I. Security

Security is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization.

II. Network security

Network security is any activity designed to protect the usability and integrity of your **network** and data. It includes both hardware and software technologies. Effective **network security** manages access to the **network**. It targets a variety of threats and stops them from entering or spreading on your **network**. Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

III. Need of Network Security:-

The network needs security against attackers and hackers. Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers. Here network security not only means security in a single network rather in any network or network of networks. Now our need of network security has broken into two needs. One is the need of information security and other is the need of computer security.
On internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers. The information security is needed for the following given reasons.

1. To protect the secret information users on the net only. No other person should see or access it.
2. To protect the information from unwanted editing, accidently or intentionally by unauthorized users.
3. To protect the information from loss and make it to be delivered to its destination properly.
4. To manage for acknowledgement of message received by any node in order to protect from denial by sender in specific situations. For example let a customer orders to purchase a few shares XYZ to the broader and denies for the order after two days as the rates go down.
5. To restrict a user to send some message to another user with name of a third one. For example a user X for his own interest makes a message containing some favorable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.
6. To protect the message from unwanted delay in the transmission lines/route in order to deliver it to required destination in time, in case of urgency.
7. To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case destination machine fails to capture it because of some internal faults.

IV. Information security

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. The information or data may take any form, e.g. electronic or physical. Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity

V. What are computer intrusions?

Computer intrusions occur when someone tries to gain access to any part of your computer system. Computer intruders or hackers typically use automated computer programs when they try to compromise a computer's security. There are several ways an intruder can try to gain access to your computer. They can:

1. Access your computer to view, change, or delete information on your computer.
2. Crash or slow down your computer.
3. Access your private data by examining the files on your system.
4. Use your computer to access other computers on the Internet.

VI. Characteristics of Computer Intrusions:

Any part of a computer system can be the target of a crime. When we refer to a computing system, that is the collection of hardware, software, storage media, data and people that an organization uses to perform computing task. Sometimes it is assume that parts of the computer system are not valuable to the outsiders, but often it is mistaken. For instance , it is tend to thing

VII. What does "secure" mean? Protecting Valuables:

A computer-based system has three separate but valuable components: **hardware, software, and data.** Each of these assets offers value to different members of the com- munity affected by the system. To analyse security, we can brainstorm about the ways in which the system or its information can experience some kind of loss or harm. For example, we can identify data whose format or contents should be protected in some way. We want our security system to make sure that no data are disclosed to unauthorized parties. Neither do we want the data to be modified in illegitimate ways. At the same time, we must ensure that legitimate users have access to the data. In this way, we can identify weaknesses in the system.

Vulnerabilities, Threats, Attacks, and Controls

Vulnerability is a weakness in the security 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 **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 vulnerability, consider the illustration in Figure 1-1. 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, over- flowing 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.

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.

There are many threats to a computer system, including human-initiated and computer-initiated ones. We have all experienced the results of inadvertent human errors, hardware design flaws, and software failures. But natural disasters are threats, too; they can bring a system down when the computer room is flooded or the data centre collapses from an earthquake, for example.

Attacks

An attack is one of the biggest security threats in information technology, and it comes in different forms. A passive attack is one that does not affect any system, although information is obtained. A good example of this is wiretapping. An active attack has the potential to cause major damage to an individual's or organization's resource because it attempts to alter system resources or affect how they work. A good example of this might be a virus or other type of malware

A human who exploits vulnerability perpetrates an attack on the system. An attack can also be launched by another system, as when one system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function. Unfortunately, we have seen this type of attack frequently, as denial-of- service attacks flood servers with more messages than they can handle.

Controls

A **control** or **countermeasure** is a means to counter threats. Harm occurs when a threat is realized against vulnerability. To protect against harm, then, we can neutralize the threat, close the vulnerability, or both. The possibility for harm to occur is called risk. We can deal with harm in several ways:

- **prevent** it, by blocking the attack or closing the vulnerability
- **deter** it, by making the attack harder but not impossible
- **deflect** it, by making another target more attractive (or this one less so)
- **mitigate** it, by making its impact less severe
- **detect** it, either as it happens or sometime after the fact
- **recover** from its effects

more than one of these controls can be used simultaneously. So, for example, we might try to prevent intrusions—but if we suspect we cannot prevent all of them, we might also install a detection device to warn of an imminent attack. And we should have in place incident-response procedures to help in the recovery in case an intrusion does succeed.

