto the man, or it could stay beneath the height of the wall, causing the wall to collapse. So the threat of harm is the potential for the man to get wet, get hurt, or be drowned. For now, the wall is intact, so the threat to the man is unrealized.

A threat is a set of *circumstances* that could cause harm.

However, we can see a small crack in the wall─a vulnerability that threatens the man's security. If the water rises to or beyond the level of the crack, it will exploit the vulnerability and harm the man.

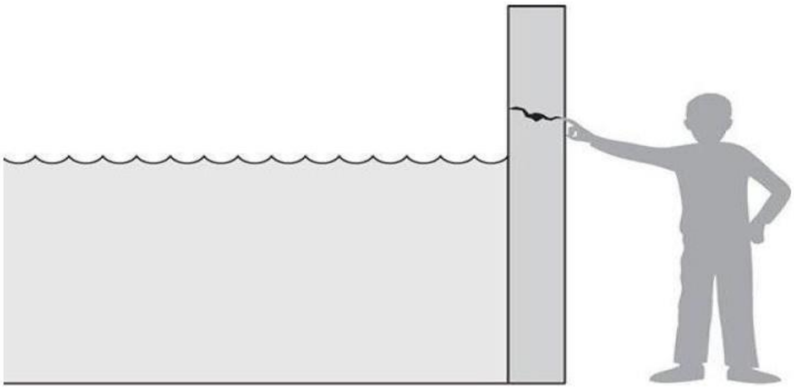

Figure 9: Threat and Vulnerability

How do we address these problems? We use a **control** or **countermeasure** as protection That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability. In Figure 9, the man is placing his finger in the hole, controlling the threat of water leaks until he finds a more permanent solution to the problem. In general, we can describe the relationship between threats, controls, and vulnerabilities in this way:

Controls prevent threats from exercising vulnerabilities.

***A threat is blocked by control of a vulnerability*.**

Identifying Types of Threats [1]

Most attacks can be categorized as one of six broad classes:

■ **Malware:** This is a generic term for software that has a malicious purpose. It includes virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to your system.

■ **Security breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server…all the things you probably associate with the term *hacking*.

■ **Denial of service (DoS) attacks:** These are designed to prevent legitimate access to your system.

■ **Web attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.

■ **Session hijacking:** These attacks are rather advanced, and involve an attacker attempting to take over a session.

■ **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.

■ Malware (Malicious Code) [1]

Malware is a generic term for software that has a malicious purpose. This section discusses three types of malware: viruses, Trojan horses and spyware. Trojan horses and viruses are the most widely encountered.

Malicious code or malware (short for MALicious softWARE) is the general name for programs or program parts planted by an agent with malicious intent to cause unanticipated or undesired effects.

According to Symantec (makers of Norton antivirus and other software products):

a virus is —a small program that replicates and hides itself inside other programs, usually without your knowledge. A computer virus is similar to a biological virus; both are designed to replicate and spread. The most common method for spreading a virus is using the victim’s email account to spread the virus to everyone in their address book. Some viruses don’t actually harm the system itself, but all of them cause network slowdowns due to the heavy network traffic caused by the virus replication.

A virus can be either transient or resident. A transient virus has a life span that depends on the life of its host; the virus runs when the program to which it is attached executes, and it terminates when the attached program ends. (During its execution, the transient virus may spread its infection to other programs.) A resident virus locates itself in memory; it can then remain active or be activated as a stand-alone program, even after its attached program ends.

A worm is a program that spreads copies of itself through a network. (John Shoch and Jon Hupp are apparently the first to describe a worm, which, interestingly, was created for nonmalicious purposes. Researchers at the Xerox Palo Alto Research Center, Shoch and Hupp wrote the first program as an experiment in distributed computing.) The primary difference between a worm and a virus is that a worm operates through networks, and a virus can spread through any medium (but usually uses a copied program or data files). Additionally, the worm spreads copies of itself as a stand-alone program, whereas the virus spreads copies of itself as a program that attaches to or embeds in other programs.

