NIST Special Publication 800-33

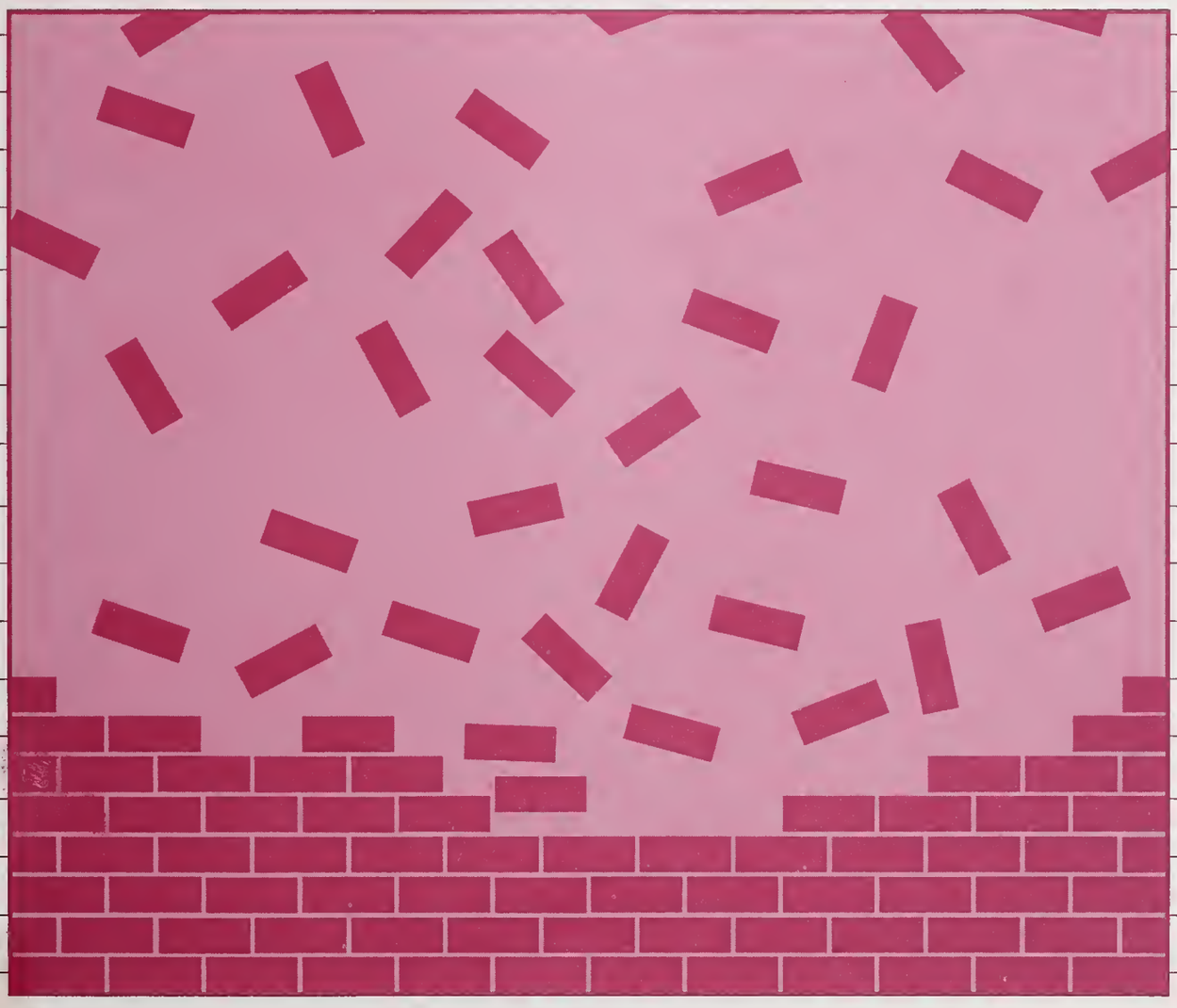
Underlying Technical Models for Information Technology Security

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

COMPUTER SECURITY



1901-2001
NIST CENTENNIAL

The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

Office of the Director
- National Quality Program
- International and Academic Affairs

Technology Services
- Standards Services
- Technology Partnerships
- Measurement Services
- Information Services

Advanced Technology Program
- Economic Assessment
- Information Technology and Applications
- Chemistry and Life Sciences
- Materials and Manufacturing Technology
- Electronics and Photonics Technology

Manufacturing Extension Partnership Program
- Regional Programs
- National Programs
- Program Development

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Radio-Frequency Technology[1]
- Electromagnetic Technology[1]
- Optoelectronics[1]

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- NIST Center for Neutron Research

Chemical Science and Technology Laboratory
- Biotechnology
- Physical and Chemical Properties[2]
- Analytical Chemistry
- Process Measurements
- Surface and Microanalysis Science

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Optical Technology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Manufacturing Metrology
- Intelligent Systems
- Fabrication Technology
- Manufacturing Systems Integration

Building and Fire Research Laboratory
- Applied Economics
- Structures
- Building Materials
- Building Environment
- Fire Safety Engineering
- Fire Science

Information Technology Laboratory
- Mathematical and Computational Sciences[2]
- Advanced Network Technologies
- Computer Security
- Information Access
- Convergent Information Systems
- Information Services and Computing
- Software Diagnostics and Conformance Testing
- Statistical Engineering

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO.

NIST Special Publication 800-33

Underlying Technical Models for Information Technology Security

Recommendation of the
National Institute of Standards and Technology

Gary Stoneburner

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

Reports on Information Security Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-33
Natl. Inst. Stand. Technol. Spec. Publ. 800-33, 27 pages (December 2001)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Table of Contents

Table of Figures

1.0 Introduction

Authority

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5)). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(3)).

This document is recommended for use by Federal organizations which process sensitive information,[1] and is consistent with the requirements of OMB Circular A-130, Appendix III.

The recommendations herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should these recommendations be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

Purpose

The purpose of this document is to provide a description of the technical foundations, termed "models," that underlie secure information technology (IT).

The intent is to provide, in a concise form, the models that should be considered in the design and development of technical security capabilities. These models encompass lessons learned, good practices, and specific technical considerations.

Audience

The intended audience consists of both government and private sectors including:

- IT users desiring a better understanding of system security,
- Engineers and architects designing/building security capabilities, and
- Those developing guidance for others to use in implementing security capabilities.

[1] The Computer Security Act defines the term "sensitive information" as: *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.*

2.0 Security Goal and Objectives

Security Goal

The goal of information technology security is to:

> Enable an organization to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners and customers.

Security Objectives

The security goal can be met through the following security objectives:

1. Availability (of systems and data for intended use only)

   Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users. This objective protects against:

   - Intentional or accidental attempts to either:
     - perform unauthorized deletion of data, or
     - otherwise cause a denial of service or data.
   - Attempts to use system or data for unauthorized purposes

   Availability is frequently an organization's foremost security objective.

2. Integrity (of system and data)

   Integrity has two facets:

   - Data integrity (the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit), or
   - System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation).

   Integrity is commonly an organization's most important security objective after availability.

3. Confidentiality (of data and system information)

   Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

   For many organizations, confidentiality is frequently behind availability and integrity in terms of importance. Yet for some systems and for specific types of data in most systems (e.g., authenticators), confidentiality is extremely important.

4. Accountability (to the individual level)

   Accountability is the requirement that actions of an entity may be traced uniquely to that entity.

   Accountability is often an organizational policy requirement and directly supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

5. Assurance (that the other four objectives have been adequately met)

   Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information it processes. The other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation when:

   - required functionality is present and correctly implemented,
   - there is sufficient protection against unintentional errors (by users or software), and
   - there is sufficient resistance to intentional penetration or by-pass.

   Assurance is essential; without it the other objectives are not met. However, assurance is a continuum; the amount of assurance needed varies between systems.

Security Objective Interdependencies

The five security objectives are interdependent. Achieving one objective without consideration of the others is seldom possible. This is depicted in Figure 2-1 and discussed below.

