**A Definition of Computer Security**

The NIST Computer Security Handbook [NIST95] defines the term *computer security*

as follows

**Computer Security:** 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).

This definition introduces three key objectives that are at the heart of computer

security:

• **Confidentiality:** This term covers two related concepts:

— **Data confidentiality:** Assures that private or confidential information is

not made available or disclosed to unauthorized individuals.

— **Privacy:** Assures that individuals control or influence what information

related to them may be collected and stored and by whom and to whom

that information may be disclosed.

• **Integrity:** This term covers two related concepts:

— **Data integrity:** Assures that information and programs are changed only

in a specified and authorized manner.

— **System integrity:** Assures that a system performs its intended function in

an unimpaired manner, free from deliberate or inadvertent unauthorized

manipulation of the system.

• **Availability:** Assures that systems work promptly and service is not denied to

authorized users.

These three concepts form what is often referred to as the **CIA triad**. The three

concepts embody the fundamental security objectives for both data and for information

and computing services. For example, the NIST standard FIPS 199 (*Standards*

*for Security Categorization of Federal Information and Information Systems*) lists

confidentiality, integrity, and availability as the three security objectives for information

and for information systems. FIPS 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

• **Confidentiality:** Preserving authorized restrictions on information access and

disclosure, including means for protecting personal privacy and proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

• **Integrity:** Guarding against improper information modification or destruction,

including ensuring information nonrepudiation and authenticity.

A loss of integrity is the unauthorized modification or destruction of information.

• **Availability:** Ensuring timely and reliable access to and use of information.

A loss of availability is the disruption of access to or use of information or an

information system.

Although the use of the CIA triad to define security objectives is well established,

some in the security field feel that additional concepts are needed to present

a complete picture. Two of the most commonly mentioned are as follows:

• **Authenticity:** The property of being genuine and being able to be verified and

trusted; confidence in the validity of a transmission, a message, or message

originator. This means verifying that users are who they say they are and that

each input arriving at the system came from a trusted source.

• **Accountability:** The security goal that generates the requirement for actions

of an entity to be traced uniquely to that entity. This supports nonrepudiation,

deterrence, fault isolation, intrusion detection and prevention, and after-action

recovery and legal action. Because truly secure systems are not yet an achievable

goal, we must be able to trace a security breach to a responsible party.

Systems must keep records of their activities to permit later forensic analysis to

trace security breaches or to aid in transaction disputes.