**COMPUTER SECURITY**

**INTRODUCTION:**

Computer Security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

**Integrity**: In lay usage, information has integrity when it is timely, accurate, complete, and consistent. However, computers are unable to provide or protect all of these qualities. Therefore, in the computer security field, integrity is often discussed more narrowly as having two facets: data integrity and system integrity. Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system."

The definition of integrity has been, and continues to be, the subject of much debate among computer security experts.

**Availability**: A requirement intended to assure that systems work promptly and service is not denied to authorized users.

**Confidentiality**: A requirement that private or confidential information not be disclosed to unauthorized individuals.

**THEORY OF COMPUTER SECURITY**

The threats to computer security can be countered by providing access control over information on a computer to ensure that only specifically authorized users are allowed access.

What we desire is a set of methods that make it possible to build a relatively small part of the system in such a way that one can even allow a clever attacker who uses malicious software to build the rest of the system and its applications, and it will still be secure. The theory of computer security gives us this.

Understanding computer security involves understanding three fundamental notions:

1. A security policy, stating the laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information;

2. The functionality of internal mechanisms to enforce that security policy; and

3. Assurance that the mechanisms do enforce the security policy.

Now we introduce these three important notions and describe how they pertain to the reference monitor concept, which provides a set of principles that can be applied to the design or selection of security features and to their implementation in ways that afford a high degree of resistance to malicious software. We begin with an example from the world of people and sensitive documents to illustrate the requirements of any information security system. We then introduce the reference monitor concept as we apply it in designing secure computer systems.

**An example: Protecting sensitive documents.** If we had a collection of extremely sensitive documents — perhaps corporate plans and strategies or classified national security information — we might go to extreme lengths to protect that collection. Thinking about the measures that we might take to provide such protection will help us find an intuitive basis for the reference monitor concept.

Restricting access:Since we are talking about documents (presumably ink on paper), we can most naturally think about locking them up. So we buy something like a bank vault to hold our little library of priceless secrets. But the documents still have to be used, so we have to provide a way for authorized people to get at them and read them. Now we have to put a door in our vault and provide some set of controls over who can and who cannot go in.

We can place a guard post in front of our vault door and staff it with a team of extremely vigilant and trustworthy guards. These guards can surely exercise control over who goes in and who goes out, but they will need some set of criteria for determining who is authorized for such access.

We can solve this problem by providing the guards with a list that specifies only those individuals we have authorized (in the national security case, those we have cleared) for access to the vault and its secrets.

Now the guards know who may and who may not enter. We are not finished, though. For when an individual shows up at the guard post and requests entry, the guards need some way to check that the person is not claiming a fake identity. We might simply rely on the guards’ powers of recognition, or we can invent a variety of measures to provide the guards with the information they need. We can give each authorized individual a badge or pass and direct the guards to check the badge against the appearance of a valid badge. Perhaps we can store each individual’s photograph, or even fingerprints, and associate them in the authorization list with individuals’ names. This information is necessary to authenticate the identification of the individual in a reliable way. We can invent schemes of almost limitless cost and complexity to help the guards assure themselves that they are admitting only authorized people to the vault.

Finally, we might want to check up on the guards to make sure that only those users on the authorization list are being admitted to the vault to use the document collection — to ensure individual accountability for the guards’ work. So we can add to our basic protection scheme a log that must be signed by both guard and visitor to give us a clear record of visits to our vault.

Of course, we must not only have a good security system; we must also implement it correctly. If a guard is subject to subversion or if our vault has walls of paper rather than steel, the security we provide will not be very effective. The extent to which we must worry about such matters will depend on the sensitivity of the information and on the threat we perceive. Perhaps we will put moderately sensitive documents in a locked room with an unarmed guard and very sensitive ones in a real bank-style vault with armed guards.

**ELEMENTS OF COMPUTER SECURITY**

Computer security is based on eight major elements:

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

Familiarity with these elements will aid the reader in better understanding how the security controls (discussed in later sections) support the overall computer security program goals.

**Computer Security Supports the Mission of the Organization**: The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake - they are put in place to protect important assets and thereby support the overall organizational mission. Security, therefore, is a means to an end and not an end in itself. For example, in a private- sector business, having good security is usually secondary to the need to make a profit. Security, then, ought to increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to the agency's service provided to citizens. Security, then, ought to help improve the service provided to the citizen. To act on this, managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission. The roles and functions of a system may not be constrained to a single organization. In an inter-organizational system, each organization benefits from securing the system. For example, for electronic commerce to be successful, each of the participants requires security controls to protect their resources. However, good security on the buyer's system also benefits the seller; the buyer's system is less likely to be used for fraud or to be unavailable or otherwise negatively affect the seller. (The reverse is also true.)

**Computer Security is an Integral Element of Sound Management**: Information and computer systems are often critical assets that support the mission of an organization. Protecting them can be as critical as protecting other organizational resources, such as money, physical assets, or employees. However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what the level of risk they are willing to accept, taking into account the cost of security controls. As with many other resources, the management of information and computers may transcend organizational boundaries. When an organization's information and computer systems are linked with external systems, management's responsibilities also extend beyond the organization. This may require that management:

* know what general level or type of security is employed on the external system(s) or
* Seek assurance that the external system provides adequate security for the using organization's needs.