The Trojan horse gets its name from an ancient tale. An electronic Trojan horse works the same way, appearing to be benign software but secretly downloading a virus or some other type of malware onto your computer from within. As an example of a computer Trojan horse, consider a login script that solicits a user's identification and password, passes the identification information on to the rest of the system for login processing, but also retains a copy of the information for later, malicious use. In this example, the user sees only the login occurring as expected, so there is no reason to suspect that any other, unwelcome action took place.

Another category of malware currently on the rise is **spyware**. Spyware is simply software that literally spies on what you do on your computer. Spyware can be as simple as a cookie—a text file that your browser creates and stores on your hard drive—that a website you have visited downloads to your machine and uses to recognize you when you return to the site. However, that flat file can then be read by the website or by other websites. Any data that the file saves can be retrieved by any website, so your entire Internet browsing history can be tracked.

A logic bomb is software that lays dormant until some specific condition is met. That condition is usually a date and time. When the condition is met, then the software does some malicious act such as deleting files, altering system configuration, or perhaps releasing a virus.

Another form of spyware, called a key logger, records all of your keystrokes. Some key loggers also take periodic screenshots of your computer. Data is then either stored for later retrieval by the person who installed the key logger or is sent immediately back via email.

■ Compromising System Security (Security breaches) [1]

Next we will look at attacks that breach your system's security. This activity is what is commonly referred to as ***hacking***, though that is not the term hackers themselves use. However, it should be noted at this point that *cracking* is the appropriate word for intruding into a system without permission, usually with malevolent intent. Any attack that is designed to breach your security, either via some operating system flaw or any other means, can be classified as cracking.

Social engineering is a technique for breaching a system's security by exploiting human nature rather than technology. This was the path that the famous hacker Kevin Mitnick most often used. Social engineering uses standard con techniques to get users to give up the information needed to gain access to a target system. The way this method works is rather simple:

The perpetrator gets preliminary information about a target organization and leverages it to obtain additional information from the system's users.

Following is an example of social engineering in action. Armed with the name of a system administrator, you might call someone in the business's accounting

department and claim to be one of the company's technical support personnel. Mentioning the system administrator's name would help validate that claim, allowing you to ask questions in an attempt to ascertain more details about the system's specifications. A savvy intruder might even get the accounting person to say a username and password. As you can see, this method is based on how well the prospective intruder can manipulate people and actually has little to do with computer skills.

The growing popularity of wireless networks gave rise to new kinds of attacks. One such activity is *wardriving*. This type of attack is an offshoot of war-dialing. With war-dialing, a hacker set up a computer to call phone numbers in sequence until another computer answered to try to gain entry to its system. War-driving is much the same concept, applied to locating vulnerable wireless networks. In this scenario, the hacker simply drives around trying to locate wireless networks. Many people forget that their wireless network signal often extends as much as 100 feet. At the 2004 DefCon convention for hackers, there was a war-driving contest where contestants drove around the city trying to locate as many vulnerable wireless networks as they could.

- **Denial of Service Attacks**

In a *denial of service (DoS)*, the attacker does not actually access the system. Rather, he or she simply blocks access from legitimate users. One common way to do prevent legitimate service is to flood the targeted system with so many false connection requests, that the system cannot respond to legitimate requests. DoS is robably the most common attack on the Web.

- **Web Attacks**

By their nature, web servers have to allow communications. Oftentimes, websites allow users to interact with the website. Any part of a website that allows for user interaction is also a potential point for attempting a web-based attack. SQL injections involve entering SQL (Structured Query Language) commands into login forms (username and password text fields) in an attempt to trick the server into executing those commands. The most common purpose is to force the server to log the attacker on, even though the attacker does not have a legitimate username and password. While SQL injection is just one type of web attack, it is the most common.

- **DNS Poisoning**

Most of your communication on the Internet will involve DNS, or Domain Name Service. DNS is what translates the domain names you and I understand (like www.ChuckEasttom.com) into IP addresses that computers and routers understand. DNS poisoning uses one of several techniques to compromise that process and redirect traffic to an illicit site, often for the purpose of stealing personal information.