Computer Security

First Semester

Why is computer Security?

It is difficult to find an aspect of modern life that does not involve a computer system, at least on some level. Online purchases, debit cards, and automatic bill pay are standard parts of modern life. It is even likely that you have taken a class online, this is because vastly of our business is done online, a great deal of personal information is stored in computers. Medical records, tax records, school records, and more are all stored in computer databases.

This leads to some very important questions:

1. How is information safeguarded?
2. What are the vulnerabilities to these systems?
3. What steps are taken to ensure that these systems and data are safe?. [1]

Before the topic of information security is explored, it is important first to understand the impact computers have on our daily lives and what information computers store that is personally important to us. As we all know, computers are everywhere and are responsible for making virtually every aspect of our lives better. Computers control everything from how you receive electricity, water, and other utilities to services ranging from air traffic control to online banking and everything in between. The main focus of this book is on the user and what typical users can do to protect themselves, the focus is not on the impact of computers in general but rather on the computers and information that you have control over and how you can protect your information from the many threats lurking on the Internet. [2]

One way to view how people rely on computers is to examine how the average person perceives the privacy of information stored on computers. People often use two different standards of privacy, one for computer data and one for noncomputer data. While most people would never walk up to a stranger on the street and hand the stranger their business card containing a wealth of their personal information (noncomputer data), people seem more than willing to disclose such information when it is in its digital form (computer data) on the Internet. Two questions you should always ask yourself when disclosing digital information in the Cyber world are, Would I give this information to someone I do not know in the real world? and What will this person do with my personal information? The answer to these questions should help guide you in classifying information as private or nonprivate.

When considering private information stored on computers, there are two different classifications of computers: personal and non personal. The owner of a ―personal computer owns both the computer hardware and the information stored on that hardware, as exemplified by the typical home computer situation. A ―nonpersonal computer is one that is owned by a third party but contains information that relates to a person. A bank computer, for example, may be bank property, but it contains personal information about both you and the bank's other clients. As will be discussed, the personal or nonpersonal categorization of a computer does not change with respect to whether the information stored or processed is private or not, but it does change how we, as individuals,

handle information privacy and possibly what information we choose to store on such computers.

Computers are often regarded as powerful tools that can help people manage their daily lives; for this reason, many own personal computers. It is estimated that 90% of individuals in the United States own a computing device, and that worldwide personal computer sales exceeded more than 364 million units in 2011. People use computers to access the Internet, to keep in touch with other people, to retain information about their lives and more. While a great deal of the information stored on your personal computer is nonprivate, there is usually some information that would be considered private. Stop and think about the information stored on your computer to which you would answer "no" to the question posed previously: Would I give this information to someone I do not know? Such information is private and therefore should be protected. Since private information is stored on a computer owned by you (a personal computer), it is your responsibility to protect that information.

Nonpersonal computers, on the other hand, are not owned by individuals but instead by third-party entities that store private information on behalf of their clients or users. Overall, there exists an enormous volume of private information stored on commercial, government, or third-party nonpersonal computers, and these entities handle the safeguarding of the information stored on these systems. While a typical user has little or no control over many aspects of the security of the information stored on nonpersonal computers, in certain cases the user has control over what information is stored and, just as important, how that information can be accessed (i.e., passwords). For example, a client of an e-commerce website freely chooses to disclose his or her name, address, and credit card number in exchange for the convenience of buying an item online. While the client cannot directly control the security of the system that processes and stores this private information, the client does have the ability to choose which e-commerce website he or she prefers to shop at or whether to shop online at all. Furthermore, if the client chooses to create an account on an e-commerce website for future use, the security of the password chosen is also a factor controlled by the client that can contribute to the overall security of the client's information.

What is security?