**Computer Security Should Be Cost-Effective**: The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the computer systems and to the severity, probability and extent of potential harm. Requirements for security vary, depending upon the particular computer system. In general, security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization may estimate that it is experiencing significant losses per year in inventory through fraudulent manipulation of its computer system. Security measures, such as an improved access control system, may significantly reduce the loss. Moreover, a sound security program can thwart hackers and can reduce the frequency of viruses. Elimination of these kinds of threats can reduce unfavorable publicity as well as increase morale and productivity. Security benefits, however, do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire-suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. All of these have to be considered in addition to the basic cost of the control itself. In many cases, these additional costs may well exceed the initial cost of the control (as is often seen, for example, in the costs of administering an access control package). Solutions to security problems should not be chosen if they cost more, directly or indirectly, than simply tolerating the problem.

**Computer Security Responsibilities and Accountability Should Be Made Explicit**: The responsibilities and accountability 10 of owners, providers, and users of computer systems and other parties 11 concerned with the security of computer systems should be explicit. The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries. Depending on the size of the organization, the program may be large or small, even a collateral duty of another management official. However, even small organizations can prepare a document that states organization policy and makes explicit computer security responsibilities. This element does not specify that individual accountability must be provided for on all systems. For example, many information dissemination systems do not require user identification and, therefore, cannot hold users accountable.

**Systems Owners Have Security Responsibilities Outside Their Own Organizations**: If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be confident that the system is adequately secure. (This does not imply that all systems must meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security.) In addition to sharing information about security, organization managers "should act in a timely, coordinated manner to prevent and to respond to breaches of security" to help prevent damage to others. However, taking such action should not jeopardize the security of systems.

**Computer Security Requires a Comprehensive and Integrated Approach**: Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

* Interdependencies of Security Controls to work effectively: security controls often depend upon the proper functioning of other controls. In fact, many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly believe that their system will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.
* Other Interdependencies: The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. Computer security needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Managers should recognize how computer security relates to other areas of systems and organizational management.

**Computer Security Should Be Periodically Reassessed**: Computers and the environments they operate in are dynamic. System technology and users, data and information in the systems, risks associated with the system and, therefore, security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connecting to external networks; a change in the value or use of information; or the emergence of a new threat. In addition, security is never perfect when a system is implemented. System users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare, and procedures become outdated over time. All of these issues make it necessary to reassess the security of computer systems.

**Computer Security is constrained by Societal Factors**: The ability of security to support the mission of the organization(s) may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on a computer system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.) Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures, such as retinal scanning, may be considered invasive in some environments and cultures. The underlying idea is that security measures should be selected and implemented with recognition of the rights and legitimate interests of others. This many involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security. The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

**COMPUTER SECURITY RISK MANAGEMENT**

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Though perhaps not always aware of it, individuals manage risks every day. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecast, or writing down a list of things to do rather than trusting to memory fall into the purview of risk management. People recognize various threats to their best interests and take precautions to guard against them or to minimize their effects. Both government and industry routinely manage a myriad of risks. For example, to maximize the return on their investments, businesses must often decide between aggressive (but high-risk) and slow-growth (but more secure) investment plans. These decisions require analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action. While there are many models and methods for risk management, there are several basic activities and processes that should be performed. In discussing risk management, it is important to recognize its basic, most fundamental assumption: computers cannot ever be fully secured. There is always risk, whether it is from a trusted employee who defrauds the system or a fire that destroys critical resources. Risk management is made up of two primary and one underlying activities; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one.

**COMPUTER SECURITY INCIDENT HANDLING**

Computer systems are subject to a wide range of mishaps - from corrupted data files, to viruses, to natural disasters. Some of these mishaps can be fixed through standard operating procedures. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe mishaps, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from deliberate malicious technical activity (e.g., the creation of viruses or system hacking).

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It is used in this chapter to broadly refer to those incidents resulting from deliberate malicious technical activity. It can more generally refer to those incidents that, without technically expert response, could result in severe damage. This definition of a computer security incident is somewhat flexible and may vary by organization and computing environment. Although the threats that hackers and malicious code pose to systems and networks are well known, the occurrence of such harmful events remains unpredictable. Security incidents on larger networks (e.g., the Internet), such as break-ins and service disruptions, have harmed various organizations' computing capabilities. When initially confronted with such incidents, most organizations respond in an ad hoc manner. However recurrence of similar incidents often makes it cost-beneficial to develop a standing capability for quick discovery of and response to such events. This is especially true, since incidents can often "spread" when left unchecked thus increasing damage and seriously harming an organization. Incident handling is closely related to contingency planning as well as support and operations. An incident handling capability may be viewed as a component of contingency planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Broadly speaking, contingency planning addresses events with the potential to interrupt system operations. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

**Characteristics of a Successful Incident Handling** **Capability**

A successful incident handling capability has several core characteristics:

* an understanding of the constituency it will serve.
* an educated constituency.
* a means for centralized communications
* expertise in the requisite technologies
* and links to other groups to assist in incident handling (as needed).