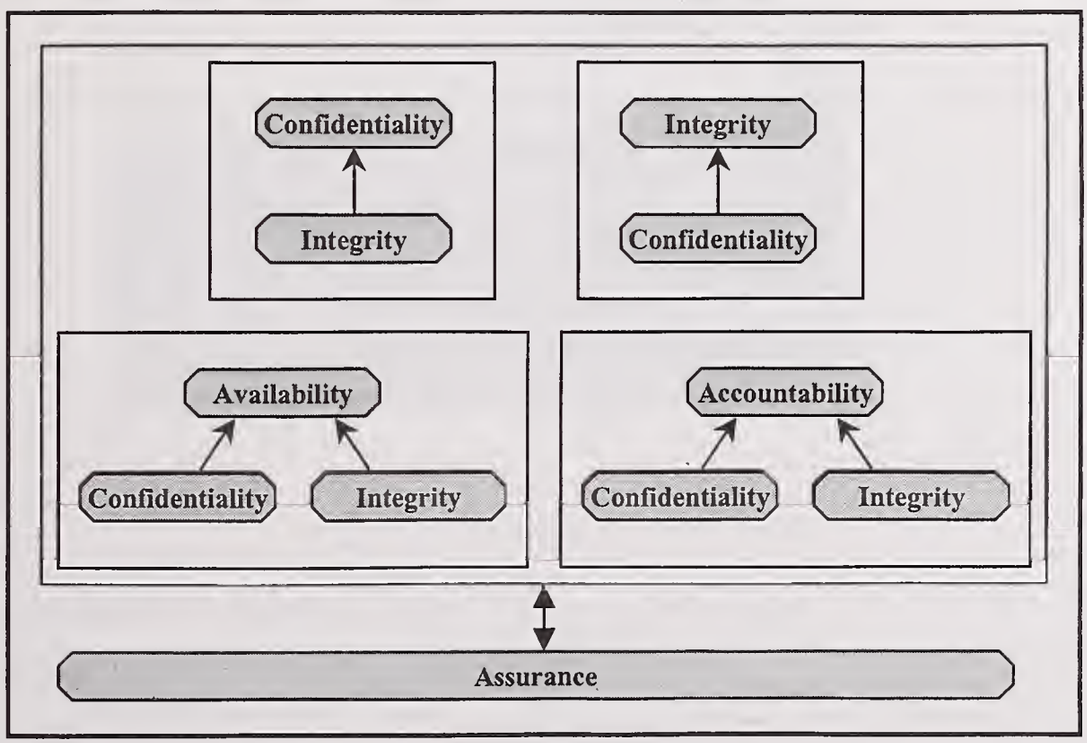


Figure 2-1 Security Objective Dependencies

The Figure 2-1 shows the following dependencies:

Confidentiality is dependent on Integrity, in that if the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid.

Integrity is dependent on Confidentiality, in that if the confidentiality of certain information is lost (e.g., the superuser password), then the integrity mechanisms are likely to be by-passed.

Availability and Accountability are dependent on Confidentiality and Integrity, in that:

- if confidentiality is lost for certain information (e.g., superuser password), the mechanisms implementing these objectives are easily by-passable; and
- if system integrity is lost, then confidence in the validity of the mechanisms implementing these objectives is also lost.

All of these objectives are interdependent with Assurance. When designing a system, an architect or engineer establishes an assurance level as a target. This target is achieved by both defining and meeting the functionality requirements in each of the other four objectives and doing so with sufficient "quality." Assurance highlights the fact that for a system to be secure, it must not only provide the intended functionality, but also ensure that undesired actions do not occur.

3.0 Security Services Model

The underlying technical security services model is depicted in Figure 3-1 which shows the primary services and supporting elements used in implementing an information technology security capability, along with their primary relationships. The model also classifies the services according to their primary purpose as follows:

- Support. These services are generic and underlie most information technology security capabilities.
- Prevent. These services focus on preventing a security breach from occurring.
- Recover. The services in this category focus on the detection and recovery from a security breach.

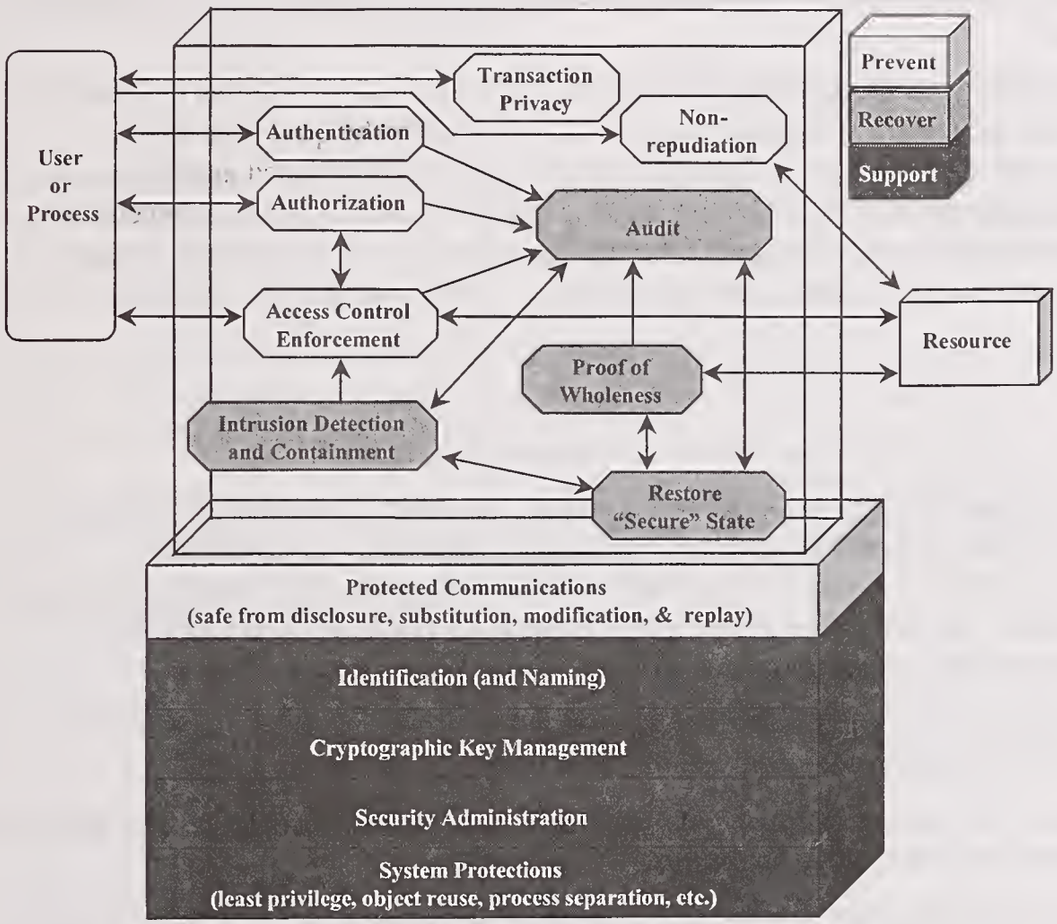


Figure 3-1 Security Services Model

Section Roadmap - This section contains the following information:

- definition for each of the services listed in the model; and
- breakout of the model for each of the five security objectives, giving the primary services for implementing each objective.

3.1 Service Definitions

Supporting:

Supporting services are, by their very nature, pervasive and inter-related with many other services. The supporting services are:

- Identification (and naming) In order to implement many of the other services, it is essential that both subjects and objects be identifiable. This service provides the capability to uniquely identify users, processes, and information resources.
- Cryptographic key management Cryptographic keys must be securely managed when cryptographic functions are implemented in various other services.
- Security administration The security features of the system need to be administered in order to meet the needs of a specific installation and to account for changes in the operational environment.
- System protections Underlying the various security functional capabilities is a base of confidence in the technical implementation. This represents the quality of the implementation from both the perspective of the design processes used and the manner in which the implementation was accomplished. Some examples of system protections are: residual information protection (also known as object reuse), least privilege, process separation, modularity, layering, and minimization of what needs to be trusted.

Prevention:

These services can prevent the security breach from ever happening.

- Protected communications In a distributed system, the ability to accomplish security objectives is highly dependent on trustworthy communications. The protected communications service ensures the integrity, availability, and confidentiality of information while in transit. In most situations all three elements are essential requirements, with confidentiality being needed at least for authentication information.
- Authentication Ensuring that a claimed identity is valid is extremely important. The authentication service provides the means to verify the identity of a subject.
- Authorization The authorization service enables specification and subsequent management of the allowed actions for a given system.
- Access control enforcement When the subject requesting access has been validated for access to particular processes, enforcing the defined security policy s still necessary. The access control enforcement service provides this enforcement, and frequently the enforcement mechanisms are distributed throughout the system. It is not only the correctness of the access control decision, but also the strength of the access control enforcement that determines the level of security obtained. Checking identity and requested access against access control lists is a common access control enforcement mechanism. File encryption is another example of an access control enforcement mechanism.