We can group controls into three largely independent classes. The following list shows the classes and several examples of each type of control.

- **Physical controls** stop or block an attack by using something tangible too, such as walls and fences
  – locks
  – (human) guards
  – sprinklers and other fire extinguishers

- **Procedural** or **administrative** controls use a command or agreement that
  – requires or advises people how to act; for example,
  – laws, regulations
  – policies, procedures, guidelines
  – copyrights, patents
  – contracts, agreements
- **Technical controls** counter threats with technology (hardware or software), including
  – passwords
  – program or operating system access controls
  – network protocols
  – firewalls, intrusion detection systems
  – encryption
  – network traffic flow regulators

VIII. Security problem in computing

To devise controls, we must know as much about threats as possible. We can view any threat as being one of four kinds: interception, interruption, modification, and fabrication. Each threat exploits vulnerabilities of the assets in computing systems;

- An **interception** means that some unauthorized party has gained access to an asset. The outside party can be a person, a program, or a computing system. Examples of this type of failure are illicit copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be discovered fairly quickly, a silent interceptor may leave no traces by which the interception can be readily detected.

- In an **interruption**, an asset of the system becomes lost, unavailable, or unusable. An example is malicious destruction of a hardware device, erasure of a program or data file, or malfunction of an operating system file manager so that it cannot find a particular disk file.
- If an unauthorized party not only accesses but tampers with an asset, the threat is a **modification**. For example, someone might change the values in a data- base, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected with simple measures, but other, more subtle, changes may be almost impossible to detect.
- Finally, an unauthorized party might create a **fabrication** of counterfeit objects on a computing system. The intruder may insert spurious transactions to a net- work communication system or add records to an existing database. Sometimes these additions can be detected as forgeries, but if skilfully done, they are virtually indistinguishable from the real thing.

IX. Method–Opportunity–Motive

A malicious attacker must have three things to ensure success: method, opportunity, and motive, depicted in Figure 1. Roughly speaking, method is the how; opportunity, the when; and motive, the why of an attack. Deny the attacker any of those three and the attack will not succeed. Let us examine these properties individually.

FIGURE 1 Method–Opportunity–Motive

Method

By **method** we mean the skills, knowledge, tools, and other things with which to perpetrate the attack. Think of comic figures that want to do something, for example, to steal valuable jewelry, but the characters are so inept that their every move is doomed to fail. These people lack the capability or method to succeed, in part because there are no classes in jewel theft or books on burglary for dummies.

Anyone can find plenty of courses and books about computing, however. Knowledge of specific models of computer systems is widely available in bookstores and on the Internet. Mass-market systems (such as the Microsoft or Apple or Unix operating systems) are readily available for purchase, as are common software products, such as word processors or database management systems, so potential attackers can even get hardware and software on which to experiment and perfect an attack. Some manufacturers release detailed specifications on how the system was designed or how it operates, as guides for users and integrators who want to implement other complementary products. Various attack tools—scripts, model programs, and tools to test for weaknesses—are available from hackers' sites on the Internet, to the degree that many attacks require only the attacker's ability to download and run a program. The term **script kiddie** describes someone who downloads a complete attack code package and needs only to enter a few details to identify the target and let the script perform the attack. Often, only time and inclination limit an attacker.

Opportunity

Opportunity is the time and access to execute an attack. You hear that a fabulous apartment has just become available, so you rush to the rental agent, only to find someone else rented it five minutes earlier. You missed your opportunity.

Many computer systems present ample opportunity for attack. Systems available to the public are, by definition, accessible; often their owners take special care to make them fully available so that if one hardware component fails, the owner has spares instantly ready to be pressed into service. Other people are oblivious to the need to protect their computers, so unattended laptops and unsecured network connections give ample opportunity for attack. Some systems have private or undocumented entry points for administration or maintenance, but attackers can also find and use those entry points to attack the systems.