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Introduction to Computer Architecture and Security

Computer architecture is to study how to design computer systems. It includes all components: the central processing unit (CPU), computer memory and storage, input and output devices (I/O), and network components. A Computer is composed of a number of different components:

- **Hardware:** Computer hardware processes information by executing instructions, storing data, moving data among input and output devices, and transmitting and receiving information to and from remote network locations.
- **Software:** Software consists of system software and application software or programs. Operating Systems such as Windows, UNIX/Linux are system software. Word, Firefox browser and iTunes are examples of application software.
- **Network:** The network communication component is responsible for sending and receiving information and data through local area network or wireless connections.
- **Data:** is the fundamental representation of information and facts but usually formatted in a special way. All software is divided into two categories: data and programs. Programs are a collection of instructions for manipulating data.

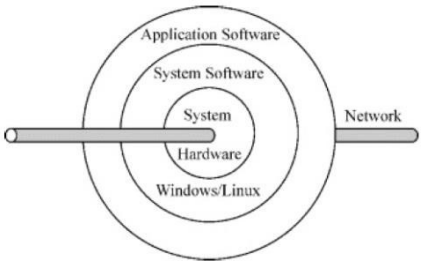

Figure 1:A conceptual diagram of a common computer system

Figure 1 shows a view of a computer system from a user perspective. Here a computer system no longer looks like an onion as traditional textbooks used to represent. Instead, a network component (including hardware and software) is added as a highway for data flowing in and out of the computer system.

Since the invention of the Internet, computer systems are no longer standalone machines. The traditional "computing" concept of the single machine model is fading away. For most users, information exchange has taken an important role in everyday computer uses.

Despite the numerous efforts to prevent attacks, the threat to computer systems is far from over. Computer compromises and data bleach are still very common. If you look back to those counter-attack techniques, most of the detection systems are based on passive techniques. They only work after attacks have taken place.
In medicine, people spent billions of dollars to develop new drugs to cure illness. However ancient Chinese people study how to eat well and exercise well to prevent illness. This is the same as now the so-called prevention medicine. If we apply the same mechanism to computer systems, we draw the conclusion that we not only need to build firewalls, more importantly we need to develop computer systems that are immune from attacks.
In early 2005, a US patent was filed to propose new technology that can prevent hackers from getting information stored in computer systems. The technology has drawn the attention of industry, academia, as well as government.

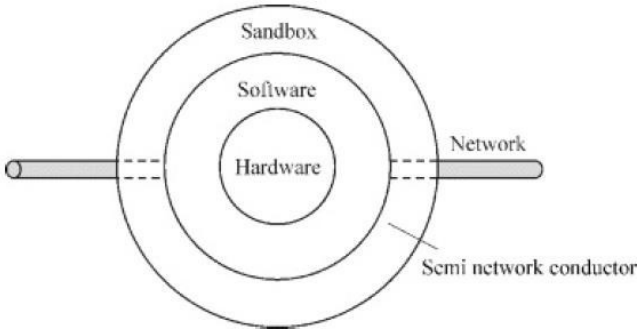

Figure 2:A conceptual diagram of a secured computer system

Figure 2 shows a conceptual diagram of the proposed secured computer system. Note that in addition to the traditional hardware and software, the system added an additional layer. It is like a sandbox that “separates” the computer system from the outside world. We could call it a "virtual semi-conductor" or "semi network conductor". It allows the computer operator to control information and data access so that hackers are no longer able to steal data from the computer system.

Security Truisms

Information security is a large and complex subject. However, there are many overarching statements --security truisms-- that can be made about information security. These security truisms apply to both personal and nonpersonal computers and should be used as guiding principles when considering information security.

1. **Security Is a Matter of Economics:** When deciding what information to protect and how to protect it, the first question that should be asked is, Is it worth it? In other words, security costs time and money, and if the information or object that is being protected has little value, it does not make much sense to spend resources to protect it. A difficult task in this type of assessment is determining the value of what you are trying to protect on your computer.