- Non-repudiation System accountability depends upon the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Non-repudiation is a service that spans prevention and detection. This service has been placed into the prevention category because the mechanisms implemented prevent the ability to successfully repudiate an action. As a result, this service is typically performed at the point of transmission or reception.
- Transaction privacy Both government and private systems are increasingly required to maintain the privacy of individuals using these systems. The transaction privacy service protects against loss of privacy with respect to transactions being performed by an individual.

Detection and Recovery:

Because no set of prevention measures is perfect, it is necessary to both detect security breaches and to take actions to reduce their impact.

- Audit The auditing of security relevant events is a key element for after-the-fact detection of and recovery from security breaches.
- Intrusion detection and containment Detecting insecure situations is essential in order to respond in a timely manner. Also, detecting a security breach is of little use if no effective response can be initiated. The intrusion detection and containment service provides these two capabilities.
- Proof of Wholeness In order to determine that integrity has been compromised, the ability must exist to detect when information or system state is potentially corrupted. The proof of wholeness service provides this ability.
- Restore "secure" state When a security breach occurs, the system must be able to return to a state that is known to be secure. That is the purpose for this service.

3.2 Achieving Security Objectives

The figures below show those services that are most important in achieving the following security objectives:

Figure 3.2-1 - Availability

Figure 3.2-2 - Integrity

Figure 3.2-3 - Confidentiality

Figure 3.2-4 - Accountability

Figure 3.2-5 - Assurance

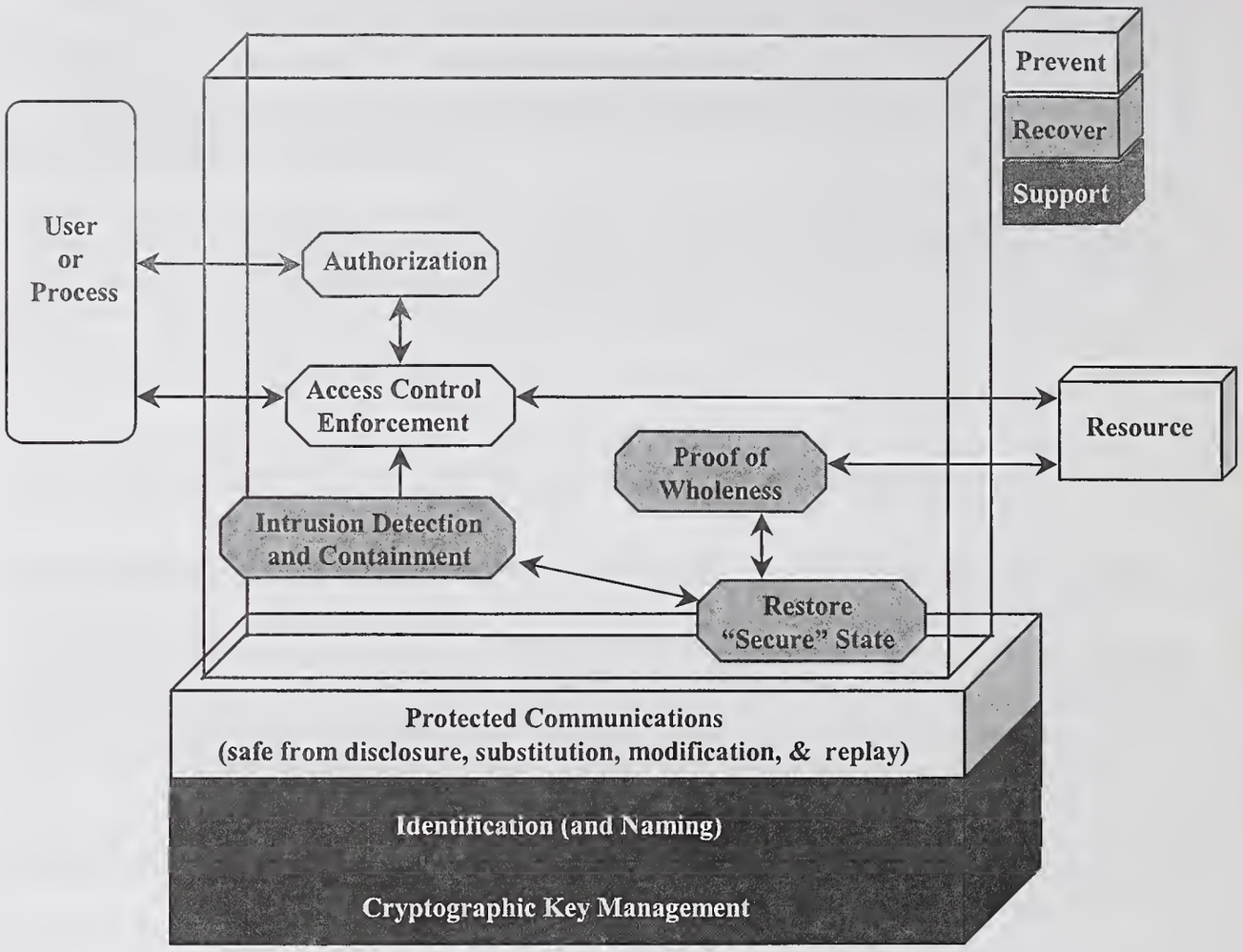


Figure 3.2-1 Primary Availability Services

The primary availability services are those that directly impact the ability of the system to maintain operational effectiveness. One aspect of maintaining effectiveness is protection from unauthorized changes or deletions by defining authorized access and enforcing this definition. Mission effectiveness is also maintained by detecting intrusions, detecting a loss of wholeness, and providing the means of returning to a secure state.

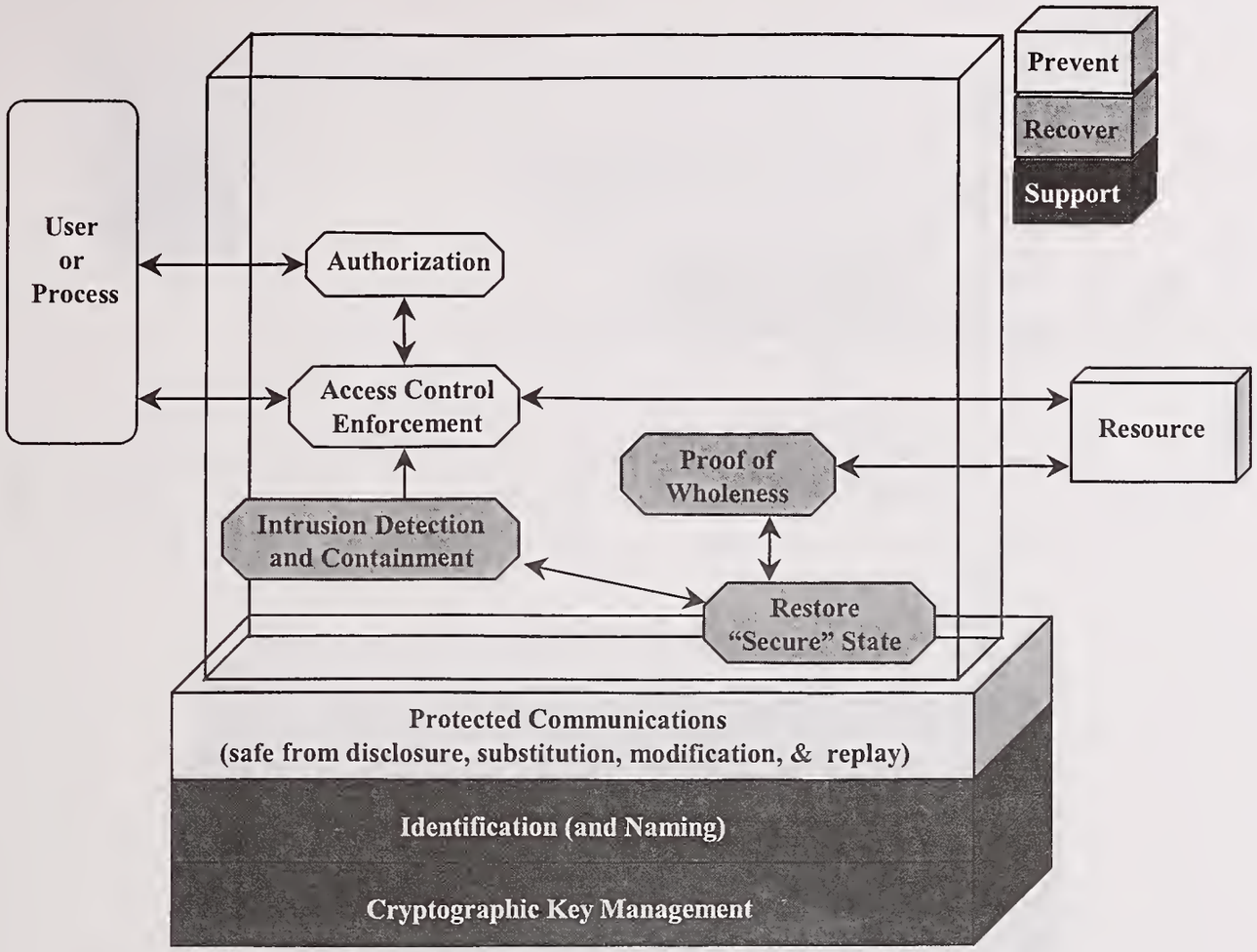


Figure 3.2-2 Primary Integrity Services

The services that provide for availability also provide for integrity. This is because maintaining or restoring integrity is an essential part of maintaining availability. Although availability is only concerned with changes (or deletions) that impact mission availability, the practical reality is that the applicable security mechanisms do not differentiate between purposes for the unauthorized access nor between impacts of loss of wholeness.

