Computer Security: A Practical Definition

Defining "computer security" is not trivial. The difficulty lies in developing a definition that is broad enough to be valid regardless of the system being described, yet specific enough to describe what security really is. In a generic sense, security is "freedom from risk or danger." In the context of computer science, security is the prevention of, or protection against,

- access to information by unauthorized recipients, and
- intentional but unauthorized destruction or alteration of that information[1]

This can be re-stated: "Security is the ability of a system to protect information and system resources with respect to confidentiality and integrity." Note that the scope of this second definition includes system resources, which include CPUs, disks, and programs, in addition to information.

A Taxonomy of Computer Security

Computer security is frequently associated with three core areas, which can be conveniently summarized by the acronym "CIA":

- **Confidentiality** -- Ensuring that information is not accessed by unauthorized persons
- **Integrity** -- Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users
- **Authentication** -- Ensuring that users are the persons they claim to be

A strong security protocol addresses all three of these areas. Take, for example, Netscape's SSL (Secure Sockets Layer) protocol. It has enabled an explosion in ecommerce which is really about trust (or more precisely, about the lack of trust). SSL overcomes the lack of trust between transacting parties by ensuring confidentiality through encryption, integrity through checksums, and authentication via server certificates (see Chapter 15 of *Unix System Security Tools*).

Computer security is not restricted to these three broad concepts. Additional ideas that are often considered part of the taxonomy of computer security include:

- **Access control** -- Ensuring that users access only those resources and services that they are entitled to access and that qualified users are not denied access to services that they legitimately expect to receive
- **Nonrepudiation** -- Ensuring that the originators of messages cannot deny that they in fact sent the messages[2]
- **Availability** -- Ensuring that a system is operational and functional at a given moment, usually provided through redundancy; loss of availability is often referred to as "denial-of-service"
- **Privacy** -- Ensuring that individuals maintain the right to control what information is collected about them, how it is used, who has used it, who maintains it, and what purpose it is used for

These additional elements don't neatly integrate into a singular definition. From one perspective, the concepts of privacy, confidentiality, and security are quite distinct and possess different attributes. Privacy is a property of individuals; confidentiality is a property of data; and security is a property assigned to computer hardware and software systems. From a practical perspective, the concepts are interwoven. A system that does not maintain data confidentiality or individual privacy could be theoretically or even mathematically "secure," but it probably wouldn't be wise to deploy anywhere in the real world.

A Functional View

Computer security can also be analyzed by function. It can be broken into five distinct functional areas:[3]

- **Risk avoidance** -- A security fundamental that starts with questions like: Does my organization or business engage in activities that are too risky? Do we really need an unrestricted Internet connection? Do we really need to computerize that secure business process? Should we really standardize on a desktop operating system with no access control intrinsics?
- **Deterrence** -- Reduces the threat to information assets through fear. Can consist of communication strategies designed to impress potential attackers of the likelihood of getting caught. See Rule 5: The Fear of Getting Caught is the Beginning of Wisdom.
- **Prevention** -- The traditional core of computer security. Consists of implementing safeguards like the tools covered in this book. Absolute prevention is theoretical, since there's a vanishing point where additional preventative measures are no longer cost-effective.
- **Detection** -- Works best in conjunction with preventative measures. When prevention fails, detection should kick in,

preferably while there's still time to prevent damage. Includes log-keeping and auditing activities

- **Recovery** -- When all else fails, be prepared to pull out backup media and restore from scratch, or cut to backup servers and net connections, or fall back on a disaster recovery facility. Arguably, this function should be attended to before the others

Analyzing security by function can be a valuable part of the security planning process; a strong security policy will address all five areas, starting with recovery. This book, however, is primarily concerned with prevention and detection.

Security Domains

Computer security is also frequently defined in terms of several interdependent domains that roughly map to specific departments and job titles:

- **Physical security** -- Controlling the comings and goings of people and materials; protection against the elements and natural disasters
- **Operational/procedural security** -- Covering everything from managerial policy decisions to reporting hierarchies
- **Personnel security** -- Hiring employees, background screening, training, security briefings, monitoring, and handling departures
- **System security** -- User access and authentication controls, assignment of privilege, maintaining file and filesystem integrity, backups, monitoring processes, log-keeping, and auditing
- **Network security** -- Protecting network and telecommunications equipment, protecting network servers and transmissions, combatting eavesdropping, controlling access from untrusted networks, firewalls, and detecting intrusions

This text is solely concerned with the latter two. System and network security are difficult, if not impossible, to separate in a UNIX system. Nearly every UNIX distribution in the past fifteen years has included a TCP/IP protocol implementation as well as numerous network services such as FTP, Telnet, DNS, and, more recently, HTTP.

A Practical Definition

In the spirit of practicality, I like the straightforward definition promulgated by Simson Garfinkel and Gene Spafford in Practical UNIX & Internet Security: "A computer is secure if you can depend on it and its software to behave as you expect."[4] In essence, a computer is secure if you can trust it. Data entered today will still be there tomorrow in unaltered form. If you made services x, y, and z available yesterday, they're still available today.

I also like the practical definition offered by Tomas Olovsson, which is narrowed a bit: "A secure system is a system on which enough trust can be put to use it together with sensitive information."[5]

These practical definitions circumvent an obvious element: a secure system should be hard for unauthorized persons to break into -- i.e., the value of the work necessary for an unauthorized person to break in should exceed the value of the protected data. Increasing attacker workload and the risks of detection are critical elements of computer security.

For the purposes of this book, I define "system security" as:

> The ongoing and redundant implementation of protections for the confidentiality and integrity of information and system resources so that an unauthorized user has to spend an unacceptable amount of time or money or absorb too much risk in order to defeat it, with the ultimate goal that the system can be trusted with sensitive information.

---

1. *Dictionary of Computing,* Fourth Ed. (Oxford: Oxford University Press, 1996).

2. Bryan Pfaffenberger, *Webster's New World Dictionary of Computing Terms,* Sixth Ed. (New York: Simon and Schuster, 1997).

3. Donn B. Parker, *Computer Security Management* (Reston, VA: Reston Publishing Company Inc., 1981).

4. Simson Garfinkel and Gene Spafford, *Practical UNIX & Internet Security,* Ed. 2 (Sebastopol, CA: O'Reilly, 1996), 6. Highly recommended.

5. Tomas Olovsson, "A Structured Approach to Computer Security," Technical Report No. 122, 1992. See *http://www.ce.chalmers.se/~ulfl/webmdemo/wmwork/www/security_122_1.html*

◀ BACK NEXT ▶

Google™ [ ] Search

● Web ○ www.albion.com

Albion Home | Netiquette | Netdictionary | Security