2. **Security Should Be Composed of Layers of Defenses:** There is no one single security mechanism that can protect all information from potential attacks. A layered approach will make it more difficult for someone to gain access to your information since an intruder must bypass multiple security methods to gain access. For example, a deadbolt lock can be used to safeguard a home. In addition, a motion detection alarm system can be used to detect whether the lock did its job or whether the intruder circumvented the lock by breaking in through a window. You might also take your most valuable items and place them in a safe within the locked and alarm-equipped house. If one layer fails, there are additional layers in place to compensate and prevent a breach of security.
3. **Absolute Security Does Not Exist:** We cannot protect against every possible event, especially when we cannot predict every potential security threat. No security system can be perfect in dealing with either the physical or the computer world. From the perspective of a practical computer user, no matter how much time and effort one places in protecting a computer, it will always be vulnerable to a certain number of attacks. Therefore, the objective of practical computer security is to raise the bar high enough to greatly reduce the number of threats able to mount a successful attack.
4. **Security Is at Odds with Convenience:** In the physical world, security often involves extra steps or procedures to protect a valued object. For example, houses are often protected with a locked door, and a key is then needed to gain access to the house. Information security is similar; passwords are used to gain access to information, requiring the user to remember and use the password every time the desired information is accessed. The more security mechanisms added to a computer system, the more intrusive security measures might be, often causing user frustration. This frustration may cause individuals to take shortcuts, like leaving a door unlocked or using a simple and easy-to-remember password that weakens the security safeguard. While added measures provide enhanced security, they are also at odds with convenience and over time convenience tends to trump security. [2]

Basic Security Terminology

Security professionals use a number of terms to describe various aspects of information security. This section provides definitions for several such commonly used terms. The first three terms dealing with the protection of information are represented the security goals (as shown in Figure 3). Together they are called the CIA model. [2]

- **Confidentiality:** Preventing unauthorized users from reading or accessing information. The purpose of the confidentiality principle is to keep information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions. A loss of confidentiality would include an attacker learning your password or credit card number.

- **Integrity:** Ensuring that an unauthorized user has not altered information (additions, deletions, alterations, etc. to data.). The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously. A bank account balance is a sound example of information that requires a high degree of integrity. A loss of integrity in this case would be detrimental to the bank or its customers.
- **Availability:** Making sure that information can be accessed when needed by authorized users. If a hard drive were erased as a result of a malware infection, this type of action would be considered a loss of availability.

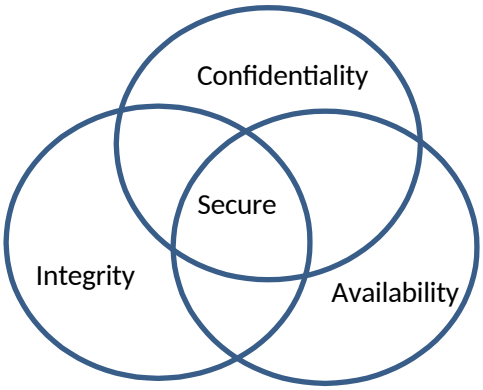

Figure 3:Security goals

The next five terms are used to describe methods attackers may use to gain access to your information or to your computer system.

- **Vulnerability:** A weakness in some aspect of a computer system that can be used to compromise a system during an attack. Vulnerabilities can exist in the *design*, the *implementation*, or the *configuration* of computers and software.

  Design vulnerabilities occur when flaws in the design of the computer or software can be used to bypass security. As illustrated in Figure 4, a physical example would be if a house plan used by a developer does not specify locks on any of the outside doors. If a thief discovered such a flaw, the thief would then be able to break into any of the houses sold by that developer (i.e., houses denoted with yellow x's).