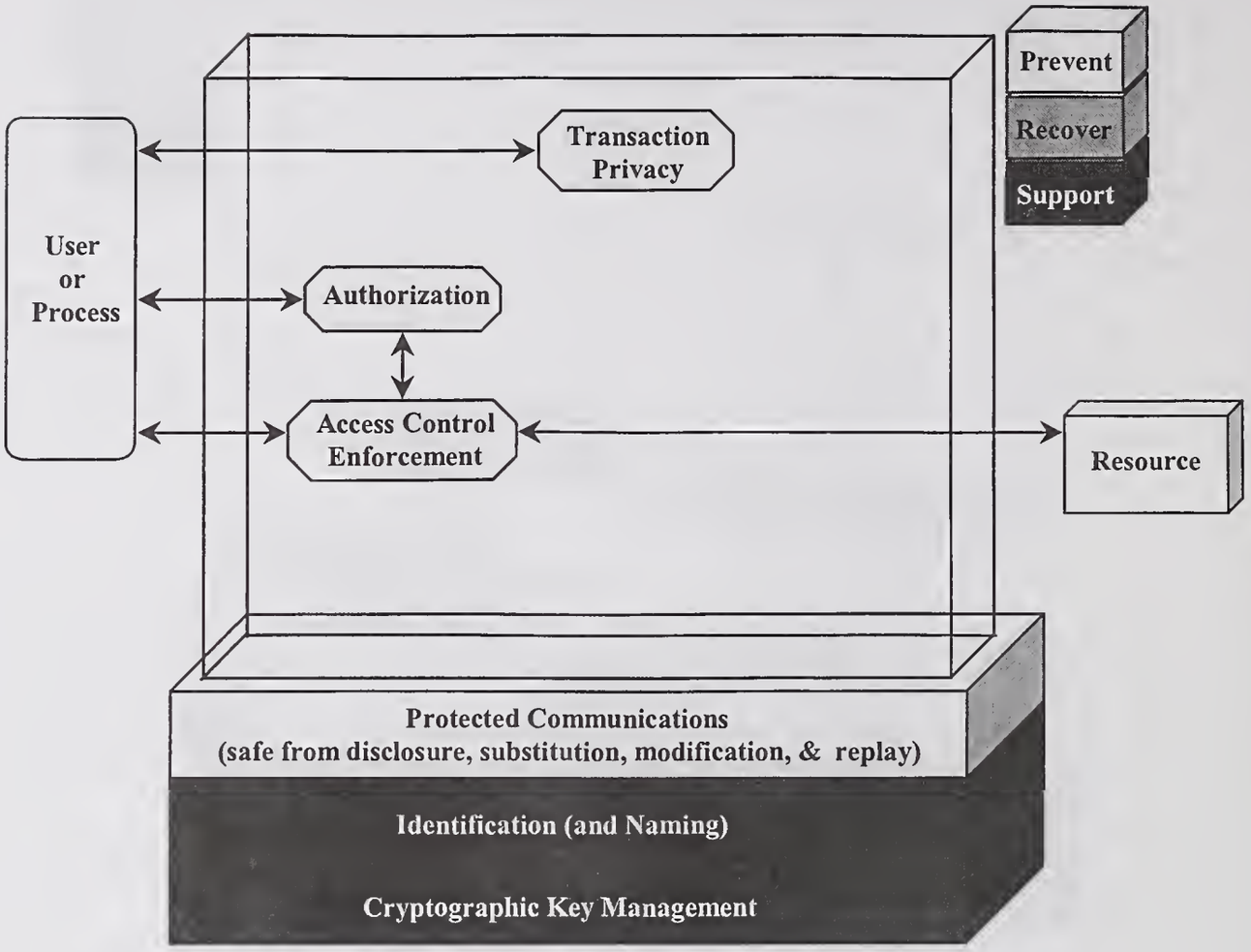


Figure 3.2-3 Primary Confidentiality Services

Once lost, confidentiality cannot be restored. Therefore, the detection and recovery services that can play an important role in maintaining availability and integrity do not apply to confidentiality. The protection of communications from disclosure, the enforcement of authorized read accesses, and the capability for privacy provide for confidentiality.

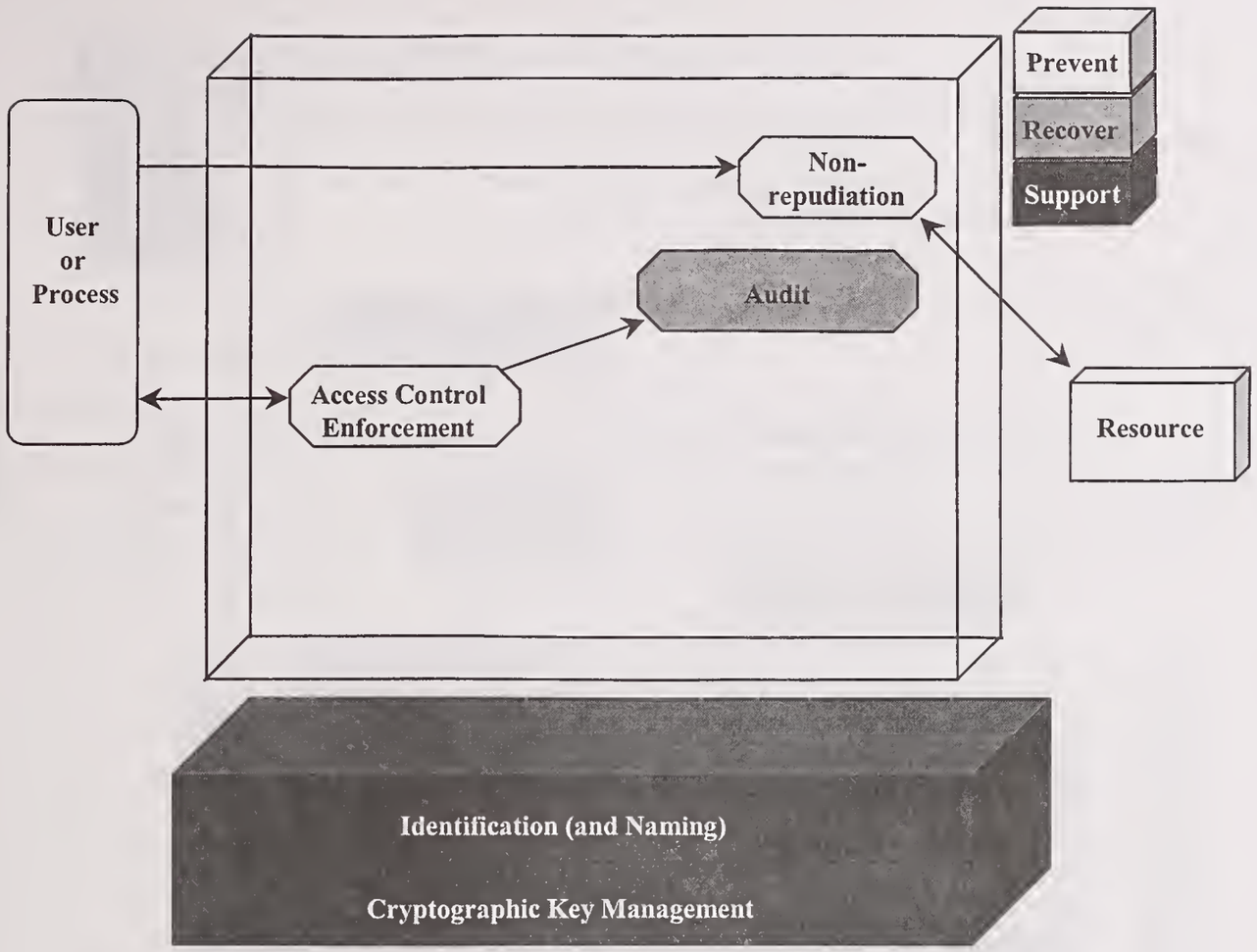


Figure 3.2-4 Primary Accountability Services

Maintaining accountability for user actions is performed primarily by the audit and non-repudiation services. Access control enforcement is also included as the primary generator of records of user actions.