Motive

Finally, an attacker must have a **motive** or reason to want to attack. You probably have ample opportunity and ability to throw a rock through your neighbor's window, but you do not. Why not? Because you have no reason to want to harm your neighbor: You lack motive.

We have already described some of the motives for computer crime: money, fame, self-esteem, politics, and terror. It is often difficult to determine motive for an attack. Some places are "attractive targets," meaning they are very appealing to attackers. Popular targets include law enforcement and defense department computers, perhaps because they are presumed to be well protected against attack (so they present a challenge and a successful attack shows the attacker's prowess). Other systems are attacked because they are easy to attack. And some systems are attacked at random simply because they are there.

X. Security Goals

We use the term "security" in many ways in our daily lives. A "security system" protects our house, warning the neighbours or the police if an unauthorized intruder tries to get in. "Financial security" involves a set of investments that are adequately funded; we hope the investments will grow in value over time so that we have enough money to survive later in life. And we speak of children's "physical security," hoping they are safe from potential harm. Just as each of these term has a very specific meaning in the context of its use, so too does the phrase "computer security."

When we talk about computer security, we mean that we are addressing three important aspects of any computer-related system: confidentiality, integrity, and availability.

Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. By "access," we mean not only reading but also viewing, printing, or simply knowing that a particular asset exists. Confidentiality is sometimes called secrecy or privacy.

Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.

Availability means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects, that access should not be prevented. For this reason, avail- ability is sometimes known by its opposite, denial of service.

Security in computing addresses these three goals. One of the challenges in building a secure system is finding the right balance among the goals, which often conflict. For example, it is easy to preserve a particular object's confidentiality in a secure system simply by preventing everyone from reading that object. However, this system is not secure, because it does not meet the requirement of availability for proper access. That is, there must be a balance between confidentiality and availability.

XI. Computer Criminals

In television and film westerns, the bad guys always wore shabby clothes, looked mean and sinister, and lived in gangs somewhere out of town. By contrast, the sheriff dressed well, stood proud and tall, was known and respected by everyone in town, and struck fear in the hearts of most criminals.

To be sure, some computer criminals are mean and sinister 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. No single profile captures the characteristics of a "typical" computer criminal, and many who fit the profile are not criminals at all.

Whatever their characteristics and motivations, computer criminals have access to enormous amounts of hardware, software, and data; they have the potential to cripple much of effective business and government throughout the world. In a sense, then, the purpose of computer security is to prevent these criminals from doing damage.

For the purposes of studying computer security, we say **computer crime** is any crime involving a computer or aided by the use of one. Although this definition is admittedly broad, it allows us to consider ways to protect ourselves, our businesses, and our communities against those who use computers maliciously.

Amateurs

Amateurs have committed most of the computer crimes reported to date. Most embezzlers are not career criminals but rather are normal people who observe a weakness in a security system that allows them to access cash or other valuables. In the same sense, most computer criminals are ordinary computer professionals or users who, while doing their jobs, discover they have access to something valuable.

When no one objects, the amateur may start using the computer at work to write letters, maintain soccer league team standings, or do accounting. This apparently innocent time-stealing may expand until the employee is pursuing a business in accounting, stock portfolio management, or desktop publishing on the side, using the employer's computing facilities. Alternatively, amateurs may become disgruntled over some negative work situation (such as a reprimand or denial of promotion) and vow to "get even" with management by wreaking havoc on a computing installation.

Crackers or Malicious Hackers

System **crackers**, often high school or university students, attempt to access computing facilities for which they have not been authorized. Cracking a computer's defenses is seen as the ultimate victimless crime. The perception is that nobody is hurt or even endangered by a little stolen machine time. Crackers enjoy the simple challenge of trying to log in, just to see whether it can be done. Most crackers can do their harm without confronting anybody, not even making a sound. In the absence of explicit warnings not to trespass in a system, crackers infer that access is permitted. An underground network of hackers helps pass along secrets of success; as with a jigsaw puzzle, a few isolated pieces joined together may produce a large effect. Others attack for curiosity, personal gain, or self-satisfaction. And still others enjoy causing chaos, loss, or harm. There is no common profile or motivation for these attackers.

