Chapter 4
Technical Security Countermeasures

The authors of the Information Assurance Technical Framework (IATF) recognize the importance of using both technical and nontechnical countermeasures in formulating an effective overall security solution to address attacks at all layers of the information infrastructure. This chapter of the IATF discusses principles for determining appropriate technical security countermeasures. It includes information on attacks, important security services, robustness strategy, the interoperability framework, and the Key Management Infrastructure (KMI)/Public Key Infrastructure (PKI). It also provides background for the detailed technical discussions contained in later sections of the IATF.

4.1 Introduction

Adversaries' primary goals fall into three general categories: unauthorized access, unauthorized modification, and denial of authorized access. Security solutions are implemented to prevent an adversary from successfully achieving these goals. This chapter discusses attacks, security services, and appropriate security technologies. By using the methodology described in Chapter 3, Information Systems Security Engineering Process, in conjunction with consideration of applicable attacks, security solutions can be proposed that support appropriate security services and objectives. Subsequently, proposed security solutions may be evaluated to determine if residual vulnerabilities exist, and a managed approach to mitigating risks may be proposed.

"Security services" are services that safeguard and secure information and information systems. Access control, confidentiality, integrity, availability, and nonrepudiation are the five primary areas of security service. These services are provided by incorporating security mechanisms, e.g., encryption, identification, authentication, access control, security management, and trust technology, into the information system to form a barrier to attack. This chapter presents an overview of each service, a breakdown of its various elements, and a detailed look at the security mechanisms that support it.

Three additional topics, robustness, interoperability, and KMI/PKI, should be considered in selecting security countermeasures. The robustness strategy provides the philosophy behind, and initial guidance for, selection of the strength of security mechanisms and the security assurance provisions that may be needed for a particular value of information and a potential threat level. This section defines the IATF strategy for measuring and assessing the need for various levels of robustness for technical, and selected nontechnical, security countermeasures. The robustness strategy is not intended to provide universal answers on needed strength or assurance, that is, it is not a "cookbook." The final selection of mechanisms, and the decision on the level of strength and assurance needed will be based on an Information Systems Security Engineering (ISSE) activity that addresses the situation of a specific user, mission, and environment.

The robustness of a security solution must be considered in relation to the system requirement for connectivity. Recognizing the growing need for connectivity, an interoperability framework provides a strategy for ensuring that security provisions (1) do not inhibit the connectivity that is otherwise available and (2) if necessary, maintain backward compatibility with existing system capabilities. The chapter continues with a discussion of KMI/PKI Considerations. It is important to consider the needs that a KMI/PKI creates and the demands it places on network users and operators in any potential network security solution.

This chapter provides a framework for considering these topics. Each aspect of the solutions addressed in this chapter should be considered in relation to the other aspects. For example, the robustness of a solution depends on the way the technology is implemented. Similarly, knowledge of the primary security services and the important security technologies will facilitate formation of effective security solutions. In addition, considering interoperability and KMI/PKI during the formulation of a security solution will help ensure the effectiveness of that solution.

4.2 Adversaries, Motivations, and Categories of Attacks

Adversaries come from various backgrounds and have a wide range of financial resources at their disposal. In this section a host of potential adversaries are examined, as are the questions. What produces an adversary? What are each adversary's motivations? What categories of attacks do the different types of each adversaries use? In addition to providing information on the various potential adversaries, this section provides examples of various types of the different categories providing a brief description of how each attack is performed and by whom.

This section also discusses the countermeasures that can be used against potential adversaries and different categories of attack.

4.2.1 Potential Adversaries

Typically adversaries are thought of as having malicious intent. However, in the context of system and information security and protection, it is also important to consider the threat posed by those without malicious intent. Table 4-1 shows examples of individuals and organizations in both of these categories.

Table 4-1. Potential Adversaries

Adversary	Description
Malicious	
Nation States	Well-organized and financed. Use foreign service agents to gather classified or critical information from countries viewed as hostile or as having economic, military, or political advantage.
Hackers	A group or individuals (e.g., hackers, phreakers, crackers, trashers, and pirates) who attack networks and systems seeking to exploit the vulnerabilities in operating systems or other flaws.
Terrorists/ Cyberterrorists	Individuals or groups operating domestically or internationally who represent various terrorist or extremist groups that use violence or the threat of violence to incite fear with the intention of coercing or intimidating governments or societies into succumbing to their demands.
Organized Crime	Coordinated criminal activities, including gambling, racketeering, narcotics trafficking, and many others. An organized and well-financed criminal organization.
Other Criminal Elements	Another facet of the criminal community, but one that is normally not very well organized or financed. Usually consists of very few individuals or of one individual acting alone.
International Press	Organizations that gather and distribute news, at times illegally, selling their services to both print and entertainment media. Involved in gathering information on everything and anyone at any given time.
Industrial Competitors	Foreign and domestic corporations operating in a competitive market and often engaged in the illegal gathering of information from competitors or foreign governments through corporate espionage.
Disgruntled Employees	Angry, dissatisfied individuals who can inflict harm on the local network or system. Can represent an insider threat depending on the current state of the individual's employment and access to the system.
Nonmalicious	
Careless or Poorly Trained Employees	Users who, through lack of training, lack of concern, or lack of attentiveness, pose a threat to information and information systems. This is another example of an insider threat or adversary.

4.2.1.1 Motivations

Individual motivations to "get inside" are many and varied. Persons with malicious intent who wish to achieve commercial, military, or personal gain are known as hackers [1]. At the opposite end of the spectrum are persons who compromise the network accidentally. Hackers range from the inexperienced professional, college student, or novice (e.g., Script Kiddy) to the highly technical and very capable (e.g., Uberhacker). Most hackers pride themselves on their skill and seek, not to destroy, but simply to gain access so that the computer or network can be used for later experimentation. Hackers often believe that by exposing a hole or "back-door" in a computer system, they are actually helping the organization to close the holes, providing a benefit to the Internet and a needed resource. Other hackers have less benign motives for getting inside.

Intelligence gathering, information operations, and psychological warfare are some motivations behind attempts to gain access. The following are some common reasons why an adversary might want to exploit a particular target:

- Gain access to classified or sensitive information. (Note: What is of high value to one person or organization might be of no value to another.)
- Track or monitor the target's operations (traffic analysis).
- Disrupt the target's operations.
- Steal money, products, or services.
- Obtain free use of resources (e.g., computing resources or free use of networks).
- Embarrass the target.
- Overcome the technical challenge of defeating security mechanisms.

From an information system standpoint, these motivations can express themselves in three basic goals: access to information, modification or destruction of information or system processes, or denial of access to information. In attacking an information processing system, an adversary accepts a certain amount of risk. This risk may be time dependent. The risk of loss to the adversary may far exceed the expected gain. Risk factors include—

- Revealing the adversary's ability to perform other types of attacks.
- Triggering responses that might prevent the success of a future attack, especially when the gain is much greater.
- Incurring penalties (e.g., fines, imprisonment, embarrassment).
- Endangering human life.

The level of risk that an adversary is willing to accept depends on the adversary's motivation.

4.2.2 Classes of Attack

Chapter 1, Introduction, Table 1-1, Classes of Attack, defines the five categories of system attack. Figure 4-1 shows each class of attack in relation to the information infrastructure. Each attack has unique characteristics that should be considered in defining and implementing countermeasures. This section provides an overview of each class of attack, with specific examples of attacks for each class. Several classes of network-based attacks are considered in the following discussion.

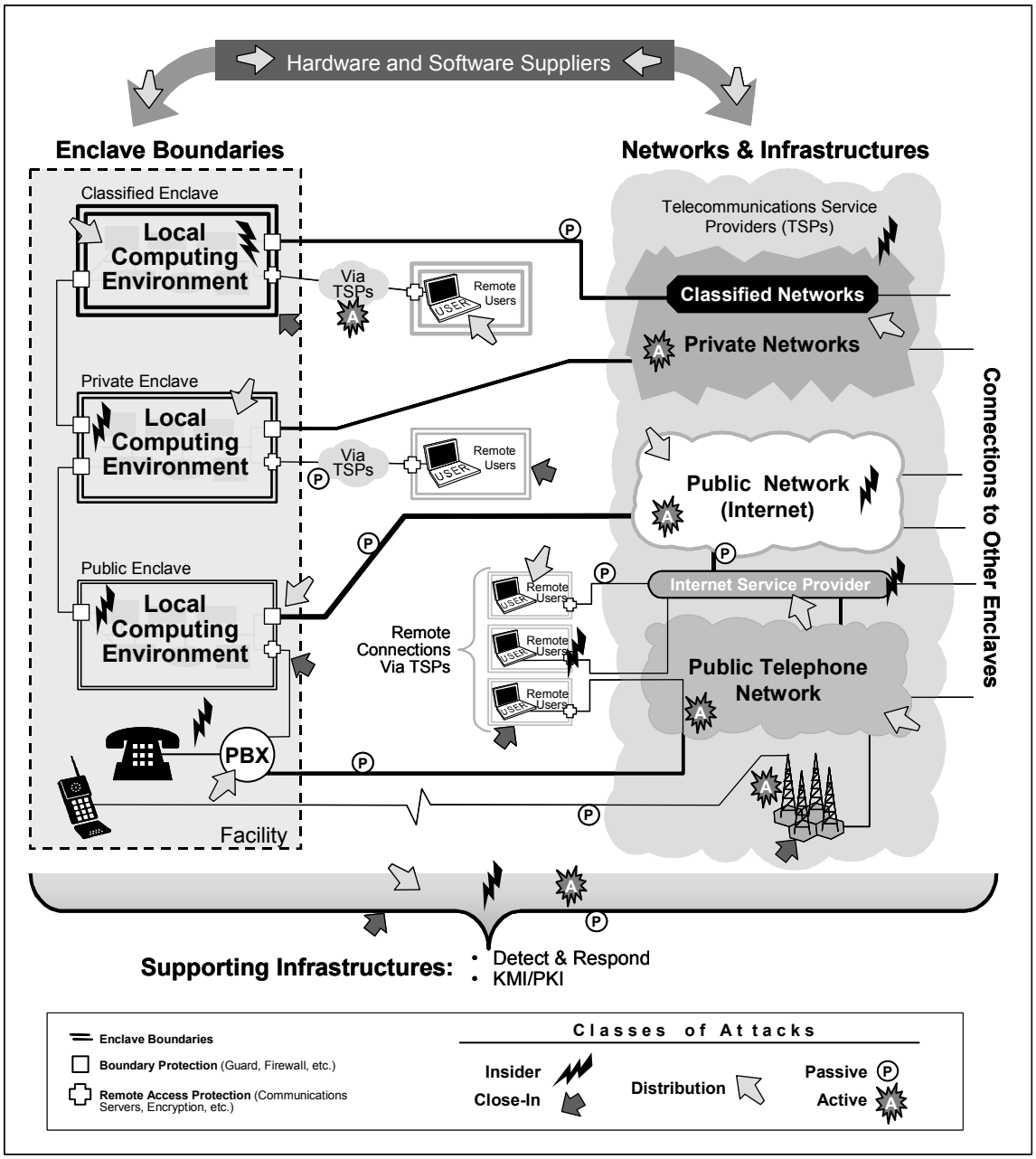

Figure 4-1. Categories of Attacks Against Networked Systems

4.2.2.1 Passive Attacks

These attacks involve passive monitoring of communications sent over public media (e.g., radio, satellite, microwave, and public switched networks). Countermeasures used against passive attacks include virtual private networks (VPN), cryptographically protected networks, and protected distribution networks (e.g., physically protected or alarmed wireline distribution network). Table 4-2 provides examples of attacks characteristic of this class.

Table 4-2. Examples of Passive Attacks

Attack	Description
Monitoring Plaintext	An attacker monitoring the network could capture user or enclave data that is not otherwise protected from disclosure.
Decrypting Weakly Encrypted Traffic	Cryptoanalytic capability is available in the public domain, as witnessed by the June 1997 collaborative breaking of the 56-bit-strength Data Encryption Standard. While the near-term potential for attack on large volumes of traffic is questionable given the number of machines and hours involved, breaking of DES does show the vulnerability of any single transaction.
Password Sniffing	This type of attack involves use of protocol analyzers to capture passwords for unauthorized reuse.
Traffic Analysis	Observation of external traffic patterns can give critical information to adversaries even without decryption of the underlying information. For example, extension of a network into a tactical theater of operations may indicate the imminence of offensive operations thereby removing the element of surprise.

4.2.2.2 Active Attacks

Active attacks include attempts to circumvent or break security features, introduce malicious code (such as computer viruses), and subvert data or system integrity. Typical countermeasures include strong enclave boundary protection (e.g., firewalls and guards), access control based on authenticated identities (ID) for network management interactions, protected remote access, quality security administration, automated virus detection tools, auditing, and intrusion detection. Table 4-3 provides examples of attacks characteristic of this class.

Table 4-3. Examples of Active Attacks

Attack	Description
Modifying Data in Transit	In the financial community, it would be disastrous if electronic transactions could be modified to change the amount of the transaction or redirect the transaction to another account.
Replaying (Insertion of Data)	Reinsertion of previous messages could delay timely actions. Bellovin shows how the ability to splice messages together can be used to change information in transit.
Session Hijacking	This attack involves unauthorized use of an established communications session.
Masquerading as Authorized User/Server	This attack involves an attacker's identifying himself or herself as someone else, thereby gaining unauthorized access to resources and information. An attacker first gets user or administrator information by employing sniffers or other means, then uses that information to log in as an authorized user. This class of attack also includes use of rogue servers to obtain sensitive information after establishing what is believed to be a trusted service relationship with the unsuspecting user.