**SECURITY CONSIDERATIONS IN COMPUTER SUPPORT AND OPERATIONS** Computer support and operations refer to everything done to run a computer system. This includes both system administration and tasks external to the system that support its operation (e.g., maintaining documentation). It does not include system planning or design. The support and operation of any computer system, from a three-person local area network to a worldwide application serving thousands of users, is critical to maintaining the security of a system. Support and operations are routine activities that enable computer systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems. The failure to consider security as part of the support and operations of computer systems is, for many organizations, their Achilles heel. Computer security system literature includes many examples of how organizations undermined their often expensive security measures because of poor documentation, old user accounts, conflicting software, or poor control of maintenance accounts. Also, an organization's policies and procedures often fail to address many of these important issues.

The important security considerations within some of the major categories of support and operations are:

* user support,
* software support,
* configuration management,
* backups,
* media controls,
* documentation,
* and maintenance.

**IDENTIFICATION AND AUTHENTICATION**

For most systems, identification and authentication (I&A) is the first line of defense. I&A is a technical measure that prevents unauthorized people (or unauthorized processes) from entering a computer system. I&A is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system be able to identify and differentiate among users. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses required to perform their duties. User accountability requires the linking of activities on a computer system to specific individuals and, therefore, requires the system to identify users. Identification is the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim.

Computer systems recognize people based on the authentication data the systems receive. Authentication presents several challenges: collecting authentication data, transmitting the data securely, and knowing whether the person who was originally authenticated is still the person using the computer system. For example, a user may walk away from a terminal while still logged on, and another person may start using it.

There are three means of authenticating a user's identity which can be used alone or in combination:

* something the individual knows (a secret- e.g., a password, Personal Identification Number (PIN), or cryptographic key);
* something the individual possesses (a token - e.g., an ATM card or a smart card); and
* something the individual is (a biometric - e.g., such characteristics as a voice pattern, handwriting dynamics, or a fingerprint).

While it may appear that any of these means could provide strong authentication, there are problems associated with each. If people wanted to pretend to be someone else on a computer system, they can guess or learn that individual's password; they can also steal or fabricate tokens. Each method also has drawbacks for legitimate users and system administrators: users forget passwords and may lose tokens, and administrative overhead for keeping track of I&A data and tokens can be substantial. Biometric systems have significant technical, user acceptance, and cost problems as well.

This section explains current I&A technologies and their benefits and drawbacks as they relate to the three means of authentication. Although some of the technologies make use of cryptography because it can significantly strengthen authentication

**I&A Based on Something the User Knows**: The most common form of I&A is a user ID coupled with a password. This technique is based solely on something the user knows. There are other techniques besides conventional passwords that are based on knowledge, such as knowledge of a cryptographic key.

* Passwords: In general, password systems work by requiring the user to enter a user ID and password (or passphrase or personal identification number). The system compares the password to a previously stored password for that user ID. If there is a match, the user is authenticated and granted access. Benefits of Passwords. Passwords have been successfully providing security for computer systems for a long time. They are integrated into many operating systems, and users and system administrators are familiar with them. When properly managed in a controlled environment, they can provide effective security. Problems With Passwords. The security of a password system is dependent upon keeping passwords secret. Unfortunately, there are many ways that the secret may be divulged. All of the problems discussed below can be significantly mitigated by improving password security, as discussed in the sidebar. However, there is no fix for the problem of electronic monitoring, except to use more advanced authentication (e.g., based on cryptographic techniques or tokens).

**I&A Based on Something the User Possesses**: Although some techniques are based solely on something the user possesses, most of the techniques described in this section are combined with something the user knows. This combination can provide significantly stronger security than either something the user knows or possesses alone. Objects that a user possesses for the purpose of I&A are called tokens. This section divides tokens into two categories: memory tokens and smart tokens.

**I&A Based on Something the User Is**: Biometric authentication technologies use the unique characteristics (or attributes) of an individual to authenticate that person's identity. These include physiological attributes (such as fingerprints, hand geometry, or retina patterns) or behavioral attributes (such as voice patterns and hand-written signatures). Biometric authentication technologies based upon these attributes have been developed for computer log-in applications. Biometric authentication is technically complex and expensive, and user acceptance can be difficult. However, advances continue to be made to make the technology more reliable, less costly, and more user-friendly.

Biometric systems can provide an increased level of security for computer systems, but the technology is still less mature than that of memory tokens or smart tokens. Imperfections in biometric authentication devices arise from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes. These may change, depending on various conditions. For example, a person's speech pattern may change under stressful conditions or when suffering from a sore throat or cold. Due to their relatively high cost, biometric systems are typically used with other authentication means in environments requiring high security.

**REFERENCES**

Guttman, Barbara. ( 1992), Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials. Special Publication 800-4. Gaithersburg, MD: National Institute of Standards and Technology.

Pfleeger, C, S. Pfleeger, and M. Theofanos. (1989), "A Methodology for Penetration Testing." Computers and Security. 8(7). pp. 613-620.

Barbara Guttman and Edward A. Roback.(1995) “An Introduction to Computer Security: The NIST Handbook”. NIST special Publication 800-12.