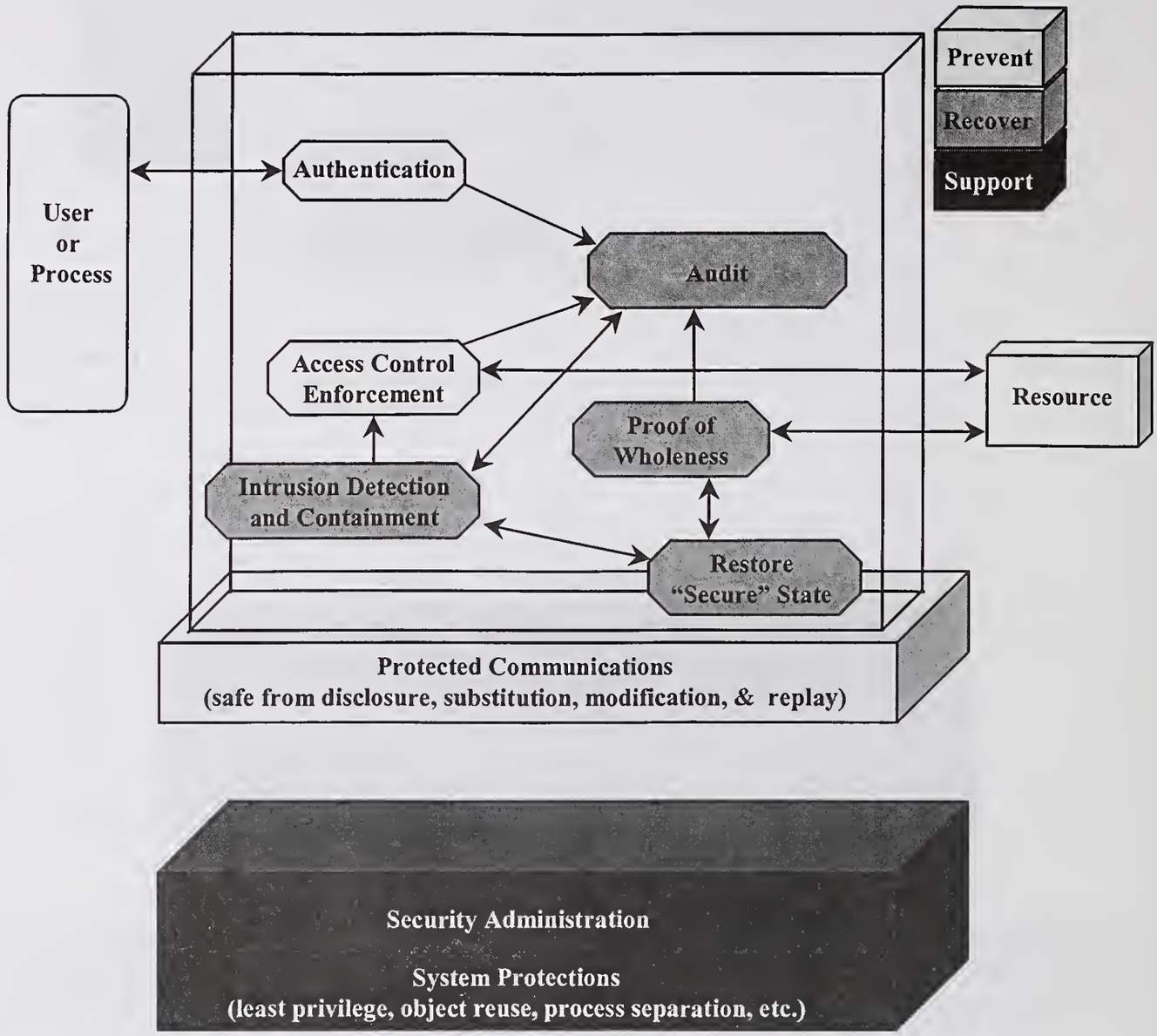


Figure 3.2-5 Primary Assurance Services

Assurance is grounds for confidence that the security objectives are met and, as indicated in section 2.0, encompasses both correct and sufficient security capabilities. This requires consideration of both "what" is provided and "how" it is provided (the architecture, design, and implementation). Also, as shown in the following section 4.1, assurance spans the system both logically and physically. Clearly assurance is pervasive and can be viewed from several perspectives. From the perspective of specific security services, assurance is most impacted by those services that directly impact the correct, on-going security capabilities of the system. In this regard the nature of the authentication being performed and the strength of the access control enforcement capability are extremely important. Additionally, the presence of an effective restoration capability can provide significant grounds for confidence. The audit service can be of great benefit in achieving assurance if used effectively and with recognition for its weaknesses. Finally, good security administration and system protections are essential to an objective basis for confidence in the security capabilities of a system.

4.0 Implementing Security Objectives – Distributed Systems

This section describes the following aspects of distributed systems:

- Security services distributed physically and logically
- Security domains
- Network views

4.1 Distributed Security Services

Figure 4-1 depicts the distributed security services and how services rest upon other services because they are logically and physically distributed across the network. Additionally, the figure shows that all services ultimately depend on operating system mechanisms, that system assurance is a key element "surrounding" the entire capability, and that system management is another important aspect of an effective security capability.

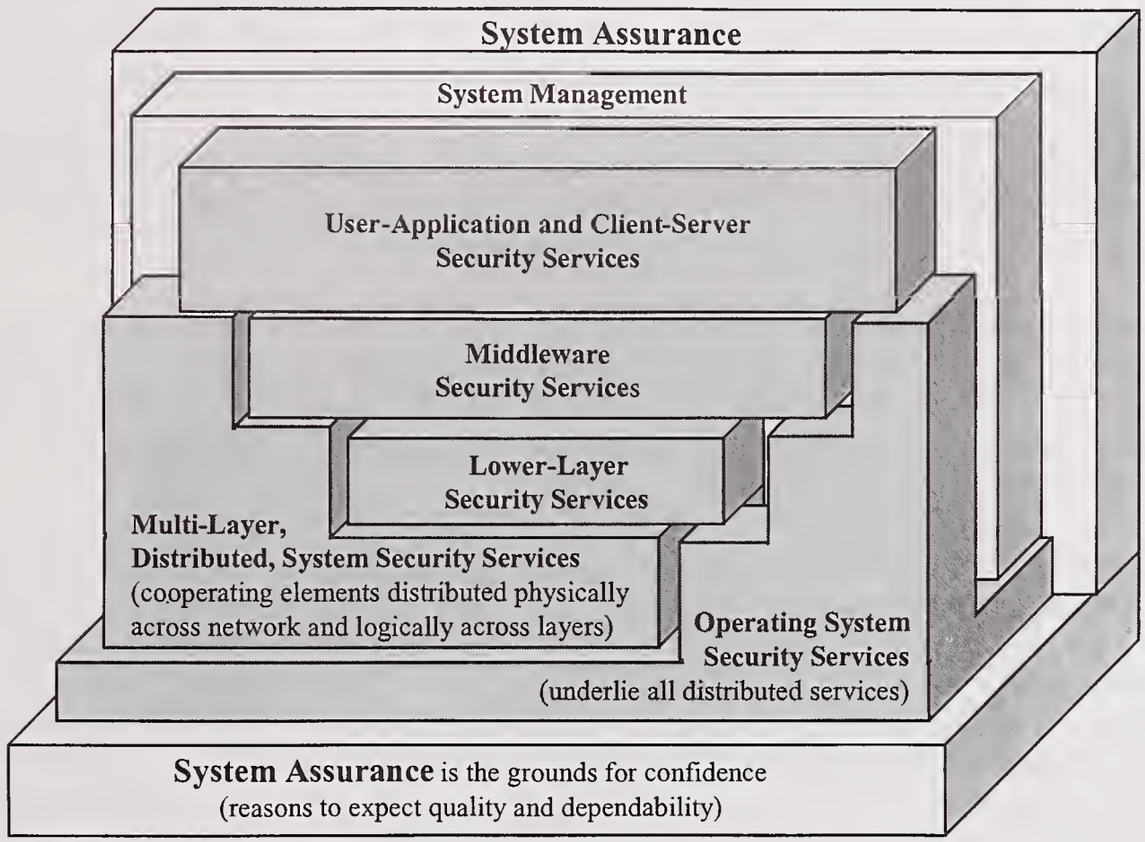


Figure 4.1-1 Distributed Security Services

Distributed security services depend on the foundations of system assurance and operating system security services.

a. System assurance. Assurance is "grounds for confidence that an entity meets its security objectives" [1]. Assurance can also be described as the system characteristic enabling confidence that the system fulfills its intended purpose. A secure system implementation must be of sufficient quality to provide confidence in the correct operation of security mechanisms and in the system's resistance to deliberate or unintentional penetration. Technology has been developed to produce and measure the assurance of information systems. System assurance can be increased by:

- Applying less complex technical solutions
- Using more trustworthy components
- Architecting to limit the impact of penetrations, both by limiting the extent of a vulnerability or by implementing detection and recovery capabilities
- Integrating technology in the context of the operational environment
- Taking advantage of non-technical countermeasures.