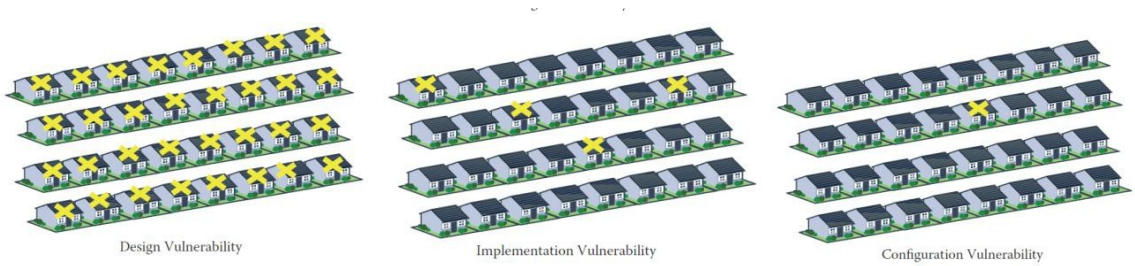

Figure 4:Vulnerability types

Implementation vulnerabilities exist when developers make errors implementing software designs. Continuing with the previous physical example in Figure 4, while the developer's plans contained designs for every house to be equipped with door locks, the locks were installed either improperly or not at all by contractors. In such a case, instead of all homes using the same plans that were vulnerable to break-ins, only those homes built by a certain contractor would be vulnerable. Implementation vulnerabilities in software can be difficult to find, but once discovered, they are often easy to fix with a software patch.

Configuration vulnerabilities occur when a user either configures the system incorrectly or uses system defaults. Continuing with the door lock example in Figure 3, this would be the case when design plans were correct and locks were installed correctly, but the homeowner fails to lock the door. The most common computer system configuration vulnerabilities occur when the user fails to change a default password, chooses a weak password, or elects not to use a password at all.

Vulnerabilities can take many forms, and some typical examples are listed here, along with the ways in which they could be exploited. It may be noted that these points reinforce the earlier observation that computer security relates to more than just the protection of the computer itself.

1. Environment and infrastructure vulnerabilities:
   - Lack of physical protection of the building, doors, and windows (could be exploited by theft);
   - Inadequate access control to rooms (could be exploited by unauthorized access);
   - Unstable power grid (could result in power failure).
2. Hardware vulnerabilities:
   - Susceptibility to temperature variation (could be caused by overheating);
   - Insufficient maintenance of storage media (could result in media failure);
   - Lack of efficient configuration change control (could be exploited by operational staff).
3. Software vulnerabilities
   - Complicated user interface (could result in user error);
   - Lack of authentication.
   - Lack of audit trail (could be exploited by unauthorized software use).
4. Communications vulnerabilities:
   - Unprotected communication lines.
   - Unprotected sensitive traffic.
   - Unprotected public network connections (could be exploited by unauthorized users).
5. Personnel vulnerabilities:
   - Unsupervised work by outside staff (could be exploited by theft);
   - Insufficient security training (could result in user error);

• Lack of monitoring mechanisms (could be exploited by use of systems in an unauthorized way);
• All of the things that could potentially exploit the vulnerabilities are regarded as threats to the system.

It should be noted that while software vulnerabilities are usually the most commonly encountered form, they are also often the easiest to fix. In most cases, vulnerabilities are fixed by the simple installation of a patch from the operating system (or application) vendor. However, this task is made increasingly difficult when organizations operate a range of operating systems and vendor applications. The United States Computer Emergency Response Team Coordination Center (CERT/CC) monitors vulnerabilities reported worldwide and produces annual reports. Figure 5 clearly shows the scale of the problem indicating a substantial increase over the period 2000–2007 (Note: the figure shown for 2007 is an estimate based on the results available from the first quarter of 2007).