Attack	Description
Exploiting System-Application and Operating System Software	An attacker exploits vulnerabilities in software that runs with system privileges. Well-known attacks involve sendmail and X-Windows server vulnerabilities. Recently, there has been an increase in alerts regarding Windows 95 and Windows NT vulnerabilities. New vulnerabilities for various software and hardware platforms are discovered almost daily. Attacks, vulnerabilities, and patches are reported through the various computer emergency response alerts and bulletins.
Exploiting Host or Network Trust	An attacker exploits transitive trust by manipulating files that facilitate the provision of services on virtual/remote machines. Well-known attacks involve UNIX commands, .rhosts and .rlogin, which facilitate workstation's sharing of files and services across an enterprise network.
Exploiting Data Execution	An attacker can get the user to execute malicious code by including the code in seemingly innocent software or e-mail for downloading. The malicious code might be used to destroy or modify files, especially files that contain privilege parameters or values. Well-known attacks have involved PostScript, Active-X, and MS Word macro viruses.
Inserting and Exploiting Malicious Code (Trojan horse, trap door, virus, worm)	An attacker can gain execution access to a user's system commands through one of the vulnerabilities previously identified and use that access to accomplish his or her objectives. This could include implanting software to be executed based on the occurrence of some future event. Hacker tools are available on the Internet. These tools have turnkey capabilities, including an insertion script, root grabbing, Ethernet sniffing, and track hiding to mask the presence of a hacker.
Exploiting Protocols or Infrastructure Bugs	An attacker exploits weaknesses in protocols to spoof users or reroute traffic. Well-known attacks of this type include spoofing domain name servers to gain unauthorized remote login, and bombing using Internet Control Message Protocol (ICMP) to knock a machine off the air. Other well-known attacks are source routing to impersonate a trusted host source, Transmission Control Protocol (TCP) sequence guessing to gain access, and TCP splicing to hijack a legitimate connection. Malicious code can exfiltrate information through a lower level tunnel within a VPN. At least one published paper points out potential security concerns revolving around use of Internet Protocol Security default security mechanisms. In addition, Bellovin points out occasions on which the integrity functions of Data Encryption Standard in Cipher Block Chaining mode can be circumvented, with the right applications, by splicing of packets.
Denial of Service	An attacker has many alternatives in this category, including ICMP bombs to effectively get a router off the network, flooding the network with garbage packets, and flooding mail hubs with junk mail.

4.2.2.3 Close-In Attacks

Close-in attacks are attacks in which an unauthorized individual gains close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. Gaining such proximity is accomplished through surreptitious entry, open access, or both. Table 4-4 provides examples of specific attacks characteristic of this class.

Table 4-4. Examples of Close-In Attacks

Attack	Description
Modification of Data/Information Gathering	This results from an individual gaining physical access to the local system and modifying or stealing information, such as, Internet Protocol addresses, login ID schemes, and passwords.
System Tampering	This type of attack results from an individual in close proximity gaining access to and tampering with the system (e.g., bugging, degrading).
Physical Destruction	This type of attack results from an individual in close proximity gaining physical access, and causing the physical destruction of a local system.

4.2.2.4 Insider Attacks

Insider attacks are performed by a person who either is authorized to be within the physical boundaries of the information security processing system or has direct access to the information security processing system. There are two types of insider attacks: malicious and nonmalicious (the latter involving carelessness or ignorance of the user). The nonmalicious case is considered an attack because of the security consequences of the user's action.

- **Malicious Insider Attacks**. Federal Bureau of Investigation (FBI) estimates indicate that 80 percent of attacks and intrusions come from within organizations (see http://www.cs.purdue.edu/coast/intrusion-detection/) [3]. An insider knows the layout of the system, where the valuable data is, and what security precautions are in place. Insider attacks originate from within the enclave and are often the most difficult to detect and to defend against.

  Sources of insider attacks can include uncleared cleaning crews (with after-hours physical access), authorized (privileged to login) system users, and system administrators with malicious intent. Often it is difficult to prevent individuals who have legitimate access to a system from accessing into more private areas to which they do not have authorized access. Insider attacks may focus on compromise of data or access and can include modification of system protection measures. A malicious insider may use covert channels to signal private information outside of an otherwise protected network. However, there are many other avenues by which a malicious insider can damage an information system.

- **Nonmalicious Insider Attacks.** These attacks are caused by authorized persons who have no intent to cause damage to the information or to the information processing system but may unintentionally do so. The damage in this case is caused by lack of knowledge or by carelessness.

Typical countermeasures include security awareness and training; auditing and intrusion detection; security policy and enforcement; specialized access control for critical data, servers, local area networks (LAN), etc., implemented by trust technology in computer and network

elements; and a strong identification and authentication (I&A) capability. Table 4-5 contains examples of attacks characteristic of this class.

Table 4-5. Examples of Insider Attacks

Attack	Description
Malicious	
Modification of Data or Security Mechanisms	Insiders often have access to information due to commonality of shared networks. This access can, allow manipulation or destruction of information without authorization.
Establishment of Unauthorized Network Connections	This results when users with physical access to a classified network create an unauthorized connection to a lower classification level or lower sensitivity network. Typically this connection is in direct violation of the classified network's security policy or user directives and procedures.
Covert Channels	Covert channels are unauthorized communication paths used for transferring misappropriated information from the local enclave to a remote site.
Physical Damage/ Destruction	This is intentional damage to, or destruction of, a local system resulting from the physical access afforded the insider.
Nonmalicious	
Modification of Data	This type of attack results when insiders, either through lack of training, lack of concern, or lack of attentiveness, modify or destroy information located on the system.
Physical Damage/ Destruction	This type of attack is listed under malicious as well. As a nonmalicious attack, it can result from carelessness on the part of the insider, for instance, failure to obey posted guidance and regulations, resulting in accidental damage to or destruction of, a system.

4.2.2.5 Distribution Attacks

The term "distribution attack" refers to the potential for malicious modification of hardware or software between the time of its production by a developer and its installation, or when it is in transit from one site to another. Vulnerability at the factory can be minimized by strong in-process configuration control. Vulnerability to distribution attacks can be addressed by use of controlled distribution or by signed software and access control that is verified at the final user site. Table 4-6 contains examples of attacks characteristic of this class.

Table 4-6. Examples of Distribution Attacks

Attack	Description
Modification of Software/Hardware at Manufacturer's Facility	These attacks can involve modifying of the configuration of software or hardware while it is cycling through the production process. Countermeasures for attacks during this phase include rigid integrity controls, including high-assurance configuration control and cryptographic signatures on tested software products.
Modification of Software/Hardware during Distribution	These attacks can involve modifying of the configuration of software or hardware during its distribution (e.g., embedding of listening devices during shipment). Countermeasures for attacks during this phase include use of tamper detection technologies during packaging, use of authorized couriers and approved carriers, and use of blind-buy techniques.

4.3 Primary Security Services

The IATF guidance incorporates five primary security services areas: access control, confidentiality, integrity, availability, and nonrepudiation. The division of network security principles into standard security service categories is convenient for this description. The categories presented below roughly coincide with the "basic security services" identified in the 1990 Recommendation X.800, "Security Architecture for Open Systems Interconnection for Consultative Committee for International Telephone and Telegraph (CCITT) Applications" (which is technically aligned with International Organization for Standardization [ISO] 7498-2, "Information Processing Systems Open Systems Interconnection, Basic Reference Model," Part 2: Security Architecture), and more recently, the ISO/International Engineering Consortium (IEC) 10181 series, Parts 1-7.

In practice, none of these security services is isolated from or independent of the other services. Each service interacts with and depends on the others. For example, access control is of limited value unless preceded by some type of authorization process. One cannot protect a system or information from unauthorized entities if one cannot determine whether that entity one is communicating with is authorized. In actual implementations, lines between the security services also are blurred by the use of mechanisms that support more than one service.

Given these caveats, this section characterizes each service according to its basic functional elements and discusses the mechanisms that are available to implement the elements of that service. Where appropriate, considerations of the relative strengths of these mechanisms are also noted.

4.3.1 Access Control

In the context of network security, access control means limiting access to networked resources (hardware and software) and data (stored and communicated). The goal of access control is to

prevent the unauthorized use of these resources and the unauthorized disclosure or modification of data. Access control also includes resource control, for example, preventing logon to local workstation equipment or limiting use of dial-in modems. For the purposes of this discussion, network access control is not concerned with denying physical access (e.g., via locked rooms or tamperproof equipment).

Access control is applied to an entity based on an identity or an authorization. An identity may represent an actual user, a process with its own identity (e.g., a program making a remote access connection), or a number of users represented by single identity (e.g., role-based access control).

Access control mechanisms are most often used as a set of mechanisms, which may be used by other security services. Confidentiality, integrity, availability, and limiting use of network resources all depend on limiting the ability of an adversary to access an item or service.

The elements of access control can be categorized as follows:

- **I&A.** Establishing the identities of entities with some level of assurance (an authenticated identity).
- **Authorization.** Determining the access rights of an entity, also with some level of assurance.
- **Decision**. Comparing the rights (authorization) of an authenticated identity with the characteristics of a requested action to determine whether the request should be granted.
- **Enforcement.** Enforcement may involve a single decision to grant or deny or may entail periodic or continuous enforcement functions (continuous authentication).

The following subsections discuss these elements and provide examples of the mechanisms that are available to implement them.

4.3.1.1 I&A

I&A is a set of security services used in conjunction with most other security services. The first step of most security services is to determine the identities of one or more of the parties participating in an action. A trusted identity must be used for access control decisions and to provide nonrepudiation and accountability evidence. Knowing the identity of an entity and the existence of a peer relationship is also fundamental to establishing communication with confidentiality and integrity. If the identity of the peer in a secure communications path is not properly established, it leaves open the possibility that an unauthorized user (an adversary) could masquerade as an authorized user, exposing the data to disclosure or manipulation.

The process of determining an authentic identity is presented in the following subsections.

4.3.1.1.1 Assigning, Binding, and Representing

There must be a mechanism for providing some assurance in the assignment of an identity. The entity that assigns the ID must have a position with some level of trust (either implied or assured by a third entity common to both with a higher position or level of trust). These trusted entities must implement a process of identity-checking that protects against assignment of improper IDs. Examples include checking driver's licenses or verifying fingerprints. Assigning an ID is the equivalent of a registration process and can take place through an existing security mechanism with its own identity establishment mechanism.

An identity must be unique within the community that will be validating that identity. This requires implementation of a community wide authentication mechanism that provides a unique ID to each entity. The community needs to implement an authentication mechanism that provides for a unique identity for each entity. All potential entities must recognize and process an identity in this mechanism. This implies the mechanism must employ a standard format for representing identity.

Identities used for network access control can be assigned and represented by many different mechanisms:

- System administrators providing accounts and passwords for UNIX user names.
- Network administrators assigning Internet Protocol (IP) addresses to machines.
- Key distribution methods that distribute symmetric keys.
- Key distribution methods that distribute public/private key pairs.
- Certification authorities (CA) generating public key certificates containing distinguished names (DN).
- Security officers associating a set of fingerprints with a common name.

The assurance level attributed to an ID depends on the processes used to verify the correctness of that identity before it is issued, the trust instilled by the entity assigning the identity, and the strength of the binding between the entity and the identity. Verification may range from requesting a mother's maiden name over the telephone to checking driver's licenses or verifying fingerprints in person. Means of instilling trust in issuers include procedural mechanisms, such as a company's assigning system administrators; legal mechanisms, such as notaries; and technological mechanisms, such as certification paths in a certification hierarchy. Mechanisms for binding entities to IDs include signed X.509 certificates and password files associated with access control lists (ACL).

Strongly establishing identities for communicating entities is the first step in countering any attack that is predicated on adversaries representing themselves as someone or something that they are not (including masquerading and insider modification attacks).

4.3.1.1.2 Communicating and Authenticating

To authenticate an entity that is attempting to gain access, an identity must be associated with the access request and provided to the communicating peer. Along with an indication of identity, the authenticating peer must have the parameters (authentication information) needed to validate that identity. Authentication is implemented by user-to-host and peer-to-peer, and trusted third party (TTP) architectures as follows.

- **User-to-Host:** When a user logs onto a host (or workstation), the user must be identified and authenticated before access to the host or network is granted. This process requires a mechanism to authenticate a real person to a machine. The best methods of doing this involve multiple forms of authentication, such as password, physical token, and biometric verification (i.e., something you *know*, something you *have*, something you *are*).
- **Peer-to-Peer Authentication:** A peer-to-peer authentication architecture, sometimes referred to as mutual authentication protocol, involves the direct communication of authentication information between the communicating entities (e.g., peer-to-peer or client host-to-server). No other entities are required. This architecture is possible only if each entity in a security domain is able to obtain the authentication information of every communicating entity in the domain.
- **Trusted Third Party Authentication:** The architecture for TTP authentication uses a third entity, trusted by all entities, to provide authentication information. A TTP may provide authentication information in each instance of authentication, in real-time, or as a precursor to an exchange (such as a CA). The amount of trust given the third party must be evaluated. Methods of establishing and maintaining a level of trust in a TTP include certification practice statements that establish rules, processes, and procedures that a CA uses to ensure the integrity of the authentication process and use of secure protocols to interface with authentication servers.

  The mechanisms used for authenticating an identity can be categorized as simple or cryptographically based. Simple mechanisms may include identification based on IDs that are verified by asking the entity to communicate information that only the entity attempting access would know (e.g., a password and locally stored password file). Assurance comes from the local binding between the password and an identity. Another example of a simple authentication method is address-based authentication. Address-based mechanisms authenticate an identity based solely on assigned network addresses (e.g., IP address) of communicating peers. The system compares the IP address assignment of entities to determine the identity of the communicating entity.

  Cryptographically based mechanisms rely on the cryptographic processing of data within a defined protocol. Peers may share a common secret key (often stored in a hardware token) to process, or encrypt the exchange, in a challenge-response protocol. Other cryptographic mechanisms rely on public key cryptography alone, or on the binding between a public key and an identity provided by public key certificates. Examples of how an identity is authenticated in each cryptographic technique are provided below.

- **Identity Is a Locally Defined Name:** Identities of all potential communicating peers are stored locally in a trusted database that associates identities with their public keys. These public keys correspond to the private key used to sign a unique piece of data. Verifying a signature by using a stored public key authenticates an identity.
- **Identity Is the Defined Name.** From the valid X.509 certificate containing the public key that corresponds to the private key used to sign a unique piece of data. A valid X.509 certificate means that the complete certification path has been validated (including certificate revocation list (CRL) and compromised key list (CKL) checks and validity periods for all certificates) to a trusted root. X.509 certificates (of communicating peers or of the entities in certification paths) may be stored locally (cached), carried in the security association protocol, accessed as needed from an X.500 directory, or any combination of these three methods. Verifying a signature by using a valid public key authenticates an identity.

For all cryptographically based mechanisms, the strength of the mechanism lies partly in the strength of the cryptographic algorithms (including key size), partly in the security of any communications protocol, and in large part, in the protection provided to secret key material.

There are a number of mechanisms for implementing and distributing identity and authentication information. Some of these mechanisms are as follows:

- Names and passwords stored in a database local to the entity making the access control decision.
- IP addresses provided by a secure domain name server (DNS).
- Passwords generated locally based on time (one-time passwords).
- Symmetric keys stored in a local database.
- Public keys stored in a local database.
- Public key certificates provided by directories in response to queries.
- Authentication information carried in the communications protocols themselves.

The assurance level of the communication of identity and authentication information processes depends on whether that information needs protecting and how well it is protected. For example, passwords are sensitive because they can be used by anyone who knows them; they should therefore be encrypted for storage and transport. Certificates can be stored in unprotected directories or carried on unencrypted communications channels because they can only be used by the entity that holds the associated private key.