Career Criminals

By contrast, the career computer criminal understands the targets of computer crime. Criminals seldom change fields from arson, murder, or auto theft to computing; more often, criminals begin as computer professionals who engage in computer crime, finding the prospects and payoff good. There is some evidence that organized crime and international groups are engaging in computer crime. Recently, electronic spies and information brokers have begun to recognize that trading in companies' or individuals' secrets can be lucrative.

Terrorists

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

- ***targets of attack:*** denial-of-service attacks and web site defacements are popular for any political organization because they attract attention to the cause and bring undesired negative attention to the target of the attack.
- ***propaganda vehicles:*** web sites, web logs, and e-mail lists are effective, fast, and inexpensive ways to get a message to many people.
- ***methods of attack:*** to launch offensive attacks requires use of computers.

We cannot accurately measure the amount of computer-based terrorism because our definitions and measurement tools are rather weak. Still, there is evidence that all three of these activities are increasing.

XII. METHODS OF DEFENSE

Computer crime is certain to continue. The goal of computer security is to institute controls that preserve secrecy, integrity, and availability. Sometimes these controls are able to prevent attacks; other less powerful methods can only detect a breach as or after it occurs.

1. Encryption

The most powerful tool in providing computer security is coding. By transforming data so that it is unintelligible to the outside observer, the value of an interception and the possibility of a modification or a fabrication are almost nullified.

Encryption provides secrecy for data. Additionally, encryption can be used to achieve integrity, since data that cannot be read generally also cannot be changed. Furthermore, encryption is important in protocols, which are agreed-upon sequences of actions to accomplish some task. Some protocols ensure availability of resources. Thus, encryption is at the heart of methods for ensuring all three goals of computer security.

Encryption is an important tool in computer security, but one should not overrate its importance. Users must understand that encryption does not solve all computer security problems. Furthermore, if encryption is not used properly , it can have no effect on security or can , in fact , degrade the performance of the entire system . Thus, it is important to know the situations in which encryption is useful and to use it effectively.

2. Software Controls

Programs themselves are the second link in computer security. Programs must be secure enough to exclude outside attack. They must also be developed and maintained so that one can be confident of the dependability of the programs.

Program controls include the following kinds of things:

. Development controls, which are standards under which a program is designed, coded, tested, and maintained

. Operating system controls, which are limitations enforced by the operating system to protect each user from all other users

. Internal program controls that enforce security restrictions, such as access limitations in a data base management program

Software controls may use tools such as hardware components, encryption, or information gathering. Software controls generally affect users directly, and so they are often the first aspects of computer security that come to mind. Because they influence the way users interact with a computing system,

software controls must be carefully designed. Ease of use and potency are often competing goals in the design of software controls.

3. Hardware Controls

Numerous hardware devices have been invented to assist in computer security. These devices range from hardware implementations of encryption to locks limiting access to theft protection to devices to verify users' identities.

(1) Policies

some controls on computing systems are achieved through added hardware or software features, as described above. Other controls are matters of policy. In fact, some of the simplest controls, such as frequent changes of passwords, can be achieved at essentially no cost but with tremendous effect.

Legal and ethical controls are an important part of computer security. The law is slow to evolve, and the technology involving computers has emerged suddenly. Although legal protection is necessary and desirable, it is not as dependable in this area as it would be in more well-understood and long-standing crimes.

The area of computer ethics is likewise unclear, not that computer people are unethical, but rather that society in general and the computing community in particular have not adopted formal standards of ethical behavior. Some organizations are attempting to devise codes of ethics for computer professionals. Although these are important , before codes of ethics become widely accepted and therefore effective , the computing community and the general public need to understand what kinds of behavior are inappropriate and why .

(2) Physical Controls

Some of the easiest, most effective, and least expensive controls are physical controls. Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters. Often the simple physical controls are overlooked while more sophisticated approaches are sought.

(3) Effectiveness of Controls

Merely having controls does no good unless they are used properly. The next section contains a survey of some factors that affect the effectiveness of controls.

. Awareness of Problem

People using controls must be convinced of the need for security; people will willingly cooperate with security requirements only if they understand why security is appropriate in each specific situation. Many users, however, are unaware of the need for security, especially in situations in which a group has recently undertaken a computing task that was previously performed by a central computing department.