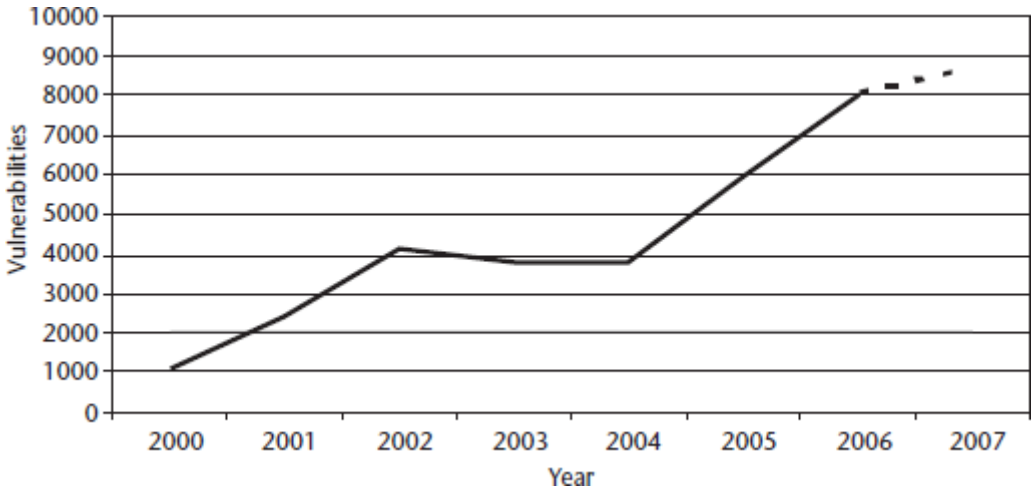

Figure 5: CERT/CC vulnerability statistics from 2000–2007.

- **Exploit:** An exploit is an unimplemented method or algorithm that is able to take advantage of a vulnerability in a computer system. Using the door lock example, an exploit might consist of knowing that if you made a bump key—a key with no notches—it will open certain locks, but you do not possess or know how to make the key. Therefore, an exploit is a potential threat underlying a potential attack.
- **Attack Code:** An attack code is a program or other implementation of an exploit used to attack a vulnerability in a computer system. An attack code would be analogous to creating a bump key that would be able to open vulnerable locks.

- **Attack**: The actual use of attack code against a system or the exploitation of a vulnerability. This is the same as using a bump key to open a vulnerable door.

  Figure 6 shows the chronological relationship among vulnerabilities, exploits, attack code, and attacks. Vulnerabilities often lay dormant in software programs for years before being discovered. Even when they are discovered, there may not be an easy way to exploit them. The time interval between when a vulnerability is discovered and an exploit is designed can be anything from days to months or even longer. Once the exploit has been identified, there may be a period of time before the attack code is created. Sometimes, the exploit is discovered directly through creation of attack code, and the time between exploit and attack code is thus zero. The time between attack code production and widespread attacks can also vary depending on the attack code type and its distribution method.

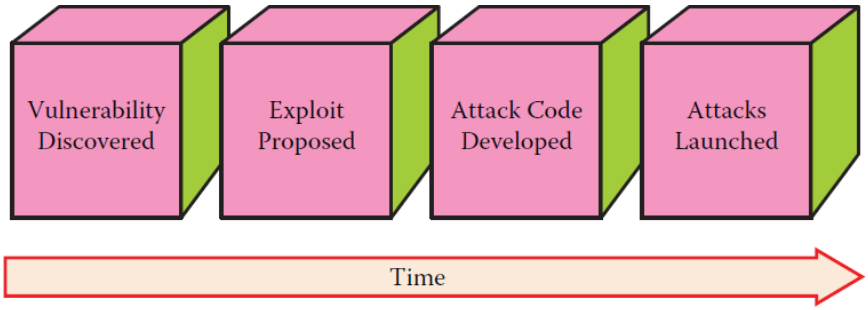

Figure 6: Relationship among vulnerabilities, exploits, and attacks.

- **Zero-Day Exploit:** When attack code is used to target a system before the vulnerability or exploit is discovered or known to exist by the security community (i.e., defenders or good guys), this action is known as a "zero-day" exploit. Zero-day exploits are particularly dangerous because security practitioners are often initially defenseless against such attacks.

The next four terms deal with quantifying the likelihood that a computer will be subjected to an attack and the resultant costs of such an attack.