Note that identity information and the information used to authenticate that identity do not have to flow over the same communications path. A common example is name and password logins. Users are queried for a name and an associated password (the identity information) over the communications protocol. The authenticity of that name and password pair is established only

by checking a locally stored database (the information used to authenticate is provided by an off-line process).

There are entire infrastructures devoted to providing identities and the means of authenticating those identities. Examples of infrastructures supporting the determination of an authentic identity include the X.509 authentication framework, the Internet Engineering Task Force (IETF) PKI, the secure DNS initiatives, and the Simple Public Key Infrastructure (SPKI).

4.3.1.2 Authorization

Another important step in an access decision is determining the authorizations of one or more of the parties participating in a communication. These authorizations result in the granting of a set of privileges to an entity. Much like IDs, authorizations must be conveyed in a commonly understood format and must be presented or maintained with some level of confidence. The process of determining an authenticated set of authorizations generally consists of the same components as that for determining an authenticated identity. A strong mechanism for determining authorizations can prevent an attack in which an entity attempts to forge access rights.

The process of determining the authorizations of an entity consists of assigning authorizations, binding authorizations to an entity, representing those authorizations in a standard format, communicating those authorizations, and establishing the authenticity of the authorizations. These steps are discussed below.

4.3.1.2.1 Assigning, Binding, and Representing

As in assigning identity, the process that determines and assigns authorizations must evoke a level of trust. Responsibility for that process falls on roles such as CA, attribute authority, ACL administrator, and system administrator. Authorizations used for network access control can be assigned by—

- System administrators, who assign user names to groups.
- Data owners, who grant authorizations to read/write/execute files.
- Network administrators, who generate ACLs.
- X.500 CAs, who generate version 3 X.509 certificates containing extensions.
- Attribute authorities, who generate American National Standards Institute (ANSI) X9.57 attribute certificates.

4.3.1.2.2 Communicating and Authenticating

Communicating authorization information follows the same model as authentication information. The information may be predistributed and stored at each entity (e.g., ACL); it may be carried in the communications protocol; or it may be provided by a TTP (e.g., X.500 directory, Radius authentication servers). There are a number of models for distributing authorization information:

- ACLs stored local to the entity making the access control decision.
- X.500 directories deployed to provide X.509 certificates.
- X.500 directories deployed to provide attribute certificates.

Authenticity of authorization information is provided either by its trusted relationship with identity information (local binding) or because it is carried in cryptographically verifiable certificates.

The level of trust attributed to the third parties used for obtaining authorization information (either the parties who generated the authorizations initially or those that distribute them when needed) is always an issue. The cryptographic techniques invoked to prove the authenticity of X.509 certificates and to bind attribute certificates to identity certificates represent one attempt to ensure that trust.

4.3.1.3 Decision

The components discussed previously provide the information required to make an access control decision. They provide mechanisms for determining both the identity and the privilege set of a communicating entity. In practice, access decisions are usually based on an access control policy, commonly referred to in the classified arena as discretionary or mandatory policies. International standards do not use the "mandatory/discretionary" terminology, but instead use the terms Identity Based Access Control (IBAC), which bases decisions on an identity, or Rule-Based Access Control (RBAC), which checks an entity's authorizations against an established rule set. Within the scope of this discussion, IBAC and discretionary policies can be considered equivalent, and RBAC and mandatory policies can be considered equivalent. In either case, the function of an access control decision is to grant or deny requests for access.

An IBAC decision grants or denies a request based on the presence of an entity on an ACL. If an entity is on the ACL, access to the requested information or resource is permitted; otherwise, access is denied. IBAC requires an authenticated identity before granting any access.

An RBAC decision depends on policies that can be algorithmically expressed and thus implemented on a computer system. These policies are stated in a way that requires resources to have restrictions and entities to have authorizations. Access to a resource is granted on the basis of an entity's authorizations rather than an entity's identity. An RBAC decision requires authorization information and restriction information to compare before any access is granted.

A composite policy, referred to as role-based policy, can be considered a variant of both IBAC and RBAC. In this case, an identity is assigned to a group that has been granted authorizations. Identities can be members of one or more groups. A current example is the Global Command and Control System (GCCS), which depends on organizational and role associations.

Most network operating systems have their own method of implementing access control, but they are all identity-based IBAC. Entities are granted access to resources based on an identity established during network logon, which is compared with one or more ACLs. These lists may

be individually administered, may be centrally administered and distributed to individual locations, or may reside on one or more central servers.

Mechanisms for establishing identities and authorizations have been discussed in previous sections. Mechanisms for establishing restrictions on access to a resource must be provided to implement an RBAC scheme. Since rule-based access controls how rules are implemented primarily in systems dealing with sensitive information, restrictions are most often expressed as policies for accessing sensitive data. To facilitate these policies, the sensitivities of a data item are conveyed in a data label and must be compared with the set of privileges assigned to an entity. Access is granted to sensitive information if an entity's privileges are appropriate for the sensitivities of the data. An example of a rule-based policy is the classifications used to distinguish information on a national security level, such as top secret, secret, and confidential, and the rule that identities authorization for any security level as also authorizing access to all lower security levels. Users who hold secret clearances will be allowed to access secret and below classified information.

Consistent with the issues surrounding identities and authorizations, data labels must also be assigned, bound, represented, communicated, and authenticated. There are currently many representations of a data security label (Federal Information Publications [FIPS] [4] 188 Standard Security Label, Secure Data Exchange (SDE)Security Label—Institute for Electrical and Electronic Engineers (IEEE) 802.10g, Internet Security Label, ISO SC-27 Security Label, Common Security Label [Military Standard (MIL STD) 2045-48501], X.411 Message Handling System (MHS): Message Transfer System (MTS) Service Definition–Security Label). Establishment of a universally accepted standard is an area for further work.

Note that an access request can actually be composed of a complicated set of parameters. For example, a particular access might be, "Execute a file labeled top secret at 3:15 p.m. during a time of war." Defining "access" in this manner allows the access decision function to provide a binary grant or deny result. This introduces a new set of information that must be represented, communicated, and authenticated, including contextual information, such as time, status, or current conditions.

4.3.1.4 Enforcement

Actual enforcement of the access control decision is the step that actually provides protection against attacks. All previously discussed mechanisms for preventing attacks come together here with the enforcement of those protections.

The concept of enforcing an access control decision is separate from the decision itself. This is because the two processes may reside in different places architecturally. This separation permits the concept of an "authentication server" that makes an access decision for the network communications process to allow or prevent a requested access from taking place. For example, the access decision may result in the subject's being provided with a token (such as a certificate) that guarantees the subject the right to access its target up to, but no more than, *n* times before a

given time. This token is called a ticket or capability. These tokens may be cached at the target to improve efficiency.

An access control decision and its enforcement can be made at either end of a communications association. An example is the difference between a client's accessing a File Transfer Protocol (FTP) server (the server limits access to files after a client request is submitted) and an e-mail message (in which the originator decides whether the recipient should receive the message before a connection is made). In the e-mail example, the recipient's mail software may also perform an additional access control check to determine whether the recipient can be allowed to view the message.

Another distinction between access control mechanisms is whether the decision and enforcement process occurs once at the initiation of a communications session, is repeated periodically throughout a session, or qualifies as "continuously authenticated." A method commonly used to ensure that access to a communications session is controlled continuously is use of encryption mechanisms to prevent loss of control of the session (session stealing or hijacking). Indeed, it can be argued that access is not completely controlled if information flowing over a public network is not protected by the confidentiality security service.

Enforcement of an access control decision may take place at many places in a network's architecture. Access controls may be enforced at network boundaries (e.g., firewalls, routers, and dial-in communications servers), at application servers, or anyplace in the protocol stack or operating system of individual workstations. An important implementation option is inclusion of access control mechanisms at many layers throughout a network architecture.

4.3.2 Confidentiality

The confidentiality security service is defined as preventing unauthorized disclosure of data (both stored and communicated). This definition is similar to, and actually a subset of, the description of access control in Section 4.3.1. In fact, it can be argued that providing access control also provides confidentiality, or conversely, that providing confidentiality is a type of access control. We include in the definition of "information," data that is not traditional user data (examples are network management data, routing tables, password files, and IP addresses on data packets). Confidentiality services will prevent disclosure of data in storage, transiting a local network, or flowing over a public Internet. One subset of confidentiality is "anonymity," a service that prevents disclosure of information that leads to the identification of the end user.

The provision of the confidentiality security service depends on a number of variables:

- **Location(s) of the Data that Needs Protection.** Data can exist on an individual machine (e.g., on a hard disk in an end system or in a file on a server), on the wires of a local network, in transport via other mechanisms (e.g., floppy disk), or flowing across a totally public medium (e.g., across the Internet or via a satellite).

- **Type of Data that Needs Protection.** Data elements may be local files (e.g., passwords or secret keys), data carried in a network protocol, or the exchanges of a network protocol (e.g., a protocol data unit).
- **Amounts or Parts of User Data that Need Protection.** It may be necessary to protect an entire data element, only parts of a data element or protocol data unit, or the existence of an entire set of protocol exchanges.
- **Value of Data that Needs Protection.** The sensitivity and perishability of the data being protected influence the provision of security services, particularly the strength of mechanisms implemented. The value of the data to the owner in assessing the threats to information.

The elements of confidentiality are as follows:

- **Data Protection.** This is prevention of disclosure of the contents of data even if it is accessible (e.g., flowing over a network). This element invokes mechanisms that act directly on the data (or act in response to characteristics of the data) rather than acting in response to an entity's attempt to access data.
- **Data Separation.** Data separation traditionally refers to the concept of providing for separate paths (Red/Black or physical) or process separation (computer security [COMPUSEC] techniques, etc.).
- **Traffic Flow Protection.** Data characteristics include frequency, quantity, destination of traffic flow, etc. Traffic flow protection includes not only characteristics but also inference information such as command structure, and even the instance of communication (e.g., a network communication).

4.3.2.1 Data Protection

In cases in which communicated data will be visible to possible adversaries (i.e., via passive monitoring attacks), the most common method for providing confidentiality by data protection is to encrypt the appropriate data. Encryption is also used to protect stored data that might be accessed by an adversary (e.g., via the network-based attacks described in Chapter 3, Information Systems Security Methodology.

Encryption is defined as the transformation of data into a form that is unreadable by anyone who does not possess the appropriate secret key. There are many ways of using encryption to provide confidentiality. A small subset includes—

- Security-enabled applications (file encryptors).
- Secure peripherals (media encryptors).
- Operating systems (encrypt local passwords).
- Secure application protocols (secure FTP).
- Security protocols (authentication and key management protocols).
- Secure upper layer network protocols (socket layer, IP layer).
- Secure lower layer network protocols (link encryptors).

Two types of cryptographic mechanisms can be used to provide encryption: symmetric cryptography, wherein entities share a common secret key, and public key cryptography (also known as asymmetric cryptography), in which each communicating entity has a unique key pair (a public key and a private key).

Implementation variables in providing encryption for protection of communications data include where in the protocol stack encryption takes place. Encryption at different layers provides different protections to the underlying data or protocol elements.

The strength of the confidentiality service may depend on a number of variables associated with the encryption function:

- The security protocol or application used to invoke the encryption function.
- The trust in the platform executing the protocol or application.
- The cryptographic algorithm.
- The length of the key(s) used for encryption/decryption.
- The protocol used to manage/generate those keys.
- The storage of secret keys (key management keys and encryption keys).

4.3.2.2 Data Separation

Data separation takes a different approach to preventing disclosure. Mechanisms that provide data separation prevent the adversary from getting at the data in the first place. This is achieved by using the normal access control mechanisms described in Section 4.4, Important Security Technologies, as well as by the additional techniques described below. An example of a commonly used data separation technique is not allowing data labeled as secret to flow onto an unclassified network.

Data separation mechanisms provide confidentiality by preventing data from reaching a location or destination where it could be disclosed to unauthorized entities. Mechanisms can be employed to prevent data from flowing into undesired areas (routing control). Other mechanisms may be employed to physically segregate those areas. Examples of routing control include a router that directs IP packets based on security labels, thereby preventing secret packets from reaching unclassified networks, and a firewall that scans e-mail messages for “dirty words” and prevents messages containing them from being released outside a local network. Examples of physically segregated data are isolated system high networks and physically protected wires.

Data separation mechanisms can be used to counter passive monitoring attacks, as well as insider attacks that inappropriately attempt to release information from a controlled area. The primary variable in the level of assurance provided by a data separation mechanism is the level of trust associated with the process or machine implementing the mechanism.

4.3.2.3 Traffic Flow Protection

Data padding can be employed to provide traffic flow protection. Addition of superfluous (usually random) data to data carried in a communications protocol can hide the characteristics (e.g., data rate, data frequency, etc.) of the underlying data. When combined with encryption, this mechanism also hides the content of the underlying data.

Address hiding can also be employed to provide traffic flow protection. Address hiding includes network address translation in which the IP addresses of machines in a local network are replaced by the address of a protecting firewall. Network layer addresses can be hidden by encrypted tunnels, which also provide data confidentiality.

4.3.2.4 Other Mechanisms

Other mechanisms for providing confidentiality include spread-spectrum and frequency hopping techniques.

4.3.3 Integrity

The integrity security service includes the following methods: prevention of unauthorized modification of data (both stored and communicated), detection and notification of unauthorized modification of data, and recording of all changes to data. Modification of both stored and communicated data may include changes, insertions, deletions, or duplications. Additional potential modifications that may result when data is exposed to communications channels include sequence changes and replay.

The requirements for provision of integrity security services are similar to those for confidentiality and include the location, type, and amount or parts of the data that needs protection.

When integrity is discussed with respect to network security, it is important to consider where in the protocol stack the integrity service is provided. Different implementation (layering) options will provide integrity to data in different protocol layers as well as to data being communicated. Sophisticated integrity schemes are likely to require service from the application using the data.

Note that integrity protection is of no value unless it is combined with a mechanism that provides authentication of the source. Without source authentication, anyone could tamper with the original data and then just reapply an integrity mechanism.

Data integrity can be divided into two types, based on the type of data to be protected. Integrity can be applied to a single data unit (protocol data unit, database element, file, etc.) or to a stream of data units (e.g., all protocol data units exchanged in a connection).

4.3.3.1 Single Unit of Data

Ensuring the integrity of a single data unit requires that the originating (sending) entity calculate an additional data item that is a function of (and bound to) the original data unit. This additional item is then carried along with the data unit. The entity that desires to verify the integrity of this data unit must recalculate the corresponding quantity and compare it with the transferred value. A failure of the two to match indicates that the data unit has been modified in transit.

Methods for calculating this data item, which is a function of the original data unit (the "check value"), vary in the processing required and the services provided. Checksums, cyclic redundancy check (CRC) values, and hashes (also known as a message digest) all meet the requirement that they depend on the entire content of the original data unit. A weakness of this method is that, if an adversary modifies the original data, these functions are easily reproducible and allow the adversary to generate a proper value for the modified data thereby defeating the integrity service. An additional mechanism can be applied to prevent access to the check value (e.g., encryption or digital signatures) to overcome this problem.