. Likelihood of Use

Of course, no control is effective unless it is used. The lock on a computer room door does no good if people block the door open. During World War Ⅱ code clerks used outdated codes because they had already learned them and could encode messages rapidly. Unfortunately, the opposite side had already broken some of those codes and could decode those messages easily.

Principle of Effectiveness. Controls must be used to be effective. They must be efficient, easy to use, and appropriate.

This principle implies that computer security controls must be efficient enough, in terms of time, memory space, human activity, or other resources used, so that using the control does not seriously affect the task being protected. Controls should be selective so that they do not exclude legitimate accesses.

4 . Overlapping Controls

Several different controls may apply to one exposure. For example, security for a microcomputer application may be provided by a combination of controls on program access to the data, on physical access to the microcomputer and storage media, and even by file locking to control access to the processing programs. This situation is shown in fig21-3.

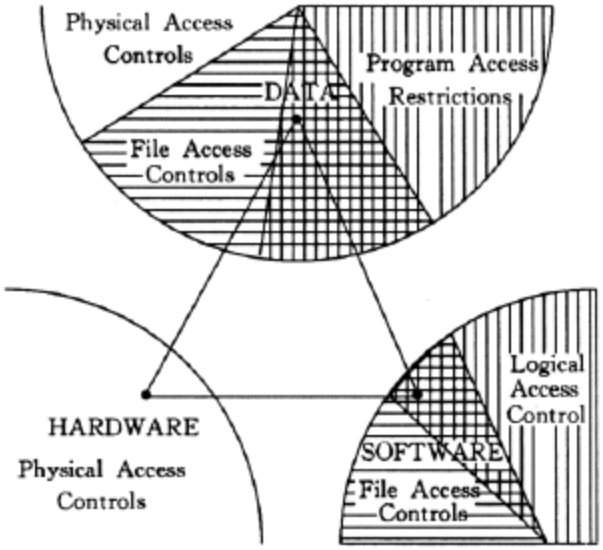

Fig.21-3 Overlapping Controls

5 . Periodic Review

Few controls are permanently effective. Just when the security specialist finds a way to secure assets against certain kinds of attacks, the opposition doubles its efforts in an effort to defeat the security mechanism. Thus, judging the effectiveness of a control is an ongoing task.

1.5 METHODS OF DEFENSE

In Chapter 11, we investigate the legal and ethical restrictions on computer-based crime. But unfortunately, computer crime is certain to continue for the foreseeable future. For this reason, we must look carefully at controls for preserving confidentiality, integrity, and availability. Sometimes these controls can prevent or mitigate attacks; other, less powerful methods can only inform us that security has been compromised, by detecting a breach as it happens or after it occurs.

Harm occurs when a threat is realized against a vulnerability. To protect against harm, then, we can neutralize the threat, close the vulnerability, or both. The possibility for harm to occur is called **risk**. We can deal with harm in several ways. We can seek to

- *prevent it,* by blocking the attack or closing the vulnerability
- *deter it,* by making the attack harder but not impossible
- *deflect it,* by making another target more attractive (or this one less so)
- *detect it,* either as it happens or some time after the fact
- *recover* from its effects

Of course, more than one of these can be done at once. So, for example, we might try to prevent intrusions. But in case we do not prevent them all, we might install a detection device to warn of an imminent attack. And we should have in place incident response procedures to help in the recovery in case an intrusion does succeed.

Hacking as Defence Mechanism

Hacking is *to gain unauthorized access to data or information.* In general, a hacker is a person who enjoys learning the details of computer systems.

A cracker is a hacker who uses the knowledge of hacking for malicious practice. There are two possible ways of a cracker to attack a system:

- an inside attack where the attacker is an inside entity who is an authorized user of the system.
- an outside attack where the attacker is not the authorized user of the system.

Hacking can be used as a methodology to provide security solutions to computer systems in all possible ways and is called *ethical hacking*.

A general audit of a system can be used as a security solution but it does not give a precise solution to security since *vulnerabilities cannot be checked in audits.* Hacking is a different perspective of implementing security in computer systems.