As depicted in Figure 4.1-1, system assurance both supports the architecture and spans it.

b. Operating system security services. Whenever such underlying services exist, system security ultimately depends on the underlying operating system services and mechanisms. If these underlying supports are weak, then security can be bypassed or subverted. System security can be no stronger than the underlying operating system. The graphic depicts a separate OS security "layer" to highlight this essential concept.

While some services reside in a particular logical level of the system hierarchy, many are implemented via mechanisms that span the system both physically and logically. This is depicted in Figure 4.1-1 by the logical levels of Application/Client-Server, Middleware, and lower layers. Each layer can depend on capabilities supplied by lower layers or, as shown, directly on operating system mechanisms.

Additionally, the figure shows that some distributed services do not exist at any one level, but are implemented by cooperating mechanisms at several levels. Common examples of distributed services are identification and authentication (I&A). The user interface, typically part of application level software (for example a Telnet client), must interact with the user to obtain the necessary information. The information must then be passed to a process that will determine whether the supplied data is correct. This process is likely to be running at the operating system level, or it might be at the presentation, session, or even network levels of the Organization for International Standardization (ISO) open system interconnect (OSI) model [3,4]. It is not uncommon for the information to be collected on one machine and transmitted across the network to another machine (a network authentication server for example). This I&A example with a network authentication server results in the security services being physically distributed across at least two machines and requiring the cooperative efforts of mechanisms residing at all seven levels of the OSI.

4.2 Security Domains

A foundation for IT security is the concept of security domains and enforcement of data and process flow restrictions within and between these domains.

A domain is a set of active entities (person, process, or device), their data objects, and a common security policy.

Domains can be logical as well as physical; dividing an organization's computing enterprise into domains is analogous to building fences (various types of security barriers), placing gates within the fences (e.g., firewalls, gateways, and internal process separation), and assigning guards to control traffic through the gates (technical and procedural security services).

Domains are defined using factors that include one or more of the following:

- Physical (e.g., building, campus, region, etc.)
- Business process (e.g., personnel, finance, etc.)
- Security mechanisms (e.g., Microsoft NT domain, Sun Network Information System (NIS), etc.)

The key elements to be addressed in defining domains are flexibility, tailored protection, domain interrelationships, and the use of multiple perspectives to determine what is important in information technology security.

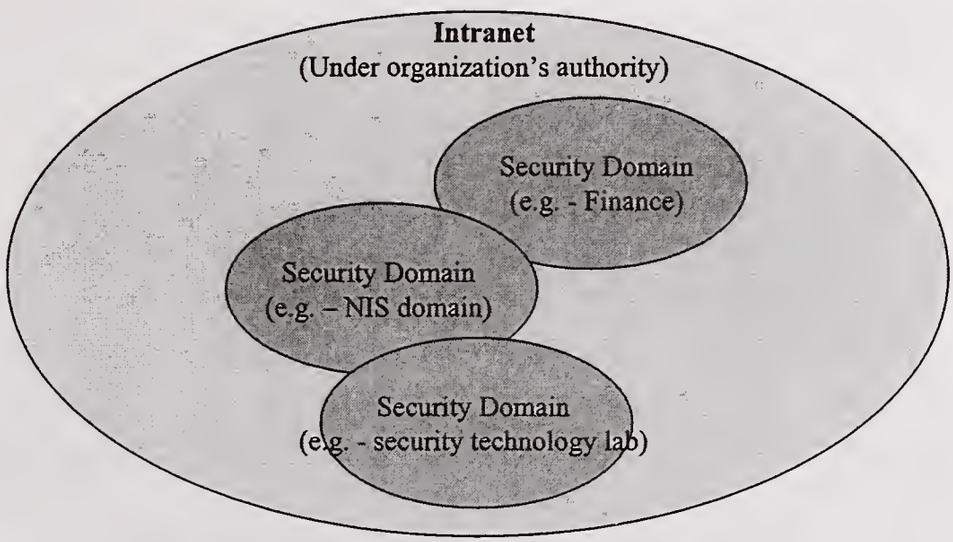


Figure 4.2-1 Overlapping Security Domains

4.3 Network Views

Distributed Intranets

An organization's intranet is typically dispersed physically and interconnected by circuits that are frequently not controlled by the organization. This is depicted in Figure 4.3-1.

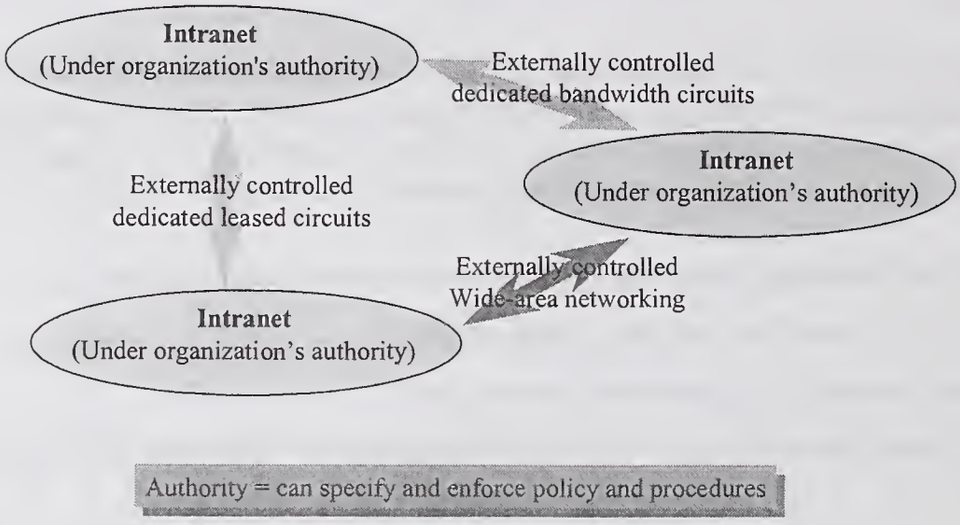


Figure 4.3-1 Distributed Intranet

Compartmentalizing the Intranet

Internally, an organization should consider compartmenting its intranet in a manner analogous to the watertight doors on a ship. This supports the enforcement of organizational policies and the limitation of damage in the event of a security breach. Figure 4.3-2 illustrates this concept.