Another method of preventing successful modification of the check value is to include a secret value along with the original data unit. This property is exhibited by message authentication codes (also known as message integrity check and keyed hashes).

The icheck value alone will not protect against an attack that replays a single data unit. A time stamp may be included along with the original data unit to provide limited protection against replay.

4.3.3.2 Sequence of Data Units

To protect the integrity of a sequence of data units (i.e., protect against reordering, losing, replaying and inserting, or modifying data), some type of ordering information must be provided within the communications protocol. Examples of ordering information are sequence numbers and time stamps. Integrity of sequences can also be provided by encrypting the sequence of data units using a cryptographic algorithm in which encryption of each sequence depends on the encryption of all previous sequences (also referred to as chaining).

4.3.4 Availability

Availability is "timely, reliable access to data and information services for authorized users." Availability in a networked environment includes not only the user's ability to access hardware and software resources (such as user agents and servers) but also the user's ability to obtain a desired quality of service or QoS (e.g., to make use of network bandwidth with reasonable throughput). Network traffic must be able to traverse LANs and wide area networks (WAN) as required to reach its intended destination.

One of the most effective methods of assuring availability is to provide a secure network environment that exhibits the common security services. Attacks that could prevent a networked system from providing availability may be countered by preventing unauthorized access to resources with access controls and protecting data from disclosure or modification with integrity and confidentiality services. Access control, integrity, and confidentiality become mechanisms to help support the availability security service.

Solutions to problems that affect availability include the following:

- **Protection from Attack.** Some network-based attacks are designed to destroy, degrade, or "crash" network resources. The solution is to harden these resources against such attacks. Means of doing this include closing security holes in operating systems or network configurations, limiting access to resources to authorized entities, and limiting an adversary's ability to manipulate or view the data flowing through and to those resources (thus preventing insertion of harmful data, such as viruses, or disclosure of sensitive network data, such as routing tables).
- **Protection from Unauthorized Use.** Availability is also limited if a resource is in use, occupied, or overloaded. If unauthorized users are using limited resources (e.g., processing power, network bandwidth, or modem connections), the resources are not available for authorized users. Identifying and authenticating the users of these resources can provide access controls to limit unauthorized use. However, the process of requesting IA too frequently may be used to slow or stop network operations (i.e., nondelivery notice floods).
- **Resistance to Routine Failures.** Normal operational failures and acts of nature also contribute to loss of availability. Solutions include use of equipment designed for high reliability, redundancy in equipment, and network connectivity that provides multiple routes.

Trusted operating system concepts are also used to limit the harmful effects of network attacks. By containing the damage caused by malicious code and ensuring the proper operation of other security mechanisms, the trusted operating system preserves availability. Another feature exhibited by trusted operating systems is process integrity. This provides assurance that processes executing on an end system provide consistent, repeatable results that are not affected by undesired (unauthorized) influences.

Critical system components must also provide physical security, not only to prevent attacks or misuse of resources, but also to ensure that the platforms and applications are not modified to bypass the invocation of those security services that provide availability.

4.3.5 Nonrepudiation

Repudiation is denial by one of the entities involved in a communication that it participated in that communication. The nonrepudiation security service provides the ability to prove to a third

party that the entity did indeed participate in the communication. When discussed in the context of networking.

- Nonrepudiation, with proof of origin, provides the recipient of a data item with proof of the identity of the originator of that data item and the time of origination.
- Nonrepudiation, with proof of delivery, provides the originator of a data item with proof that the data item was delivered to the intended recipient (and in some cases, the time of receipt).
- Auditing services help enforce accountability of the parties involved in exchanges requiring nonrepudiation, by recording relevant events that can be traceable to persons who can be held responsible for their actions.

The nonrepudiation service is primarily provided by application layer protocols. Users are most often concerned with providing nonrepudiation for application data (such as an e-mail message or a file). Providing nonrepudiation at a lower protocol layer will only provide proof that a particular connection was made; it will not bind the data that flowed over that connection to a particular entity.

Nonrepudiation is provided by the authenticating characteristics of digital signatures. A digital signature on a data element (or on the hash of that element) irrevocably ties that data element to the identity contained in the public key certificate associated with the private key that generated the signature. Of course, data integrity must be provided to that data element to ensure that the element was not changed after the application of the signature.

Because nonrepudiation depends on an identity contained in a public key certificate, and certificates become invalid, it is important to be able to establish to a third party the validity of the certificate. It must be possible to prove the validity of that certificate at the time of the original communication and at any time in the future. This can be accomplished with a combination of trusted time stamps, third-party notaries, or archived CRLs.

Time stamping achieves the goal of establishing the time at which a communication or transaction occurred. For the highest levels of assurance, time stamps are applied by a trusted time stamping service that digitally signs the data item (or a hash of the data item) along with the time stamp before delivery to the intended recipient.

4.4 Important Security Technologies

An overview of technical security countermeasures would not be complete without at least a high-level description of the widely used technologies underlying those countermeasures. This section highlights selected technologies as an introduction to the detailed technology assessments included in Sections 5 through 9. For convenience, these technologies are listed alphabetically.

- **Application Layer Guard.** The need for a separate mechanism to perform a gatekeeper function, checking the invocation of security features, gives rise to a need for security at the application layer. This gatekeeper has recently taken the form of an application layer guard that implements firewall mechanisms (performing I&A functions and enforcing security policies, such as allowing or disallowing connections based on ID and/or requested protocol processing). Guard functionality includes such features as cryptographic invocation check on information that is allowed outside the protected enclave and data content filtering to support sensitivity regrade decisions. The guard functionality, while effective for non-real-time applications (e.g., e-mail) on networks with low sensitivity, has been difficult to scale to highly classified networks and real-time applications.

- **Application Program Interface (API).** APIs are a means of isolating a computing platform from the details of the implementation of cryptographic functions (both the actual algorithms and the hardware implementations). It provides standard interfaces so that multiple vendors can provide interoperable solutions.

- **Common Data Security Architecture (CDSA).** The CDSA is a set of layered security services that address communications and data security problems in the emerging Internet and intranet application space. CDSA focuses on security in peer-to-peer distributed systems with homogeneous and heterogeneous platform environments. The architecture also applies to the components of a client/server application. The CDSA addresses security issues and requirements in a broad range of applications by—
  - Providing layered security mechanisms (not policies).
  - Supporting application-specific policies by providing an extensibility mechanism that manages add-in (policy-specific) modules.
  - Supporting distinct user markets and product needs by providing a dynamically extensible security framework that securely adds new categories of security service.
  - Exposing flexible service provider interfaces that can accommodate a broad range of formats and protocols for certificates, cryptographic keys, policies, and documents.
  - Supporting existing, secure protocols, such as Secure Sockets Layer (SSL), Secure/Multipurpose Internet Mail Extension (S/MIME), and Secure Electronic Transaction (SET).

- **Circuit Proxy.** Circuit gateways are another type of proxy firewall. A circuit-level proxy becomes an intermediate connection point in a session between a client and a server. To reach a distant server, a client initially connects to a Transmission Control Protocol (TCP) port on the circuit proxy machine. The circuit proxy then completes the connection (after making an access control decision) to the target server. Access controls are based on the identity of the initiating machine without interpreting the application protocol or viewing the contents of protocol packets. A circuit-level proxy can be used across several application protocols; however, client modifications may be necessary to use the circuit-level protocol.

- **CryptoAPI.** The Microsoft Cryptographic API provides services that enable application developers to add cryptography to their Win32 applications. Applications can use the

functions in CryptoAPI without knowing anything about the underlying implementation, in much the same way that an application can use a graphics library without knowing anything about the particular graphics hardware configuration.

- **Cryptographic Service Providers (CSP).** Both CDSA and CryptoAPI make use of the concept of CSPs, which are independent modules that perform the real cryptographic work. Ideally, CSPs are written to be completely independent of any particular application, so that a given application will run with a variety of CSPs. In reality, however, some applications may have very specific needs that require a custom CSP.

  A CSP may implement one or more of the following cryptographic functions: bulk encryption algorithm, digital signature algorithm, cryptographic hash algorithm, unique identification number, random number generator, secure key storage, and custom facilities unique to the CSP.

  A CSP may be implemented in software, hardware, or both. The CSP or an independent module can also deliver key management services, such as key escrow or key recovery. CSPs should not reveal key material unless it has been wrapped. Also, the key-generation function of a CSP should be made as tamper resistant as possible.

- **File Encryptors.** These provide confidentiality and integrity for individual files, provide a means of authenticating a file's source, and allow the exchange of encrypted files between computers. File encryptors typically implement a graphical user interface (GUI) that allows users to choose files to be encrypted or decrypted. This protects individual files but does not protect all of the files on the drive.

  Many applications generate temporary files that may contain user data. These files are normally erased when the application is closed; but when the application does not close in an orderly fashion, these temporary files may remain. In addition, some operating systems do not actually erase data when files are deleted. Instead, they alter the name of the file in the file allocation table. The user's data remains on the hard drive until the space is reallocated to another file and overwritten. Thus, unencrypted and potentially classified user data can remain on the hard drive after system shutdown, either through failure to erase temporary files or by design of the operating system's erasing function.

- **Hardware Tokens.** A number of hardware token approaches are available. The approaches range from a token that is an external memory device only to a token with significant levels of processing. One hardware token that is prominent in the Department of Defense (DoD) community is the FORTEZZA® Crypto Card. The FORTEZZA® card provides the cryptographic algorithms required to provide security services to a FORTEZZA®-based system. It stores the private key information for each user personality, the certificates of its issuers, and the public keys needed for cryptography. It also performs the digital signature and hash algorithms, public or private key exchange functions, encryption, and decryption. The interface to the card depends on the hardware platform and its configuration, and the operating system.

- **Intrusion and Penetration Detection.** Intrusion detection and response systems can protect either a network or individual client platforms. Effective intrusion detection systems detect both insider and outsider attacks. In general, intrusion detection systems are intended to protect against and respond to situations in which the available countermeasures have been penetrated, either through allowed usage or the exploitation of vulnerabilities that are unknown or have not been patched. The objective of these systems is to detect malicious and unintended data and actions (e.g., altered data, malicious executables, requests that permit unintended resource access, and unintended use of intended services). Once the intrusion is detected, an appropriate response is initiated (e.g., disconnect attacker; notify operator; respond automatically to halt or lessen the attack; trace attack to proper source; and counter the attack, if appropriate). Intrusion detection mechanisms operating at the transport layer can view the contents of transport packets (e.g., TCP packets) and are able to detect more sophisticated attacks than are mechanisms that operate at the network layer. Intrusion detection mechanisms operating at the network layer can view the contents of network packets (e.g., IP packets) and are thus only able to detect attacks that are manifested at the network layer (e.g., port scans).

- **Internet Protocol Security (IPSec).** IPSec is the security framework standardized by the IETF as the primary network layer protection mechanism. IPSec consists of two parts: an authentication header (AH), whose purpose is to bind the data content of IP frames to the identity of the originator, and an encapsulating security payload (ESP), for privacy. The AH is intended for use when integrity of information is required but privacy is not. ESP is intended for use where data confidentiality is required. ESP defines two methods (or modes) of encapsulating information. Tunnel mode, when used at an enclave boundary, aggregates traffic flow from site to site and thereby hides end-system identification. Transport mode leaves end-system identification in the clear and is most advantageous when implemented at the end system.

- **Internet Key Exchange (IKE) Protocol.** IKE was developed by the IETF as a standard for security attribute negotiation in an IP network. It provides a framework for creating security associations between endpoints on an IP network, as well as the methodology to complete the key exchange. IKE is based upon the Internet Security Association Key Management Protocol (ISAKMP) with Oakley extensions. The structure of ISAKMP is sufficiently flexible and extensible to allow inclusion of future security mechanisms and their associated algorithms and can be tailored to other networking technologies.

- **Media Encryptors.** Media encryptors protect the confidentiality and integrity of the contents of data storage media. They can also perform a role in maintaining the integrity of the workstation by verifying the Basic Input/Output System (BIOS) and ensuring that configuration and program files are not modified. Media encryptors need to leave some system files unencrypted so that the computer can boot from the hard drive. Most of these files can have their integrity protected by a cryptographic checksum; this will not prevent a tamper attack but will alert the user that the data has been altered. However, some system files contain data that changes when the computer is booted; these files cannot be protected. With the exception of some system files, media encryptors encrypt the entire contents of the drive.

- **Packet Filter.** Packet filtering firewalls (also called screening routers) commonly operate at the network layer (Open Systems Interconnection [OSI] Layer 3). These firewalls check the IP and protocol headers against a set of predefined rules. They can typically filter packets based on host and destination IP address, port number, and the interface. This type of firewall is generally inexpensive, fast, and transparent to the user. However, screening routers generally do not have a very robust auditing capability, nor do they allow the use of strong authentication on incoming connections. The combination of a packet filtering system and another product (authentication server) may provide strong authentication capability.

- **PKI Certificate Management Protocol (CMP).** For managing public key material, the Internet community has developed the Internet X.509 PKI CMP. Management protocols are required to support on-line interactions between PKI components. For example, a management protocol might be used for interactions between a CA and a client system with which a key pair is associated or between two CAs that cross-certify each other. At a high level, the set of operations for which management messages are defined can be grouped as follows:
  - **CA Establishment.** When establishing a new CA, certain steps are required (e.g., production of initial CRL, export of CA public key).
  - **End-Entity Initialization.** This includes importing a root CA public key and requesting information about the options supported by a PKI management entity.
  - **Certification**. Various operations result in the creation of new certificates:
    - Initial registration/certification
    - Key pair update
    - Certificate update
    - CA key pair update
    - Cross certification
    - Cross-certificate update.
  - **Certificate/CRL Discovery Operations.** Some PKI management operations result in the publication of certificates or CRLs:
    - Certificate publication
    - CRL publication.
  - **Recovery Operations.** Some PKI management operations are used when an end entity has “lost” its key material.
  - **Revocation Operations.** Some PKI operations result in the creation of new CRL entries and/or new CRLs.

- **SSL.** SSL exists just above the transport layer and provides security independent of application protocol, although its initial implementation was meant to secure the Hypertext Transfer Protocol (HTTP). This effort has migrated to the IETF as the Transport Layer Security (TLS) protocol, which provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. TLS negotiates the invocation of cryptographic algorithms (from a fixed set) and protects all application layer data.