Ethical hackers use the same methodology as crackers to detect vulnerabilities in information systems but *unlike crackers* they *provide countermeasures against vulnerabilities*; whereas crackers detect, explore and take undue advantage of vulnerabilities.

Ethical hackers, thus, have to be one step ahead of crackers. They should know the possible potential threats to systems.

Hacking is not as simple as it seems. For the purpose of hacking, a hacker must have the knowledge of the system to hack. This knowledge may be about networking, TCP/IP, the operating system of the target machine, and also a good knowledge of programming.

The Methodology of Hacking

The general phases involved in hacking are foot printing, scanning, gaining access, maintaining access, and covering tracks. These are discussed below.

1. Foot printing / Reconnaissance: This phase involves the process of gathering information about the system to be attacked. This information can be collected either internally or externally, that is, by authorized or unauthorized access.

   Social engineering is a technique in which the hacker or a person on behalf of a hacker smooth talks to people to collect *sensitive information* like login ids, passwords, IP addresses, unlisted phone numbers, etc. Another way is *dumpster diving*, where the hacker collects information from trash or discarded sensitive information. Internet is a big resource of collecting information about different enterprise systems.

   Social engineering and dumpster diving can be considered as *passive reconnaissance* techniques since the hacker does not directly interact with the system.
2. Scanning: Pre-attack is another term associated with this phase. The hacker uses different tools and techniques to detect vulnerabilities in a computer system. These vulnerabilities may be some open ports (detected using three-way handshake), accessible hosts (detected using ICMP echo request and response), router locations (detected using TRACEROUTE), network mapping, details of operating systems, and applications running on it.
3. Gaining access: In this phase, the hacker may or may not always need access to the computer system to cause damage. Attacks like *denial of service* can stop services of the computer system. This can be done by killing processes on the computer systems with a high degree of vulnerability.

   An *attacker unlike a hacker* may use techniques like spoofing in which malformed packet containing a bug is sent to target machine to exploit vulnerability. Packet flooding may be used to remotely stop availability of essential services.

   The access gaining depends upon the architecture of the target computer system, the skill level of the hacker, and the initial level of access obtained (reconnaissance).
4. Maintaining access: Once the hacker gains access to the target system, he/she can use the access to secure the system to work as an *ethical hacker* or damage the system to work as an attacker (*cracker*).

   Sometimes attackers use Trojans to gain access to the computer system in future. Applications like *rootkit* can be installed after gaining access to the computer systems that enable the hacker to become super users of the system. There are different ways using which organizations can detect intruders like intrusion detection system (IDS), honey pots, etc.
5. Covering tracks: Here the attackers try to keep themselves hidden and undetected on the target computer systems. There are different reasons for this like evading criminal punishment, maintaining access in future, etc. He/she does this by removing contents of log files that contain information about events in the system in detail. Applications like rootkit help the hacker to hide himself. An *ethical hacker* has to be aware of tools and techniques that may be deployed by attackers to ensure protection of the system.

Classification of Hackers

Depending upon the activity profile of hackers, they can be broadly classified as the following:

1. Black Hats: The hackers in this class become crackers by using their talent and computer skills for destruction of the computer systems. They exploit vulnerabilities and after gaining access to the computer system, they follow wrong practices leading malpractice to criminal activities.
2. White Hats: This category of hackers uses the talent and computer skills for defense. They work as security analysts and always think of threats to a computer system and the countermeasures to be used for it.
3. Grey Hats: This category of hackers may work as black hats and white hats at different times.
4. Blue Hats: This category of hackers work with computer security consulting firms to bug test a system prior to its launch, looking for exploits so they can be closed. For example a security professional invited by Microsoft to find vulnerabilities in Windows.