- **Risk:** Risk is a measure of the criticality of a situation—the likelihood of something being attacked. Risk is based on several metrics, as subsequently described. The risk of attack associated with a given situation consists of several factors, commonly described as threats, vulnerabilities (previously discussed), and impact.
- **Threat:** Threat is a measure of likelihood that a computer system will be attacked or the confidentiality of information lost. For example, a web server placed on the public Internet may have a high probability of being attacked, while a web server located on a private corporate network not connected to the Internet would have a significantly lower probability of being attacked. Determining the threat of an attack can be difficult to quantify and is

dependent on many factors. Consider a web server hosted on a private corporate network; the threat is low from an Internet-based attack. However, the threat might be much higher if the attack consists of a company employee determined to steal information from the internal web server to which he or she has access.

- **Impact:** Impact is the measure of potential consequences if the computer system or the confidentiality of information was compromised as the result of a security breach or information leak. Impact is sometimes a hard-to-quantify factor based on the overall consequences of a security breach for a specific organization. Again, consider an attack in which a public web server is compromised. Such a loss might be considered to be low impact since the data hosted on the server is already public. However, if an internal server that contains employee or customer records were compromised, the impact would likely be very high.

In summary, risk is a combination of a system's vulnerability to attack, attack likelihood (threat), and attack impact. The relationship between these factors can be described using three examples.

1. The first example is one in which a system is not vulnerable to a specific attack. Consider the case in which an Internet-connected Macintosh computer (i.e., Mac) running the OS X operating system is being attacked by attack code designed to exploit a vulnerability for the Windows operating system. In this case, because the considered attack code is ineffective against a Mac, the risk for the Mac computer is zero even though the attack may have a high impact if successful, and the threat of attack for the system is high.
2. The second example considers a situation in which the impact of an attack is zero, or at least very small. This example is less likely since there typically is some nonzero impact resulting from a successful attack. Often, the impact level is considered to be either high impact or low impact. A low-impact system would be one containing little important or private information. For example, because the disclosure of information found on a public web server is already public, the impact of such loss of confidentiality would be low. Thus, the overall risk would be low even though the system under consideration possesses a high threat of being attacked and may also be vulnerable to multiple types of attacks.
3. The last example is when the threat is zero. Although highly improbable, this occurs when a system cannot be attacked because of the manner in which it is connected or accessed. It has been said that "the only truly secure computer is one buried in concrete, with the power turned off and the network cable cut". Even if the system possesses many vulnerabilities and contains important information, if it cannot be attacked, then the risk is zero.

- **Risk Assessment:** Risk assessment is a process or procedure in which the importance of a system or data is evaluated and a determination is made regarding how many resources must be devoted to its protection. The idea is

that not all data must be protected at the same security level. Many books and other resources dedicated to risk assessment are available, and there are consulting firms engaged in the lucrative business of performing risk assessment for organizations.

Example:

Sidebar 1-2: Why Universities Are Prime Targets

Universities make very good targets for attack, according to an Associated Press story from June 2001 [HOP01]. Richard Power, editorial director for the Computer Security Institute, has reported that universities often run systems with vulnerabilities and little monitoring or management. Consider that the typical university research or teaching lab is managed by a faculty member who has many other responsibilities or by a student manager who may have had little training. Universities are havens for free exchange of ideas. Thus, their access controls typically are configured to promote sharing and wide access to a population that changes significantly every semester.

A worse problem is that universities are really loose federations of departments and research groups. The administrator for one group's computers may not even know other administrators, let alone share intelligence or tools. Often, computers are bought for a teaching or research project, but there is not funding for ongoing maintenance, either buying upgrades or installing patches. Steve Hare, managing director of the computer security research group at Purdue University, noted that groups are usually strapped for resources.

David Dittrich, a security engineer at the University of Washington, said he is certain that cracker(s) who attacked the eBay and CNN.com web sites in 2000 first practiced on university computers. The large and frequently changing university student body gives the attacker great opportunity to maintain anonymity while developing an attack.