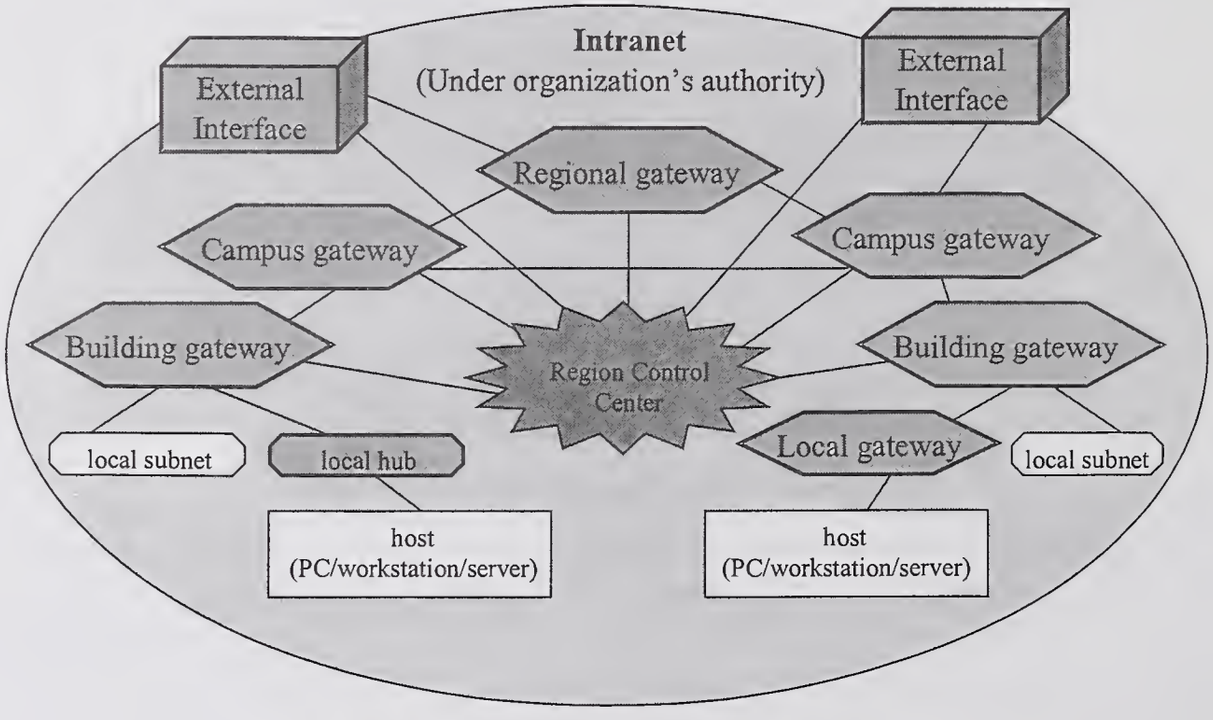


Figure 4.3-2 Compartmentalized Intranet

"Inside" versus "Outside"

"External" is no longer easy to determine. Distinctions can be made between transactions that are truly from "outside" and those that are the equivalent of being internal. As shown in Figure 4.3-3, the use of end-to-end encrypted paths is a possible solution for the latter.

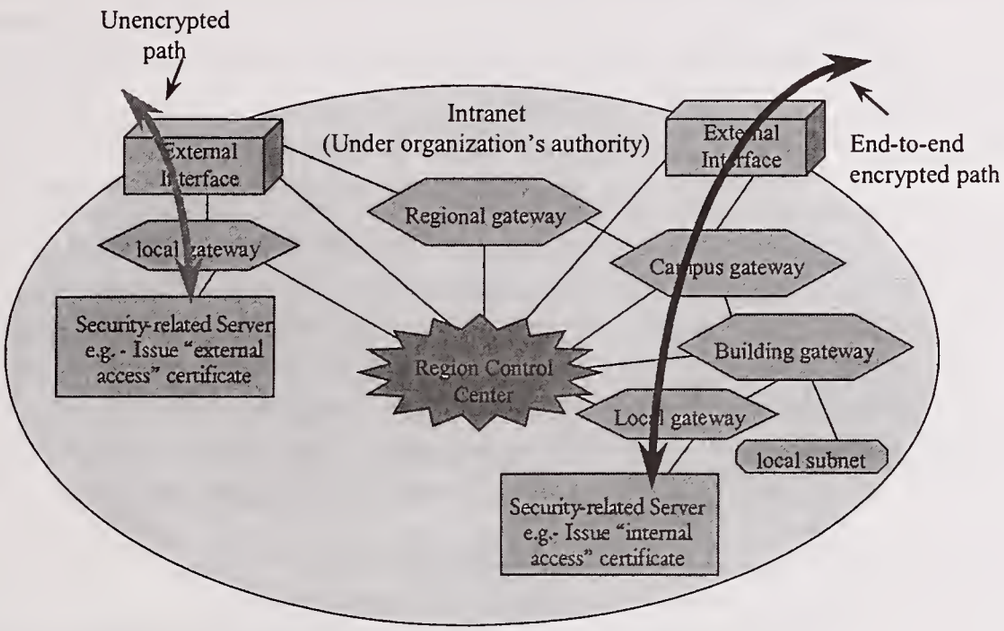


Figure 4.3-3 "External" Transactions

Detect and Contain

The ability to detect and to respond to a security breach is an essential part of an effective information technology security capability. This can be achieved by incorporating detection, analysis, and response components into the organization's intranet, as depicted in Figure 4.3-4.

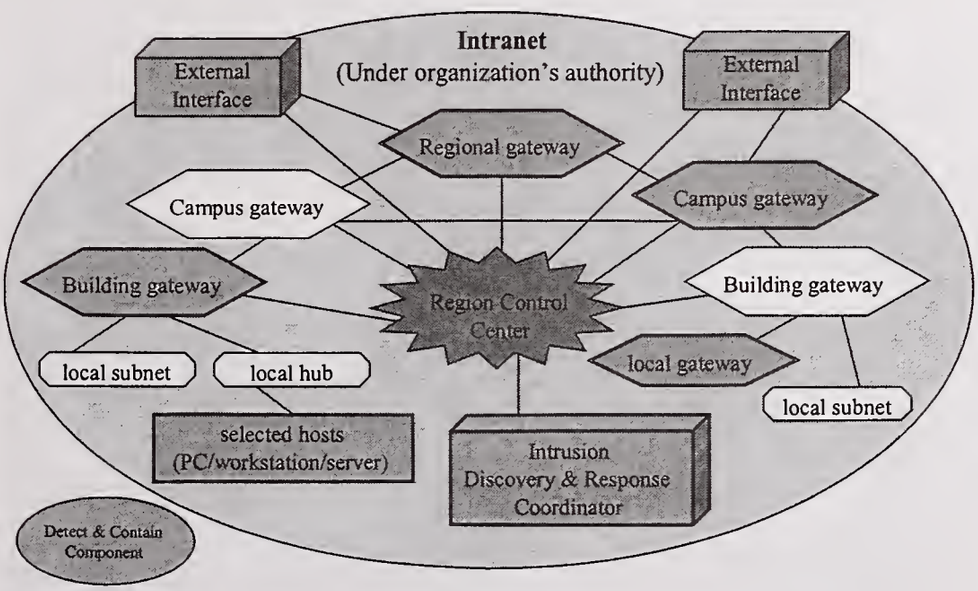


Figure 4.3-4 Detect and Contain

5.0 Risk Management

This section gives an overview of risk management for the purpose of highlighting where technology capabilities are best applied in mitigating risk. As indicated in the glossary, the following definitions are used:

Vulnerability	A weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.
Threat-source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.
Threat	The potential for a "threat source" to exploit (intentional) or trigger (accidental) a specific vulnerability.
Risk	The net mission/business impact (probability of occurrence combined with impact) from a particular threat source exploiting, or triggering, a particular information technology vulnerability. IT related-risks arise from legal liability or mission/business loss due to: – Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. – Non-malicious errors and omissions. – IT disruptions due to natural or man-made disasters. – Failure to exercise due care and diligence in IT implementation and operation.

Figure 5-1 shows where risk mitigation is accomplished in the face of intentional "attacks." The term "attack" is placed in quotation marks because the issue is "intentional," not malicious. It is relatively common for security to sometimes be intentionally "attacked" for non-malicious purposes such as "just getting the job done."