Controls

To consider the controls or countermeasures that attempt to prevent exploiting a computing system's vulnerabilities, we begin by thinking about traditional ways to enhance physical security. In the Middle Ages, castles and fortresses were built to protect the people and valuable property inside. The fortress might have had one or more security characteristics, including

- a strong gate or door, to repel invaders
- heavy walls to withstand objects thrown or projected against them
- a surrounding moat, to control access
- arrow slits, to let archers shoot at approaching enemies
- crenellations to allow inhabitants to lean out from the roof and pour hot or vile liquids on attackers
- a drawbridge to limit access to authorized people
- gatekeepers to verify that only authorized people and goods could enter

Similarly, today we use a multipronged approach to protect our homes and offices. We may combine strong locks on the doors with a burglar alarm, reinforced windows, and even a nosy neighbor to keep an eye on our valuables. In each case, we select one or more ways to deter an intruder or attacker, and we base our selection not only on the value of what we protect but also on the effort we think an attacker or intruder will expend to get inside.

Computer security has the same characteristics. We have many controls at our disposal. Some are easier than others to use or implement. Some are cheaper than others to use or implement. And some are more difficult than others for intruders to override. Figure 1-6 illustrates how we use a combination of controls to secure our valuable

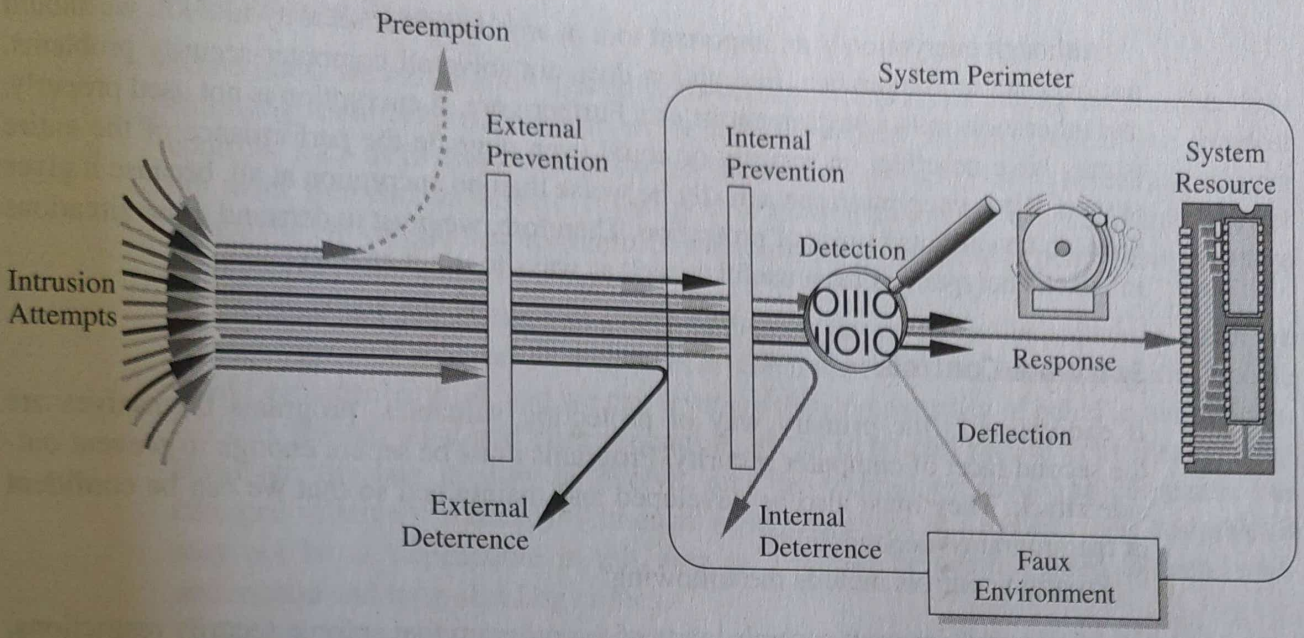

FIGURE 1-6 Multiple Controls.

resources. We use one or more controls, according to what we are protecting, how the cost of protection compares with the risk of loss, and how hard we think intruders will work to get what they want.

In this section, we present an overview of the controls available to us. In later chapters, we examine each control in much more detail.

Encryption

We noted earlier that we seek to protect hardware, software, and data. We can make it particularly hard for an intruder to find data useful if we somehow scramble the data so that interpretation is meaningless without the intruder's knowing how the scrambling was done. Indeed, the most powerful tool in providing computer security is this scrambling or encoding.