- **S/MIME.** S/MIME is a specification for adding security for e-mail in Multipurpose Internet Mail Extensions format, supporting binary attachments as well as text. It offers authentication and confidentiality. S/MIME uses a hybrid approach to providing security, referred to as a digital envelope. The bulk message is encrypted with a symmetric cipher, a public key algorithm is used for key exchanges and for digital signatures, and X.509 certificates support authentication. S/MIME supports anonymity to the extent that it applies the digital signature first and then encloses the signature and the original message in an encrypted digital envelope, so that no signature information is exposed to a potential adversary.

  The S/MIME specification is currently an Internet draft that recommends three symmetric encryption algorithms: Data Encryption Standard (DES), Triple-DES, and RC2 (a symmetric block cipher with a 40-bit key to meet the U.S. Government's export requirements). It also builds on the Public Key Cryptography Standards (PKCS), specifically PKCS #7, providing a flexible and extensible message format to represent the results of cryptographic operations, and PKCS #10, a message syntax for certification requests. The S/MIME specification has been submitted to the IETF in an effort to make it an industry-accepted standard.

- **SOCKS.** This protocol supports application-layer firewall traversal. The SOCKS protocol supports both reliable TCP and User Datagram Protocol (UDP) transport services by creating a shim-layer between the application and the transport layers. The SOCKS protocol includes a negotiation step whereby the server can dictate which authentication mechanism it supports. Compliant implementations must support Generic Security Services (GSS)–API and user name/password authentication modes.

- **Stateful Packet Filter.** Stateful packet filters look at the same headers as do packet filters, but also examine the content of the packet. In addition, this technology is capable of dynamically maintaining information about past packets or state information. Security decisions can then be based on this state information. Because they can retain state information, stateful packet filters permit UDP-based services (not commonly supported by firewalls) to pass through the firewall. Thus they are advertised as offering greater flexibility and scalability. Stateful packet filtering technology also allows logging and auditing and can provide strong authentication for certain services.

- **Trusted Computing Base (TCB).** A trusted computer system is a system that employs sufficient hardware and software assurance measures to allow its use for simultaneous processing of a range of sensitive or classified information. Such a system is often achieved by employing a TCB. A TCB is the totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy across a product or system. The TCB's ability to correctly enforce a unified security policy depends solely on the mechanisms within the TCB and on system administration personnel's correct input of parameters (e.g., a user's clearance level) related to the security policy.

- **Virus Detectors.** Virus detectors can be used to protect a network or an individual client. A virus can be considered a special form of intrusion involving the classic Trojan horse attack with the ability to reproduce and spread. The virus is normally considered to be limited to the authorizations of the user who is executing the code, but viruses may also exploit flaws in the network that allow them to cause a serious privilege state harm.

4.5 Robustness Strategy

Purpose

The robustness strategy, when completed in a later release of the IATF, will provide guidance on assessing the degree of robustness. This is defined as the level of security mechanism strength and assurances recommended (considered "good enough") for an Information Systems Security (INFOSEC) solution. At its current stage of development, the strategy deals primarily with the levels within individual security services and mechanisms, based on information on a given valuein a particular (static) threat environment. As discussed below, this strategy is not a complete answer, and is not intended to provide an endorsement or credentials for specific products. It also is not intended as a "recipe" for robust solutions; rather, it offers security engineering guidance to the developers, integrators, and risk managers engaged in risk management. Users of the IATF can employ the robustness strategy to—

- Help developers and integrators assess what strength of mechanisms, what levels of assurance (in development methodology, evaluation, and testing) and what criteria are recommended for a particular configuration meant to protect information of a particular value; with a specific intelligence life; in a specific, static threat environment.
- Define product requirements for different customer scenarios (value of information, threat, configuration, etc.), for example, as described in the IATF.
- Provide feedback to security requirements developers, decision makers, customer representatives, customers, etc.
- Constitute developmental requirements when a security solution does not exist.
- Work with academe to foster research in the network security arena and to educate future engineers, architects, and users on network security technology.
- Perform subsequent risk assessments made necessary by reconfiguration of the system or network under review or by a change in threat or value of information.

As technology in general and INFOSEC threats in particular evolve, countermeasures must also evolve, and with them the corresponding application guidance. This paper is a strategy for the development of a general security mechanism and countermeasure valuation scheme. Rather than directly defining the security requirements that must be met, it characterizes the relative strength of mechanisms that provide security services and provides guidance on selecting these mechanisms.

Trained information systems security engineers [11] support customer organizations in defining and applying security solutions to address the organization's information assurance (IA) needs. Working with a customer from initial contact through solution acceptance, the systems security engineer helps ensure that the customer's security needs are appropriately identified and that acceptable solutions are developed. Within the context of the IATF robustness strategy, he or she helps the organization assess the value of its information and assets and the security threat within the operational environment, identifies the security services necessary to provide appropriate protection, and provides guidance on the characteristics of the specific security mechanisms that provide those services.

Different applications of the same system or environment but by differently trained systems security engineers may result in different guidance, although all such outcomes would be consistent with the recommended use of the strategy. There is no concept of official "compliance" with the robustness strategy as a condition for approval of a solution. Rather, the strategy is an aid to "get you there".

Robustness Strategy Section Overview

Section 4.5.1 describes the general process including assumptions and output. Section 4.5.2 presents an approach for determining recommended robustness levels (strength of mechanism and assurance) based on the value of information to be protected and the threat environment. Section 4.5.3 breaks down security services into supporting mechanisms and identifies corresponding strength levels. The Level of Assurance section (Section 4.5.4) discusses related aspects of obtaining assurance. Section 4.5.5 demonstrates how the process would be applied in developing specific guidance. These sections are followed by a discussion of robustness strategy evolution (Section 4.5.6), which provides recommendations for those who would carry on the work outlined in this document. Finally, Section 4.5.7, demonstrates real-world application of the robustness strategy.

4.5.1 Overview of the General Process

The robustness strategy is intended for application in the development of a security solution and is meant to be consistent with IATF Chapter 3, Information Systems Security Engineering, which describes the overall process. An integral part of the process is determining the recommended strength and degree of assurance for proposed security services and mechanisms that become part of the solution set. The strength and assurance features provide the basis for the selection of the proposed mechanisms and a means of evaluating the products that implement those mechanisms. This section provides guidance on determining recommended strength and assurance.

This process should be applied to all components of a solution, both products and systems, to determine the robustness of configured systems and their component parts. It applies to commercial off-the-shelf (COTS), government off-the-shelf (GOTS), and hybrid solutions. As indicated above, the process is to be used by security requirements developers, decision makers, information systems security engineers, customers, and others involved in the solution life cycle.

Clearly, if a solution component is modified, or threat levels or the value of information changes, risk must be reassessed with respect to the new configuration.

Various risk factors, such as the degree of damage that would be suffered if the security policy were violated, threat environment, and so on, will be used to guide determination of an appropriate strength and an associated level of assurance for each mechanism. Specifically, the value of the information to be protected and the perceived threat environment are used to obtain guidance on the recommended strength of mechanism level (SML) and evaluation assurance level (EAL).

4.5.2 Determining the Degree of Robustness

We define the degree of robustness as the level of strength and assurance recommended for potential security mechanism(s). To determine this level for a given security service in a particular application, the customer and the information systems security engineer should consider the value of the information to be protected (in relation to the operational mission), and the perceived threat environment. Guidelines for determining these values are provided below. Once a determination has been made regarding the information value and threat environment, the security engineer uses the robustness table, Table 4-7, to determine required EALs and SMLs.

Table 4-7. Degree of Robustness

Information Value	Threat Levels						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML2 EAL2	SML2 EAL2	SML2 EAL3	SML2 EAL3
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML2 EAL3	SML2 EAL3	SML2 EAL4	SML2 EAL4
V4	SML2 EAL1	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL5	SML3 EAL6
V5	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6	SML3 EAL7

The robustness strategy focuses specifically on individual security services and mechanisms. When the robustness of an overall network solution is considered, the individual solutions at each layer within the network must also be considered. IA mechanisms can be applied at the host, subnet, boundary, and backbone levels. Robustness should take into account the implications of composing layered protection mechanisms and also incorporates an overall assessment of vulnerabilities and residual risks for each layer.

Many customers, in support of their mission, must protect information or an information system whose compromise could adversely affect the security, safety, financial posture, or infrastructure of the organization. Five levels of information value have been defined:

- **V1.** Violation of the information protection policy would have negligible adverse effects or consequences.
- **V2.** Violation of the information protection policy would adversely affect and/or cause minimal damage to the security, safety, financial posture, or infrastructure of the organization.
- **V3.** Violation of the information protection policy would cause some damage to the security, safety, financial posture, or infrastructure of the organization.
- **V4.** Violation of the information protection policy would cause serious damage to the security, safety, financial posture, or infrastructure of the organization.
- **V5.** Violation of the information protection policy would cause exceptionally grave damage to the security, safety, financial posture, or infrastructure of the organization.

Similarly, the customer must work with a systems security engineer to define the threat environment in which the mission will be accomplished. Factors to consider when determining the threat to a particular solution include level of access, risk tolerance, expertise, and resources available to the adversary. These threats should be considered in the context of the system security policy.

The following threat levels were derived from various relevant works (e.g., Security Management Infrastructure [SMI] Task 1 Team, Threat and Vulnerability Model for Information Security, 1997 [12]), and discussions with subject matter experts throughout the Information Systems Security Organization (ISSO):

- **T1.** Inadvertent or accidental events (e.g., tripping over a power cord).
- **T2.** Passive, casual adversary with minimal resources who is willing to take little risk (e.g., listening).
- **T3.** Adversary with minimal resources who is willing to take significant risk (e.g., unsophisticated hackers).
- **T4.** Sophisticated adversary with moderate resources who is willing to take little risk (e.g., organized crime, sophisticated hackers, international corporations).
- **T5.** Sophisticated adversary with moderate resources who is willing to take significant risk (e.g., international terrorists).
- **T6.** Extremely sophisticated adversary with abundant resources who is willing to take little risk (e.g., well-funded national laboratory, nation-state, international corporation).

- **T7.** Extremely sophisticated adversary with abundant resources who is willing to take extreme risk (e.g., nation-states in time of crisis).

After a determination is made regarding the value of the information to be protected and the threat environment, the systems security engineer can provide guidance on how strong the security mechanism should be and what assurance activities that should be performed. Table 4-7 indicates the minimal recommended SML and EAL [6] for protecting information or information systems of a given value (V1 to V5) against a given threat level (T1 to T7). EALs are defined in Sections 4.5.3 and 4.5.4, respectively.

Using an applicable capability maturity model (CMM), Capability Level 2 or the equivalent is recommended for EALs 1 to 3 and Capability Level 3 or the equivalent is recommended for EALs 4 to 7. A CMM describes the stages through which processes advance as they are defined, implemented, and improved.[1]

One example of an applicable CMM is the SSE-CMM. The SSE-CMM is designed to support a host of improvement activities, including self-administered appraisals or internal appraisals augmented by experts (e.g., information systems security engineers) from inside or outside of the organization.[2]

The systems security engineer, working with the customer, would apply the SSE-CMM (or another applicable CMM) as a baseline capability. The assessment of compliance would still be left to the discretion of the customer. Reasonable justification is still necessary, and it should be denoted that acquisition personnel must be knowledgeable about the CMM used.

4.5.3 Strength of Mechanism

SML are presented in a series of tables focusing on specific security services. Since robustness strategy is still being formulated, these tables are not yet considered complete or adequately refined. There are still a number of additional security mechanisms that are not detailed in the tables but that may be appropriate for providing some security services. Further, the strategy is not intended, by itself, to provide adequate information for selection of the desired (or sufficient) mechanisms for a particular situation. An effective security solution will result only from the proper application of ISSE skills to specific operational and threat situations. The strategy does offer a methodology for structuring a more detailed analysis. The security services itemized in these tables have several supporting services that may result in recommendations for inclusion of additional security mechanisms and techniques.

For each service, guidance on each SML is given for the various mechanisms that provide the overall service. In some cases, a group of mechanisms will be required to provide the necessary protection. It should also be noted that a systems security engineer, in conjunction with a customer, could decide to use a stronger or weaker mechanism than is recommended, depending

---

1 System Security Engineering Capability Maturity Model Description document

2 System Security Engineering Capability Maturity Model Summary

on the environment. It is the intent of the strategy to ensure that mechanisms across services at the same strength level provide comparable protection, in that they counter equivalent threats. The selection of mechanisms from the service tables is an independent event, in the sense that one mechanism does not necessarily require others. Higher strength mechanisms do not necessarily contain features of lower strength mechanisms (i.e., security functions do not necessarily accumulate at higher strength levels). Table entries are preliminary estimates based on consultation with subject matter experts and are likely to be revised based on technology evolution, threat assessment, and cost development.

The strength referred to below is a *relative* measure of the effort (cost) required to defeat the mechanism and is not necessarily related to the cost of implementing such countermeasures. All things being equal (especially cost), the highest strength mechanism should always be chosen. Three SMLs are defined:

- **SML1** is defined as basic strength or good commercial practice. It is resistant to unsophisticated threats (roughly comparable to T1 to T3 threat levels) and is used to protect low-value data. Examples of countered threats might be door rattlers, ankle biters, and inadvertent errors.
- **SML2** is defined as medium strength. It is resistant to sophisticated threats (roughly comparable to T4 to T5 threat levels) and is used to protect medium-value data. It would typically counter a threat from an organized effort (e.g., an organized group of hackers).
- **SML3** is defined as high strength or high grade. It is resistant to the national laboratory or nation-state threat (roughly comparable to T6 to T7 threat levels) and is used to protect high-value data. Examples of the threats countered by this SML are an extremely sophisticated, well-funded technical laboratory and a nation-state adversary.

Based on these definitions, the customer and the systems security engineer will apply their knowledge of the specific operational and threat situation to determine what strength of mechanism is recommended for each of the mechanisms listed in the following sections.

4.5.3.1 Mechanisms Supporting Security Management

Recommended mechanisms for establishing needed security management are depicted in Table 4-8. The degree of awareness and control with respect to the following will identify the SML target.

- **Compromise Recovery.** In addition to achieving a secure initial state, secure systems must have a well-defined status after failure, either to a secure failure state or via a recovery procedure to a known secure state.
- **Poor System Administration.** This is a leading cause of security weaknesses and vulnerabilities. It is the first line of defense in enforcing the security policy. (See IATF

Chapter 3, Information Systems Security Engineering for more information on system security administration.)