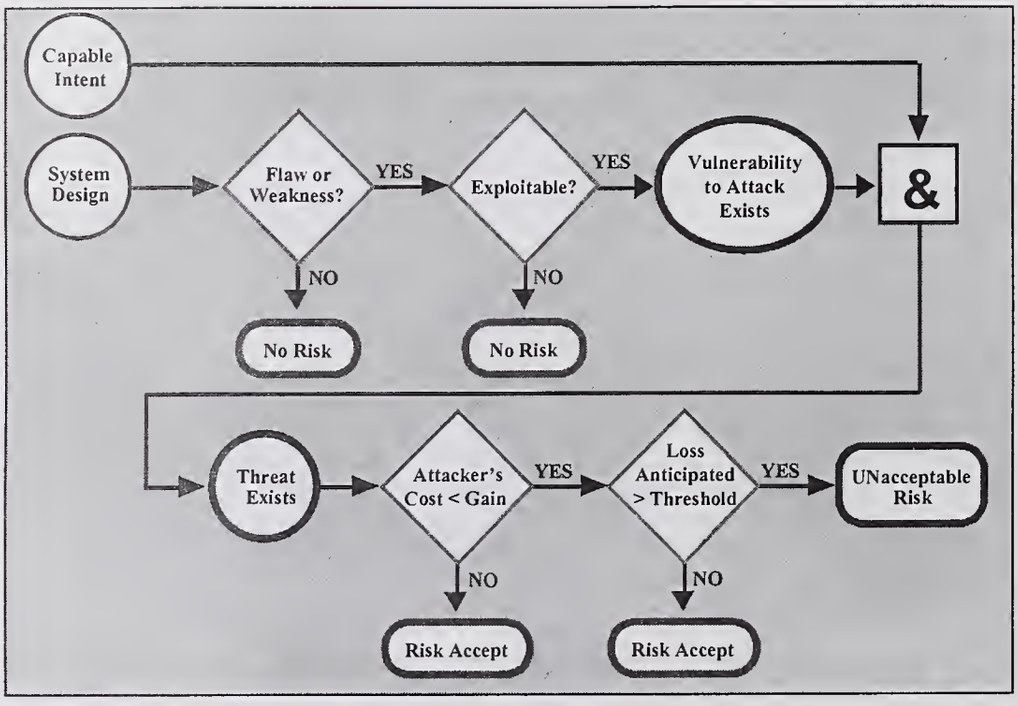


Figure 5-1 Basics of Risk Mitigation - "Attacks"

The mitigation of risk from attack by technical means can be accomplished at the following points:

- Flaw exists. –**Remedy:** Implement assurance techniques to reduce the likelihood of a flaw.
- Flaw is exploitable. –**Remedy:** Apply layered protections and architectural designs to prevent exploitability.
- Attacker's cost is less than gain –**Remedy:** Apply protections to increase attacker's cost (note that non-technical choices such as limiting what is processed can significantly reduce attacker's gain)
- Loss is too great. –**Remedy:** Apply design principles, architectural designs, and technical protections to limit extent of attack, thereby reducing loss. (Again, note that non-technical choices such as limiting what is processed may provide the most effective risk mitigation.)

Figure 5-2 shows how risk mitigation is applied for risks arising from system errors and from user actions not intended to violate security policy. For these situations the mitigation of risk is very similar:

- Flaw exists. –**Remedy:** Implement assurance techniques to reduce the likelihood of a flaw.
- Flaw is exploitable. –**Remedy:** Apply layered protections and architectural designs to prevent exploitability.
- Since the security breach is not the result of an explicit decision, there is no consideration of cost to an attacker.
- Loss is too great. – **Remedy:** Apply design principles, architectural designs, and technical protections to limit the extent of a security breach, thereby reducing loss.

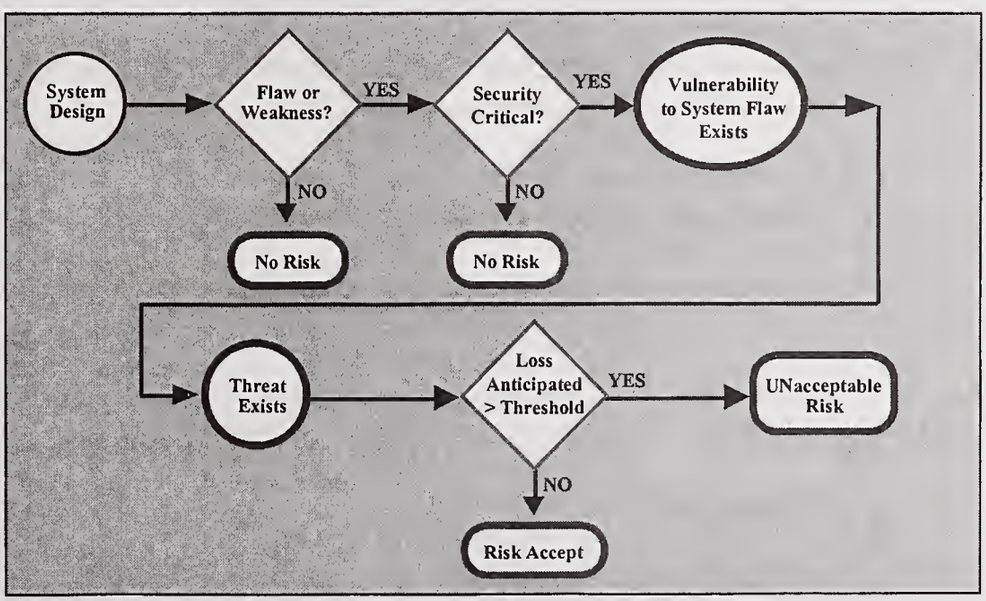


Figure 5-2 Basics of Risk Mitigation - Errors/Mistakes

6.0 Definitions

TERM	DEFINITION
access control	Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.
accountability	The security objective that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
assurance	Grounds for confidence that the other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
authorization	The granting or denying of access rights to a user, program, or process.
availability	The security objective that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.
confidentiality	The security objective that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
computing security methods	Computing security methods are security safeguards implemented within the IT, using the networking, hardware, software, and firmware of the IT. This includes (1) the hardware, firmware, and software that implements security functionality and (2) the design, implementation, and verification techniques used to ensure that system assurance requirements are satisfied.
data integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
data origin authentication	The verification that the source of data received is as claimed.
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations.
domain	See "security domain."
entity	Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

integrity	The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
identity	Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.
identity-based security policy	A security policy based on the identities and/or attributes of the object (system resource) being accessed and of the subject (user, group of users, process, or device) requesting access.
IT-related risk	The net mission/business impact (probability of occurrence combined with impact) from a particular threat source exploiting, or triggering, a particular information technology vulnerability. IT related-risks arise from legal liability or mission/business loss due to: 1. Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. 2. Non-malicious errors and omissions. 3. IT disruptions due to natural or man-made disasters. 4. Failure to exercise due care and diligence in the implementation and operation of the IT.
IT Security Architecture	A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.
IT security objective	See "security objectives."
non-computing security methods	Non-computing methods are security safeguards which do not use the hardware, software, and firmware of the IT. Non-computing methods include physical security (controlling physical access to computing resources), personnel security, and procedural security.
object	A passive entity that contains or receives information. Note that access to an object potentially implies access to the information it contains.
reference monitor	The security engineering term for IT functionality that (1) controls all access, (2) cannot be by-passed, (3) is tamper-resistant, and (4) provides confidence that the other three items are true.
residual risk	The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat.
risk	Within this document, synonymous with "IT-related risk."

risk analysis	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
risk assessment	See "risk analysis."
risk management	The total process of identifying, controlling, and mitigating information technology related risks. It includes risk analysis; cost-benefit analysis; and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission/business and constraints due to policy, regulations, and laws.
rule-based security policy	A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes by the subjects requesting access.
security	Security is a system property. Security is much more than a set of functions and mechanisms. Information technology security is a system characteristic as well as a set of mechanisms which span the system both logically and physically.
security domain	A set of subjects, their information objects, and a common security policy.
security goal	The IT security goal is to enable an organization to meet all mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners, and its customers.
security policy	The statement of required protection of the information objects.
security objectives	The five security objectives are integrity, availability, confidentiality, accountability, and assurance.
subject	An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state.
system integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
threat	The potential for a "threat source" (defined below) to exploit (intentional) or trigger (accidental) a specific vulnerability.
threat source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.
threat analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
traffic analysis	The inference of information from observation of traffic flows (presence, absence, amount, direction, and frequency).

traffic flow confidentiality	A confidentiality service to protect against traffic analysis.
vulnerability	A weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

APPENDIX A: References

1. _____; *Common Criteria for Information Technology Security Evaluation* (CC), Version 2.1, August 1999.
2. Stoneburner, Gary; *Developing a Commercial Security Architecture*, tutorial presented at the 11th Computer Security Applications Conference, New Orleans, LA, December 1995.
3. _____; *Open Systems Interconnect Reference Model*, ISO 7498, Organization for International Standardization (ISO).
4. Shipman, Stephen; *Mr. Shipman's Network Primer*, Chapter 1 "The OSI Model," http://personal.hartfordschools.org/~stephen/library/network_primer/ch01.html

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in metrology and related fields of physical science, engineering, applied mathematics, statistics, biotechnology, and information technology. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Institute of Physics (AIP). Subscription orders and renewals are available from AIP, P.O. Box 503284, St. Louis, MO 63150-3284.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency or Internal Reports (NISTIR)—The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). In general, initial distribution is handled by the sponsor; public distribution is handled by sales through the National Technical Information Service, Springfield, VA 22161, in hard copy, electronic media, or microfiche form. NISTIR's may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

U.S. Department of Commerce
National Institute of Standards
and Technology
Gaithersburg, MD 20899–0001