Encryption is the formal name for the scrambling process. We take data in their normal, unscrambled state, called **cleartext**, and transform them so that they are unintelligible to the outside observer; the transformed data are called **enciphered text** or **ciphertext**. Using encryption, security professionals can virtually nullify the value of an interception and the possibility of effective modification or fabrication. In Chapters 2 we study many ways of devising and applying these transformations.

Encryption clearly addresses the need for confidentiality of data. Additionally, it can be used to ensure integrity; data that cannot be read generally cannot easily be changed in a meaningful manner. Furthermore, as we see throughout this book, encryption is the basis of **protocols** that enable us to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to a desired result. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security.

Although encryption is an important tool in any computer security tool kit, we should not overrate its importance. Encryption does not solve all computer security problems, and other tools must complement its use. Furthermore, if encryption is not used properly, it may have no effect on security or could even degrade the performance of the entire system. Weak encryption can actually be worse than no encryption at all, because it gives users an unwarranted sense of protection. Therefore, we must understand those situations in which encryption is most useful as well as ways to use it effectively.

Software Controls

If encryption is the primary way of protecting valuables, programs themselves are the second facet of computer security. Programs must be secure enough to prevent outside attack. They must also be developed and maintained so that we can be confident of the programs' dependability.

Program controls include the following:

- *internal program controls:* parts of the program that enforce security restrictions, such as access limitations in a database management program
- *operating system and network system controls:* limitations enforced by the operating system or network to protect each user from all other users
- *independent control programs:* application programs, such as password checkers, intrusion detection utilities, or virus scanners, that protect against certain types of vulnerabilities
- *development controls:* quality standards under which a program is designed, coded, tested, and maintained to prevent software faults from becoming exploitable vulnerabilities

We can implement software controls by using tools and techniques such as hardware components, encryption, or information gathering. Software controls frequently affect users directly, such as when the user is interrupted and asked for a password before being given access to a program or data. For this reason, we often think of software controls when we think of how systems have been made secure in the past. Because they influence the way users interact with a computing system, software controls must be carefully designed. Ease of use and potency are often competing goals in the design of a collection of software controls.

Hardware Controls

Numerous hardware devices have been created to assist in providing computer security. These devices include a variety of means, such as

- hardware or smart card implementations of encryption
- locks or cables limiting access or deterring theft
- devices to verify users' identities
- firewalls
- intrusion detection systems
- circuit boards that control access to storage media

Policies and Procedures

Sometimes, we can rely on agreed-on procedures or policies among users rather than enforcing security through hardware or software means. In fact, some of the simplest controls, such as frequent changes of passwords, can be achieved at essentially no cost but with tremendous effect. Training and administration follow immediately after establishment of policies, to reinforce the importance of security policy and to ensure their proper use.

We must not forget the value of community standards and expectations when we consider how to enforce security. There are many acts that most thoughtful people would consider harmful, and we can leverage this commonality of belief in our policies. For this reason, legal and ethical controls are an important part of computer security. However, the law is slow to evolve, and the technology involving computers has emerged relatively suddenly. Although legal protection is necessary and desirable, it may not be as dependable in this area as it would be when applied to more well-understood and long-standing crimes.

Society in general and the computing community in particular have not adopted formal standards of ethical behavior. As we see in Chapter 11, some organizations have devised codes of ethics for computer professionals. However, before codes of ethics can become widely accepted and effective, the computing community and the general public must discuss and make clear what kinds of behavior are inappropriate and why.

Physical Controls

Some of the easiest, most effective, and least expensive controls are physical controls. Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters. Often the simple physical controls are overlooked while we seek more sophisticated approaches.

Effectiveness of Controls

Merely having controls does no good unless they are used properly. Let us consider several aspects that can enhance the effectiveness of controls.

Awareness of Problem

People using controls must be convinced of the need for security. That is, people will willingly cooperate with security requirements only if they understand why security is appropriate in a given situation. However, many users are unaware of the need for security, especially in situations in which a group has recently undertaken a computing task that was previously performed with lax or no apparent security.

Likelihood of Use

Of course, no control is effective unless it is used. The lock on a computer room door does no good if people block the door open. As Sidebar 1-5 tells, some computer systems are seriously uncontrolled.