- **Training.** Operators and users require training on security features and system operation. Knowledgeable users are more likely to exercise due care in protecting information assets.
- **Operational Security (OPSEC) Process**. This process is a coordinated, multidisciplinary, five-step activity involving identification of critical information, threat identification and analysis, vulnerability identification and analysis, risk assessment, and adoption of countermeasures. Each use of the process addresses, and is adapted to, a specific activity of concern, which is examined for potential disclosure to specific adversaries, upon which to base directly pertinent countermeasures. Consult with the interagency operation support staff for consideration of individual cases.
- **Trusted Distribution.** This is a calculated/controlled method of distributing security-critical hardware, software, and firmware components. It protects the system from modification during distribution and detects any changes.
- **Secure Operations.** This is the level of standard operating procedures needed to provide security given the classification, sensitivity, and criticality of the data and resources being handled or managed. Secure operations includes security doctrine.
- **Mechanism Management.** Certain security mechanisms (e.g., cryptographic algorithms) have ancillary support needs (e.g., key management).

Table 4-8. Security Management Mechanisms

	Compromise Recovery	System Administration	Training	OPSEC	Trusted Distribution	Secure Operations	Mechanism Management
SML1	Informal plan	See Ch. 4, Counter-measures	Training available at user's discretion	Implementing OPSEC at user's discretion	Direct vendor purchase	Informal plan of operation	Procedural, at user's discretion
SML2	Detailed plan that is reviewed and approved	See Ch. 4, Counter-measures	Formal training plan	OPSEC training required; implementatio n at user's discretion	Certificate of authenticity, virus scan, validation	Formal plan of operation	Procedural, reminders, at user's discretion
SML3	Detailed plan that is reviewed and approved	See Ch. 4, Counter-measures	Knowledge / skill certification required	OPSEC training required, implementatio n required	Protective packaging, checksums, validation suite	Detailed, formal plan of operation	Automated support

4.5.3.2 Mechanisms Supporting Confidentiality

Confidentiality is the protection of information against disclosure to unauthorized entities or processes. Possible security mechanisms for this security service are depicted in Table 4-9. These mechanisms can be obtained individually or in combination.

- If cryptographic algorithm is chosen, some factors that must be considered are the management of keying material and the effective length of the key, which includes the strength of the underlying cryptographic algorithm. Effective key length is defined as the nominal key length, reduced by the effect of any known attacks against the cryptographic algorithm (assuming correct implementation). The supporting KMI [9] categories are defined in Chapter 8, Supporting Infrastructures.
- Physical security includes tangible security mechanisms, such as guards, locks, and fences. The idea is to build a physically secure enclave, providing guards and high walls.

Table 4-9. Confidentiality Mechanisms

	Cryptographic Algorithm		Physical Security	Technical Security		Anonymity	
	Effective Key Length	Key Management		Anti tamper	TEMPEST	TRANSEC	Cover & Deception
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat X, 80+ exponent 512+ modulus public key length, 80+ hash key length	Comparable to [7]	[6] Level 1 or 2	Comply with applicable EMI/EMC Federal Communications Commission standards or portions of [8]	Low power unit	TBD
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat Y, 160+ exponent 1024+ modulus public key length, 160+ hash key length	Comparable to [7]	[6] level 3 or 4	[8]	Commercial spread spectrum signal techniques	TBD
SML3	Because of the complicated nature of this level, consult a qualified systems security engineer.[3]	SMI Cat Z, also consult with a qualified systems security engineer.[3]	Comparable to [7]	[6] level 4 or better	[8]	cryptographic spread-spectrum signal techniques	TBD

[3] DoD users should consult with a National Security Agency information systems security engineer. Other government users are directed to contact an information systems security engineer at the National Institute of Standards and Technology for

- Technical security is a protection mechanism for hardware. Tampering is unauthorized modification that alters the proper functioning of an information security device or system in a manner that degrades the security or functionality it provides. Antitamper mechanisms detect such alterations. TEMPEST is the investigation, study, and control of compromising emanations from telecommunications and automated information system (AIS) equipment.
- Anonymity is the desire for a user to remain unknown during a virtual transaction. Some applications requiring anonymity might be Internet voting and Internet cash. This area is relatively immature and is currently addressed by the transmission security (TRANSEC)[10] and cover and deception disciplines. TRANSEC mechanisms provide various degrees of covertness to prevent detection, identification, and exploitation. Cover and deception can be provided through such mechanisms as anonymous remailers, "onion routing," or "Web anonymizers." Cover-and-deception currently has no differentiated levels.

4.5.3.3 Mechanisms Supporting Integrity

Table 4-10 shows four mechanisms that, singly or in combination, will help ensure integrity. In the current context, integrity, as a security service, means protection of information against undetected, unauthorized modification or undetected destruction.

Table 4-10. Integrity Mechanisms

	Cryptographic Algorithm		Physical Security	Signature Checksum	Redundancy
	Effective Key Length	Key Management			
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat., 80+ exponent 512+ modulus public key length, 80+ hash key length	Comparable to [7]	Parity, or commercial checksum, hash, and signature with SML1 algorithm	Not applicable
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat, 160+ exponent 1024+ modulus public key length, 160+ hash key length	Comparable to [7]	Cryptographic checksum, hash, and signature with SML2 algorithm	Redundant data path with 100 percent correct comparison
SML3	Due to the complicated nature of this level, consult a qualified information systems security engineer.[4]	SMI Cat, also consult a qualified information systems security engineer.[5]	Comparable to [7]	Cryptographic checksum, hash, and signature with SML3 algorithm	Multiple data paths with 100 percent correct comparison

guidance. Nongovernment users should consult a qualified information systems security engineer, or an equivalent representative within their organization.

4 DoD users should consult with a National Security Agency information systems security engineer. Other government users are directed to contact an information systems security engineer at the National Institute of Standards and Technology for

- A cryptographic algorithm in an error extension mode will emphasize the error and should be used in conjunction with a detection mechanism (e.g., parity or human review).
- Physical security is described in Table 4-9.
- Signature Checksum provides data integrity by digitally signing data. Typically, the data requiring protection is used to calculate a smaller value, such as a parity, checksum, or hash. This value can then be digitally signed.
- Redundancy is the availability of multiple methods to obtain the same information.

4.5.3.4 Mechanisms Supporting Availability

Availability is also known as service assurance. To ensure availability of data, the system must employ both preventive and recovery mechanisms. This security service is quantified in Table 4-11 and can be obtained through a combination of the services as appropriate for the applications.

- TRANSEC is used to overpower potential jammers. A strong enough signal is provided for this antijam capability. TRANSEC can also be used to hide a signal to prevent jamming. (Note that, because of the real-time nature of exploitation, it may not be necessary to use an SML3 algorithm strength to meet the SML3 level for this mechanism.)
- Antitamper mechanisms are described in Table 4-9.
- Physical security is described in Table 4-9.
- Redundancy or redundant paths should be available to allow information flow without violating the site security policy. Such information flow might include bypassing any problem areas, including congested servers, hubs, cryptography, and so on.
- Data recovery is the ability to recover data that might otherwise be unavailable due to the loss of key, storage media, etc.

---

guidance in this area. Nongovernment users should consult a qualified information systems security engineer or an equivalent representative within their organization.

5 DoD users should consult with a National Security Agency ISSE. Other government users are directed to contact an ISSE at the National Institute of Standards and Technology for guidance in this area. Non-government users should consult with a qualified ISSE or an equivalent representative within their organization.

Table 4-11. Availability Mechanisms

	TRANSEC	Antitamper	Physical Security	Redundancy	Data Recovery
SML1	High power	Level 1 or 2 [4]	Comparable to [7]	Bypass channel available	Informal archival plan, user backs up own key or data
SML2	Commercial spread spectrum signal techniques	Level 3 or 4 [4]	Comparable to [7]	Backup data path, hot spare	Formal archival plan, central backups
SML3	Cryptographic spread-spectrum signal techniques	Level 4 or better [4]	Comparable to [7]	Multiple data paths, multiple hot spares	Formal archival plan, central, off-site backups

4.5.3.5 Mechanisms Supporting I&A

I&A is required for effective access control. This usually includes a process for enabling recognition of an entity within or by an AIS and a security measure for establishing the validity of a transmission, message, or originator or verifying an individual's eligibility to receive specific categories of information. These attributes of I&A are listed in Table 4-12 and can be described as follows:

- Identification, or system identification (SID) in particular, is one way in which a system might recognize the entity (which may be a person) requesting authentication. Biometrics might be used to identify a living person.
- Human-to-machine authentication could use alphanumeric phrases, like passwords, personal identification numbers (PIN), or challenge, response exchanges that are memorized by a human or used with a token calculator. Physical devices, such as hardware tokens also provide such authentication (e.g., a credit card-type physical entity).
- Peer-to-peer authentication can use certificates to identify and authenticate entities. Such certificates are bound to the entity by a SML cryptographic algorithm, with a digital signature. Authentication is provided by a trusted third party (a separate, but knowledgeable entity). Within this area, one could use a cryptographic algorithm (as discussed under Confidentiality, above) and personnel security policy, in which a security clearance is obtained for a particular person to reduce the risk of an insider's attacking the system.

Table 4-12. I&A Mechanisms

	Identification		Human-to-Machine Authentication		Peer-to-Peer Authentication			
						Cryptographic Algorithm		
	System IDs	Bio-metrics	Passwords PINS Challenge/ Response	Tokens	Certifi-cates	Effective Key Length	Key Management	Personnel Security
SML1	Uniqueness	Not applicable	Use of any of these methods.	Badge/ key static	Bind with SML1 crypto-graphic algorithm	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat. X, 80+ exponent 512+ modulus public key length, 80+ hash key length	Commercial hiring practices
SML2	Uniqueness and minimum character length	Use of any biometric method	Minimum effective length – TBD	Memory device, updated period-ically	Bind with SML2 crypto-graphic algorithm	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat Y, 160+ exponent 1024+ modulus public key length, 160+ hash key length	Equivalent of secret clearance
SML3	Uniqueness and minimum number of characters, minimum distance (e.g., Hamming)	Use of any biometric mechan-ism with a liveness test	Minimum effective length - TBD	CIK, updated every time	Bind with SML3 crypto-graphic algorithm	Because of the complicated nature of this level, consult a qualified systems security engineer 6	SMI Cat Z, also consult with a qualified systems security engineer.[6]	Equivalent of top secret clearance

4.5.3.6 Mechanisms Supporting Access Control

Beyond I&A, access control can be thought of as a "super service" encompassing all security services. In the context of network security, access control is concerned with limiting access to networked resources (hardware and software) and data (stored and communicated). The primary goal here is to prevent unauthorized use, unauthorized disclosure, or modification of data by unauthorized entities. A secondary goal is to prevent an availability attack (e.g., denial-of-service attack). Several mechanisms that help provide the access control service are shown in Table 4-13.

6 DoD users should consult with a National Security Agency information systems security engineer. Other government users are directed to contact an information systems security engineer at the National Institute of Standards and Technology for guidance in this area. Nongovernment users should consult with a qualified ISSE, or an equivalent representative within their organization.

The mechanisms in Table 4-13 can be described as follows:

- Antitamper is described under Confidentiality in Table 4-9.
- Mandatory access control (MAC) consists of the system's automatic imposition of authorized access to data through use of labels and the binding of those labels to the associated data. In implementing MAC, one must consider both the integrity of the label itself and the strength of the binding between the label and the data. In other words, if SML2 is required for MAC, the integrity of the label must be provided with SML2 and the function (possibly a cryptographic algorithm) binding the label to the data must also be SML2. Other implementation concerns include making the labeling non-bypassable and fail-safe.
- Discretionary access control (DAC) is different from MAC in that the choice of who can and cannot be given authorized access to the data is made by the owner of the data to be accessed rather than by the machine. For SML1, this is comparable to setting UNIX permission bits (owner/group/world) to grant access. For SML2 and SML3, use of ACLs further refines the mechanism. ACLs can specifically allow certain identities access to information (e.g., specific users within a group can be granted access). Again, DAC mechanisms should be non-bypassable (changeable only by the owner of the data) and fail-safe, and should possess the same SML level of integrity as that associated with the required level of DAC.
- Certificates are described in Table 4-12.
- Personnel security is described in Table 4-12.

Table 4-13. Access Control Mechanisms

	Anti-Tamper	Mandatory Access Control	Discretionary Access Control	Certificates	Personnel Security
SML1	Level 1 or 2 [4]	Not applicable	Comparable to UNIX permission bits	Bind with SML1 cryptographic algorithm	Commercial hiring practices
SML2	Level 3 or 4 [4]	Labels bound to data having both integrity and binding function at the SML2 leve	ACLs	Bind with SML2 cryptographic algorithm	Equivalent of secret clearance
SML3	Level 4 or better [4]	Labels bound to data having both integrity and binding function at the SML3 leve	ACLs	Bind with SML3 cryptographic algorithm	Equivalent of top secret clearance

4.5.3.7 Mechanisms Supporting Accountability

Accountability can be considered a special type of nonrepudiation. The accountability security service is basically holding each network entity responsible for its actions on that network. Mechanisms that can be used to provide the security service of accountability are shown in Table 4-14 and discussed below.

- When implementing the audit mechanism, the following components should be considered.
  - What is being audited and what relevant events are detected.
  - How the audit (detected) data is protected, analyzed, and reported.
  - What the reaction strategy is to the audit data analysis and reporting.

  These components should be considered for each SML level, and in SML2 and 3, should be detailed in a plan. As with all mechanisms, consideration should be given to noncircumvention or non-bypassability and the effects of failure.

- Intrusion detection is still in relativinfancy. This mechanism monitors a network and detects either (1) known attacks being mounted against the system or (2) differences in a profiled use of the system. Several aspects may be associated with an intrusion detection mechanism–for example, whether it is static (SML1) i.e., set up to filter only on known attacks and profiles; dynamic (SML2), i.e., set up to filter on known attacks and profiles but updatable perhaps through software downloads; or dynamically adaptable (SML3) incorporating the aspect of "artificial intelligence" in which the system learns new profiles based on usage. Depending on the SML level, a reaction mechanism to a detected intrusion must be either informally (SML1) or formally (SML2 and SML3) detailed and implemented.

- I&A is described in Table 4-12.

Table 4-14. Accountability Mechanisms

	Audit	Intrusion Detection	I&A
SML1	Informal reaction mechanism	Static system with informal reaction mechanism	See Table 4-12 for SML1
SML2	Formal reaction plan and strategy	Dynamic system with formal reaction mechanism	See Table 4-12 for SML2
SML3	Formal reaction plan and strategy	Dynamic, adaptive system with formal reaction mechanism	See Table 4-12 for SML3

4.5.3.8 Mechanisms Supporting Nonrepudiation

The security service of nonrepudiation provides the sender of data with proof of delivery and the recipient with assurance of the sender's identity, so that neither can later deny processing the

data. Table 4-15 shows the various mechanisms for providing this service at various security levels. These mechanisms are described below:

- Signature is used to digitally sign data in such a way that only the sender and receiver could have respectively sent and received the message. The sender signs the original data to prove that it was sent. The receiver signs a receipt as proof of receipt of the original data. Validation of these signatures is always required.
- The trusted third party mechanism is used to prearrange a method by which a third party may receive the information from the sender and transmit it to the receiver in a way that ensures that the sender and receiver are confident that they are communicating with the correct party.
- Accountability is described in Section 4.5.3.7. in Table 4-14
- I&A is described in Section 4.5.3.5. Table 4-12.
- Archive is the ability to store data so that it can be recovered if necessary.

Table 4-15. Nonrepudiation Mechanisms

	Signature	Trusted Third Party	Accountability	I&A	Archive
SML1	Sign with SML1 cryptographic algorithm	See Table 4-12, Personnel Security for SML1	See Table 4-12 for SML1	See Table 4-12 for SML1	Informal archival plan, user backs up own key or data
SML2	Sign with SML2 cryptographic algorithm	See Table 4-12, Personnel Security for SML2	See Table 4-12 for SML2	See Table 4-12 for SML2	Formal archival plan, central backups
SML3	Sign with SML3 cryptographic algorithm	See Table 4-12, Personnel Security for SML3	See Table 4-12 for SML3	See Table 4-12 for SML3	Formal archival plan, central, off-site backups

4.5.4 Level of Assurance

The discussion of the need to view strength of mechanisms from an overall system security solution perspective is also relevant to level of assurance. Again, while an underlying methodology is offered, a real solution can only be deemed effective after a detailed analysis that considers the specific operational and threat situations and the system context for the solution.

Assurance is the measure of confidence in the ability of the security features and architecture of an automated information system to appropriately mediate access and enforce the security policy. The assurance measures listed here are from the Common Criteria [6].

The Common Criteria provide assurance through active investigation. Such investigation is an evaluation of the actual product or system to determine its actual security properties. The Common Criteria philosophy assumes that greater assurance results come from greater evaluation efforts in terms of scope, depth, and rigor. This approach has led to the seven EALs described below:

- **EAL 1, Functionally Tested.** Applicable where some confidence in correct operation is required, but when the threats to security are not viewed as serious. This EAL is of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection. An example is the protection of personal information.
- **EAL 2, Structurally Tested.** Requires the cooperation of the developer in the delivery of design information and test results, but should not demand more effort (or substantially increased cost or time) than is consistent with good commercial practice. This EAL is applicable where a low to moderate level of independently assured security is required in the absence of an available development record. An example is securing legacy systems, or cases in which access to the developer is limited.
- **EAL 3, Methodically Tested and Checked.** Permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. It is applicable where a moderate level of independently assured security is required.
- **EAL 4, Methodically Designed, Tested, and Reviewed.** Permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices, which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. This is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. It is applicable in those circumstances in which a moderate to high level of independently assured security in conventional products is required, and where developers or users are prepared to incur additional security-specific engineering costs.
- **EAL 5, Semiformally Designed and Tested.** Permits a developer to gain maximum assurance from security engineering based on rigorous commercial development

practices supported by moderate application of specialized security engineering techniques. This EAL is applicable where a high level of independently assured security in a planned development is required along with a rigorous development approach.

- **EAL 6, Semiformally Verified Design and Tested.** Permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment to protect high value assets against significant risks. It is applicable to the development of security products that will be used in high-risk situations.
- **EAL 7, Formally Verified Design and Tested**. Applicable to the development of products to be used in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Realistically, it is limited to products with tightly focused functionality that is amenable to extensive formal analysis.

These assurance levels are composed of the following assurance classes: configuration management, delivery and operation, development, guidance documents, life-cycle support, tests, and vulnerability assessments. These classes incorporate the concepts of correct implementation, non-bypassable mechanisms, failure to a secure state, secure start-up, and others.

In addition to the tasks addressed in the Common Criteria, there are other assurance tasks that the Common Criteria do not discuss, including failure analysis and test, TEMPEST analysis and test, and tamper analysis and test. If these apply to a particular product or system, they should be added to the requirements of the appropriate EALs.

4.5.5 Examples of Process Application

Assumptions for these examples are as follows:

- Security evaluation is a necessary part of solution development.
- A trained information systems security engineer (or equivalent) is the strategy consumer.

The methodology for correct employment of the robustness strategy is as follows:

- The responsible customer party knows, and has appropriately documented, mission objectives, concept of operation, value of information to be protected, threat environment context, and security policy.
- A solution is then engineered according to IATF Chapters 5 through 9, providing guidance on the security mechanisms required.
- Risk factors (e.g., degree of damage if security policy is violated, threat environment) are used to help determine the appropriate strength and associated level of assurance for each mechanism in the set of security service tables. The risk addressed is the residual risk, not the overall (or initial) risk, that is, what remains after other countermeasures have been applied, and what would be the target of doctrine if additional security measures were not taken. For example, a system high workstation in a secure office setting would

have a different residual risk from that same workstation operating in a public environment.

- Working with an information systems security engineer, the customer will then select COTS/GOTS products providing the necessary strength and assurance.
- The system is evaluated and the residual risk is highlighted.

4.5.5.1 Example One

The following example uses an abbreviated description of the media protection portion of the IATF Remote Access (Section 6.2), Secret Dial-in Case, to demonstrate how the robustness strategy would typically be used in conjunction with other guidance sections of the IATF. No attempt was made to consider an actual customer's needs or an actual recommended solution.

In this example, the customer will be processing secret data at a continental United States (CONUS) site (perhaps in a work-at-home or temporary duty [TDY] situation) on a remote access dial-in system. The customer is required to protect this data and feels the threat to the data is primarily from adversaries with the following resource and risk-tolerance profile:

- Minimal resources at their disposal (i.e., they have enough money or contacts so that they can get someone to steal the laptop from a house or hotel room).
- Willing to take significant risk (i.e., if the person is caught stealing, the adversaries are willing to be prosecuted or know that if the thief gets caught the theft will not be traced back to them).

For this example, a media encryptor is recommended to ensure confidentiality of the customer's secret data on the hard drive of the remote computer. Because the data is secret, according to the current classification manual, compromise of that data would cause serious damage to the security of the United States. Based on the situation described here, the customer, in conjunction with the information systems security engineer, determines that the value of his or her information is at the V4 level (violation of the information protection policy would cause serious damage to the security, safety, financial posture, and/or infrastructure of the organization) and that the perceived threat is at the T3 level (adversary with minimal resources who is willing to take significant risk). According to the Degree of Robustness table, reproduced in Table 4-16, the minimum SML and EAL recommended is SML2 and EAL3 based on the threat and information levels.

Table 4-16. Example Assessment Using Degree of Robustness Table

Information Value	Threat Levels						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML2 EAL2	SML2 EAL2	SML2 EAL3	SML2 EAL3
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML2 EAL3	SML2 EAL3	SML2 EAL4	SML2 EAL4
V4	SML2 EAL1	SML2 EAL2	**SML2 EAL3**	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6
V5	SML2 EAL1	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6	SML3 EAL7

For our example, the information systems security engineer and the customer, by applying the IATF guidance, determined that confidentiality and security management services are recommended. The user of the remote access dial-in system will want to keep the secret data on the laptop inaccessible while in storage. Not only must the data be encrypted on the media, but also the system must be operated in a secure manner; furthermore, the issue of recovering the data if it is compromised must be addressed. The systems security engineer and customer together decide that media encryption will be one mechanism used. Based on the discussions above, a media encryptor of strength SML2 should be considered.

Once the security service has been selected (confidentiality in, this case), the mechanism should be chosen from the columns of the table. In this case, the mechanism chosen is cryptographic algorithm. This mechanism was chosen because it was the cheapest, simplest, and most practical to implement. Physical security was not chosen because it was impossible to apply uniformly, in a timely manner, at different remote sites, without knowing all the sites in advance. Technical security was not chosen because of the wide variety of COTS laptops, which currently are not built with technical security countermeasures. According to the Confidentiality Mechanisms table, Table 4-17, the implementation should look for a cryptographic algorithm capability with an effective key length of 80+ bits, supported by a KMI/PKI providing the strength under category “Y,” as further described in Chapter 8-1, KMI/PKI.

Table 4-17. Application of Confidentiality Mechanisms Table for Example One

	Cryptographic Algorithm		Physical Security	Technical Security		Anonymity	
	Effective Key Length	Key Management		Antitamper	TEMPEST	TRANSEC	Cover
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat X, 80+ exponent 512+ modulus public key length, 80+ hash key length	Comparable to [7]	Level 1 or 2 [4]	Comply with applicable EMI/EMC FCC standards or portions of [8]	Low power unit	TBD
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat, 160+ exponent 1024+ modulus public key length, 160+ hash key length	Comparable to [7]	Level 3 or 4 [4]	[8]	Commercial spread-spectrum signal techniques	TBD
SML3	Because of to the complicated nature of this level, a qualified information systems security engineer should be consulted.[7]	SMI Cat Z, also consult a qualified NSA information systems security engineer.[7]	Comparable to [7]	Level 4 or better [4]	[8]	Cryptographic spread-spectrum signal techniques	TBD

Because the remote access dial-in users will not have direct access to their system administrator or support services, the customer and the information systems security engineer found that the security management mechanisms of training and secure operations were of paramount importance and should be supplied at the SML3 level. Similarly, because of the "remote" use of the system, they thought that compromise might be more likely; and therefore, that the compromise recovery mechanism was also of paramount importance and should be addressed at the SML3 level. Further, because of the value of the information and the threat to the information, it was decided that the components should be characterized as methodically tested and checked, consistent with the Common Criteria EAL3. (Note that this depicts a situation in which the initial SML and EAL recommendations from the strategy were considered inadequate and were thus increased, presumably based on a detailed analysis of the situation.) Table 4-18 depicts how the Security Management Mechanisms table would typically be used.

Note that in using the tables in this section, not all columns must be used, and various SML levels may be employed as needed for the specific mechanism in question. In the media encryption example, it may be determined that security management mechanisms are of paramount importance; therefore, SML3 will be chosen for these mechanisms whereas confidentiality may be adequately provided with a SML2 cryptographic algorithm.

---

7 DoD users should consult with a National Security Agency information systems security engineer. Other government users are directed to contact an information systems security engineer at the National Institute of Standards and Technology for guidance in this area. Nongovernment users should consult with a qualified ISSE, or equivalent representative within their organization.

Table 4-18. Use of Security Management Mechanisms Table

	Compromise Recovery	System Admin-istration	Training	OPSEC	Trusted Distribution	Secure Operations	Mechanism Management
SML1	Informal plan	See Ch. 4, Counter-measures	Training available at user's discretion	Implementing OPSEC at user's discretion	Direct vendor purchase	Informal plan of operation	Procedural, at user's discretion
SML2	Detailed plan that is reviewed and approved	See Ch. 4, Counter-measures	Formal training plan	OPSEC training required, implementation at user's discretion	Certificate of authenticity, virus scan, validation	Formal plan of operation	Procedural, reminders, at user's discretion
SML3	Detailed plan that is reviewed and approved	See Ch. 4, Counter-measures	Knowledge/ skill certification required	OPSEC training required; implementation required	Protective packaging, checksums, validation suite	Detailed, formal plan of operation	Automated support

4.5.5.2 Example Two

A second example of the use of the strategy is where a sensitive compartmented information facility (SCIF) is used for physical protection. Very different security mechanisms would probably be chosen to protect the information. If a DoD system is processing top secret data (V5), and the threat is very high (T6), one would normally apply rigorous SML and EAL levels. However, because the SCIF is used (and there is no connectivity outside the SCIF), the confidentiality requirement is mostly satisfied by physical security at the SML3 level. The access control requirement may also be satisfied by personnel security at the SML3 level. Any residual risk in the areas of confidentiality and access control may be mitigated by additional mechanisms at the SML1 level. This example shows the importance of layering security mechanisms to reduce risk.

4.5.5.3 Example Three

A third example involves a corporation with a large intranet that processes only unclassified data. The corporation has stringent legal requirements for protecting its data from unauthorized access or modification. It maintains a large, heterogeneous network with Internet access protected by firewalls. All data requiring legal protection is maintained in isolated subnets and is not available to authorized users via the network. Off-line stand-alone access is required to view the protected data. The security objective is to upgrade the network to allow the protected data to be securely accessible to all authorized users. Although the data being processed is unclassified, it must be protected from unauthorized access. Using the applicable CMM, a Capability Level 2 or equivalent is recommended. Taking all this into consideration, the customer and the systems security engineer determined that the information was at the V3 level (violation of the information protection policy would cause some damage to the security safety, financial posture, and/or infrastructure of the organization) and the perceived threat was at the T4

level (sophisticated hackers, international corporations). Using the Degree of Robustness table, reproduced in Table 4-19, the minimum SML and EAL recommended is SML2 and EAL3 based on the threat and information levels.

Table 4-19. Example Assessment Using Degree of Robustness Table

Information Value	Threat Levels						
	T1	T2	T3	T4	T5	T6	T7
V1	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML1 EAL2	SML1 EAL2
V2	SML1 EAL1	SML1 EAL1	SML1 EAL1	SML2 EAL2	SML2 EAL2	SML2 EAL3	SML2 EAL3
V3	SML1 EAL1	SML1 EAL2	SML1 EAL2	SML2 EAL3	SML2 EAL3	SML2 EAL4	SML2 EAL4
V4	SML2 EAL1	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL5	SML3 EAL6
V5	SML2 EAL2	SML2 EAL3	SML3 EAL4	SML3 EAL5	SML3 EAL6	SML3 EAL6	SML3 EAL7

In examining at the corporation's security objectives, the customer and systems security engineer determined that access control to the sensitive data and confidentiality of the data as it transits the intranet are the security services required. The mechanisms for implementation must operate on both Windows NT and HP UNIX platforms.

The confidentiality mechanisms for the SML2 category recommend a minimum 80+ bit symmetric key length, 160+ exponent 1024+ modulus public key length. The firewall key scheme includes ISAKMP/OAKLEY with DES or 3DES capability. 3DES is the scheme being evoked. The I&A mechanisms for the SML2 category recommend a system ID and a password with minimum character lengths. The corporation implements user IDs that are a minimum of six characters long and passwords with a minimum of eight characters, with an alphanumeric mix. However, because this was an internal intranet, no security services for integrity, availability, and nonrepudiation were considered necessary.

Each server requiring protection will have their own firewall installed, with the rules base requiring positive user identification and authentication before access is allowed. Initially, this process will be accomplished by using user IDs and passwords; however, it eventually will migrate to a PKI certificate-based capability. Confidentiality will be provided by the VPN capability resident to the firewall product. Client VPN software will be installed on each client machine enforcing the connection and VPN rules for the protected servers (if the client VPN is disabled, no connection is allowed to a protected server).

The following security mechanisms are employed.

- Fronting each server that contains protected data with a firewall.
- Invoking VPNs between client machines and the server and printers (using 3DES algorithm).
- Implementing user I&A using the VPN user ID and password.
- Implementing the firewall rule base to allow access only to users from authorized workstations.

Consideration was also being given to replacing the VPN-only client with a client that provides the VPN capability and extended the firewall policies to the user's desktop.

4.5.6 Robustness Strategy Evolution

Although robustness is now an inherent part of the IATF, it is a relatively new term in the IA lexicon and is not clearly seen as a unifying successor to a variety of similar existing concepts, such as completeness, assurance, and accreditation.

The security mechanism tables shown previously provide guidance at three strength levels to support a variety of security services. At another level of table refinement, security functions would appear, each of which would implement a particular mechanism. For example, each cryptographic algorithm would be a security function to implement a cryptographic algorithm mechanism in support of, for instance, a confidentiality security service. Many security functions implement each mechanism.

To compare and contrast these functions, there must be a way to cost the relative strengths. This effort would require development of cost metrics for each security service. Although functional specifications might be a relatively modest enhancement, the development of multiple costing schemes is likely to be a monumental effort. This level of refinement, which would enable uniform comparison of the protection provided by security mechanisms, is the goal of the strategy.

The IATF layered approach to security means that a variety of services and mechanisms might be needed to achieve the necessary protection. A broader view must be developed, looking across all needed services and the mechanisms proposed for providing those services. The residual risk to a system product must be addressed based on the environment in which it is implemented.

In addition to the above concerns, and because threat environments and security technologies are changing continually, the guidance provided is subject to frequent revision. To the extent possible, all mechanism recommendations should be by indirect references to formally endorsed documents. When this is not possible, periodic revision and trained ISSE application is the best way to ensure that guidance is current.

4.5.7 Real-World Applications

In the real world, it quickly becomes too complicated and impractical to determine layered solution approaches and describe, offer, support, and implement them for more than a small number of robustness levels. The threat levels and information value levels described previously simply yield too many combinations of SML and EAL levels, as shown in Table 4-7. The Office of Secretary of Defense (OSD) Information Assurance guidance and policy for DoD's Global Information Grid (GIG) divides robustness into three levels, a more practical approach.

The OSD GIG policy uses an implementation approach to robustness that draws conclusions based on real-world conditions (see Appendix E, OSD IA Policy Robustness Levels).

4.5.7.1 Future Work

The following areas need further attention:

- The network rating model/methodology also addresses "goodness." How can that effort be incorporated into the strategy?
- Composition of metrics must be addressed in the framework of layered security.
- There is a need to ensure that the terminology used in the strategy is definitive and consistent with that used in the remainder of the IATF.
- The current approach to security is considered nonscalable, meaning that the process used for small systems may not be appropriate for large systems. This issue is also known as the composibility problem and the layering problem. How can the robustness strategy help address this issue?
- The mechanism tables must be reviewed for uniformity of detail and to identify nonquantifiable entries.
- The strategy must be updated to incorporate Common Criteria language throughout, rather than only in the description of the EALs.
- The effect of recommended robustness on return on investment to the customer must be considered.

4.6 Interoperability Framework

Users are becoming increasingly more dependent on information systems, creating a need for connectivity and interoperability at the application level. As information and telecommunications systems are introduced and updated, interoperability of these systems has become a major concern of the organizations that use them. When these systems must be secure, efficient interoperability becomes more difficult to achieve and manage. This section of the

IATF provides a high-level strategy for dealing with interoperability at the architecture and technology levels. Later releases of the IATF will address the issue of interoperability comprehensively, making users aware of options and trade-offs, and providing guidance on this important challenge.

4.6.1 Major Elements of Interoperability

This section identifies numerous elements that must be addressed to achieve interoperability. Typically, all of these elements must be addressed to achieve interoperability. The elements and the issues associated with them are discussed below.

- **Architecture.** A first step in achieving interoperability is an agreement on the nature of the security services, the type of security mechanisms to be used, and their allocation to functional components (e.g., enclave boundary interfaces, end-user terminals of the architecture, and the layers at which security mechanisms are applied).
- **Security Protocols.** Systems must use compatible communications protocols to achieve user-to-user connectivity. When this connectivity must be secure, several security elements associated with security protocols also must be considered. These elements include security services, cryptographic algorithms (with modes and bit lengths), synchronization techniques, and key exchange techniques. If options are permitted, common provisions are also needed for algorithm selection and broader security option negotiation. Typically, security protocol designers deal with these elements.
- **Product Compliance with Standards.** Another element needed for interoperability stems from the need to assure that products used to implement a network security solution actually comply with the standards they claim to support. There are a number of initiatives with the commercial sector and in Government that will verify compliance, as discussed in Section 4.6.3, Interoperability Strategy.
- **Interoperable KMI/PKI Support.** The services and techniques used to provide KMI/PKI constitute another element needed for interoperability. This element includes key and certificate formats, token mechanisms, cross certification (to facilitate communication across KMI/PKI security domains), directory systems, and compromise recovery capabilities. These considerations are discussed further in Section 4.7, Key Management Infrastructure/Public Key Infrastructure Considerations.
- **Security Policy Agreement.** Beyond all of the technical issues that must be addressed to allow interoperability, there is the fundamental need for organizational security policies that establish ground rules for permitting interoperability. The network or system owners must determine what minimum protection mechanisms and assurances (perhaps for particular types of data or destinations) are needed before they are willing to allow users from other networks or systems to communicate or interact with users of their resources and information. Because this important topic is beyond the scope of this document, it is assumed in the IATF that organizations wishing to interoperate have resolved any

incompatibilities in organizational security policy and that the only barriers are technical or economic.

4.6.2 Challenges for Interoperability

In formulating an IA solution, the following potential impediments tend to act as obstacles to achieving interoperability:

- Backward compatibility with legacy systems that do not use accepted standards and lack the negotiation mechanisms needed to interoperate with newer standards-based implementations (even if backward-compatible protocols and modes are available).
- Security solutions–lagging behind the rapid evolution of information technologies, often making security an adjunct capability.
- Evolution of standards or lack of standards accepted by either the user community or the commercial product marketplace.
- De facto proprietary standards or closed systems.
- Lack of an accepted source of testing to verify that products implementing standards do so correctly and that sufficient options from the standards are implemented to assume users that the resultant products are, in actuality, interoperable.

The challenge is to recognize and surmount these obstacles, yet still find a way to achieve the interoperability needed by our customers.

4.6.3 Interoperability Strategy

At this point in the IATF, it is appropriate to establish a basic, high-level strategy for dealing with interoperability. This strategy focuses on the following efforts.

- Fostering standards for secure applications and communications protection that are based on open architectures.
- Supporting security negotiation protocol standards that allow users to have varying policies and that provide a vehicle for negotiating elements of interoperability.
- Developing a strategy for migration from the interim solutions to open standards in environments where emerging technology dominates and users accept interim solutions that are not standards based.
- Defining initial interoperability standards, and influencing and migrating to a standards-based approach where gaps exist.

A major issue still remains. It is imperative to ensure that products and system components correctly implement these standards and options so that interoperability is actually realized. A number of initiatives within the Government and the private sector exist to address this issue.

These include the following:

- **Automotive Network eXchange® (ANX)**. The automotive industry has recognized the importance of interoperability for the transmission of trading partner electronic information. The ANX network service is positioning itself to provide automotive trading partners with a single, secure network for electronic commerce and data transfer, replacing the complex, redundant, and costly multiple connections that exist throughout the automotive supply chain.
- **International Computer Security Association (ICSA)**. The ICSA promotes the open exchange of information between security product developers and security service providers. ICSA acts as an independent third party that offers a number of initiatives, including a product certification program. ICSA certification develops criteria by which industry wide categories of products are tested. It certifies products on an annual basis and spot-checks for compliance throughout the year against the latest version of each product. Through use of this process, buyers of ICSA-certified products can be assured that they are getting the most secure products available at the time.
- **National Information Assurance Partnership (NIAP)**. The NIAP is a joint industry-government initiative, led by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to establish commercial testing laboratories where industry product providers can have security products tested to verify their performance against vendor claims. As with the ICSA initiatives, a natural result of this testing will be user assurance that products advertising compliance with standards will indeed be interoperable.

These activities, and a number of others similar to them, will help product and system providers deliver solutions that support the interoperability needs of their broad customer base.

The interoperability strategy presented in this section is embodied throughout the IATF. In a later release of the IATF document, a more detailed treatment of specific issues affecting interoperability will be included in subsequent sections. Specifically, IATF Chapters 5 through 9 will include discussions of interoperability issues specific to each of the user requirement categories. These will include interoperability concerns or needs reflected in the captured requirements, technology assessments (to identify the degree to which the available solutions deal with interoperability issues), and recommendations (that deal with selection of architectures and protocols that achieve the needed interoperability). Chapter 8, Supporting Infrastructures will deal with interoperability issues associated with KMI/PKI.

4.7 Key Management Infrastructure/ Public Key Infrastructure Considerations

A KMI/PKI capability is needed to support most technical security countermeasures. This section provides a high-level discussion of the role of, and features associated with, a KMI/PKI. Detailed guidance on the architecture of KMI/PKI can be found in Chapter 8, Supporting Infrastructures.

4.7.1 KMI/PKI Overview

The KMI/PKI process generates, distributes, and manages security credentials. It can be considered as a set of interrelated activities providing security services that are needed to enable the framework's security solutions presented in IATF Chapters 5, 6, 7, and 9. KMI/PKI is a unique user requirement category in the IATF because it does not directly satisfy a user's security requirements; rather, it facilitates the use of security building blocks that are needed by other security mechanisms.

Current KMI/PKI implementations consist of numerous stovepipe infrastructures that support different user solutions. These are run by various organizations, even though the end user may need support from several stovepipe infrastructures for a single application. A complete system approach to any network security solution must include a KMI/PKI architecture that provides effective and efficient operations while maintaining the requisite security features and assurances.

A KMI/PKI architecture depends heavily on the specific applications it supports. For example, a VPN provides an encrypted pipe between two enclaves. The KMI/PKI provides keys and certificates to the cryptographic devices that provide authentication and encryption to establish and maintain the pipe. KMI/PKI could also provide additional services, including data recovery and a directory to provide access to users' public certificates.

A second way in which KMI/PKI differs from other solutions in the IATF is that its security is distributed through a number of separate elements. These elements require extensive security (e.g., encryption, certificate management, compromise recovery) among themselves to protect the user's key or certificate. Because of the serious repercussions of a successful attack against the KMI/PKI, internal infrastructure security requirements are often more stringent than is user services security. There are also unique requirements for the infrastructure (e.g., policy management), and the level of assurance for the KMI/PKI services is often higher.

4.7.2 KMI/PKI Operational Services

Four operational services are supported by the KMI/PKI. These services support different user applications and consequently employ different (but related) mechanisms and have unique security requirements. The first user service is symmetric key generation and distribution. This is still the primary key management mechanism within the classified community.

The second service, PKI, addresses both digital signature (for authentication and integrity) and key agreement with its associated certificate management. This is the primary key management mechanism within the commercial community.

The third service, directory service, is used to provide access to the public information required with PKI, such as the public certificate, the related infrastructure certificates, and the compromised-key information. Directory services can be provided either by a global set of distributed directories (e.g., X.509 Defense Message System [DMS] directories), or by an on-line repository at a single site. Although directories can be used for other things, they are normally very closely coupled with PKI.

The final service is managing the infrastructure itself. The distributed nature of the infrastructure places additional functional and procedural requirements on the KMI/PKI, and the sensitivity of the application imposes additional security requirements on the KMI/PKI. The internal structure of the infrastructure varies with the application it supports.

These services are discussed in greater detail in Section 8.1.

4.7.3 KMI/PKI Processes

KMI/PKI consists of a numerous processes that all must work together correctly for a user security service to be truly secure. Each of these processes is necessary at some level in all KMI/PKI architectures. The processes include the following:

- **Registration.** Enrolling those individuals who are authorized to use the KMI/PKI ..
- **Ordering.** Requesting the KMI/PKI to provide a user with either a key or a certificate.
- **Key Generation.** Generating the symmetric or asymmetric key by an infrastructure element.
- **Certificate Generation.** Binding the user information and the asymmetric key to a certificate.
- **Distribution.** Providing the keys and certificates to the user in a secure, authenticated manner.
- **Accounting.** Tracking the location and status of keys and certificates.

- **Compromise Recovery.** Removing invalid keys and certificates from the system in an authenticated manner.
- **Rekey.** Periodically replacing keys and certificates in a secure, authenticated manner.
- **Destruction.** Destroying the secret key when it is no longer valid.
- **Data Recovery.** Being able to recover encrypted information without direct access to the original key.
- **Administration.** Running the infrastructure.
- **Value-Added PKI Processes.** Supporting optional value-added processes, including archive, time stamp, and notary service (PKIs only).

The complete set of KMI/PKI processes is usually distributed to several elements performing independent tasks, requiring extensive coordination and security processing between elements. For most processes, there are numerous ways of implementing the services, based on the application supported, the security required, and the cost (e.g., money, people, and performance) the user is willing to pay. Each process contributes to the overall security of the KMI/PKI and is associated with various forms of attacks and countermeasures.

References

1. Humphrey, Jeff and Gabrielson, Bruce "Phreakers, Trashers, and Hackers," presented at AFSEA INFOSEC Engineering Course, 1995, Burke, VA. http://blackmagic.com/ses/bruceg/hackers.html

2. Reserved.

3. Coast Security Pages at http://www.cs.purdue.edu/coast/intrusion-detection/.

4. FIPS PUB 140-1, National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, http://www.itl.nist.gov/div897/pubs/fip140-1.htm.

5. NSTISSI No. 4009, National INFOSEC Glossary.

6. Common Criteria for Information Technology Security Evaluation. CCIB-98 (ISO/IEC 15408), version 2.0, 1998, http://csrc.nist.gov/cc/.

7. DoD Reg. 5200.1-R, Information Security Program, 1997.

8. NSTISSAM TEMPEST/1-92 Compromising Emanations Laboratory Test Requirements Electromagnetics, 1992.

9. Laing, Alan "DoD PKI Level of Protection and The Appropriateness of Proposed Solutions for Various Applications" (Draft) 1998.

10. National Security Agency Specification for General Functional Security Requirements for a Telecommunications System (FSRS), 1989.

11. Information Systems Security Engineering Handbook, Release 1.0, 28 February 1994.

12. Security Management Infrastructure (SMI) Task 1 Team, Threat and Vulnerability Model for Information Security, 1997.

Additional References

a. NSA/CSS Dir. No. 120-1 NSA/CSS Operations Security Program, 1990.

b. National Security Agency Specification for Unified INFOSEC Criteria, 1991.

c. Ford, Warwick: *Computer Communications Security,* Englewood Cliffs, NJ: Prentice Hall PTR, 1994.