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

Special Publication 800-36 (Draft)

Guide to Selecting Information Technology Security Products

Recommendations of the National Institute of Standards and Technology

Timothy Grance
Marissa Myers
Marc Stevens

THIS PAGE INTENTIONALLY LEFT BLANK.

NIST Special Publication 800-36 (Draft)

Guide to Selecting Information Technology Security Products

Recommendations of the National Institute of Standards and Technology

Timothy Grance, Marissa Myers, Marc Stevens

COMPUTER SECURITY

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

October 2002

U.S. Department of Commerce

Donald L. Evans, Secretary

Technology Administration

Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology

Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

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

National Institute of Standards and Technology Special Publication 800-36
Natl. Inst. Stand. Technol. Spec. Publ. 800-36, ## pages (Oct. 2002)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2002

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

Acknowledgements

The authors, Timothy Grance of NIST, and Marissa Myers and Marc Stevens of Booz Allen Hamilton, wish to express their thanks to the staff at NIST and at Booz Allen Hamilton who reviewed drafts of this document and provided valuable insights that contributed substantially to the technical content of this document.

Executive Summary

The selection of IT security products is an integral part of the design, development and maintenance of an IT security infrastructure that ensures confidentiality, integrity, and availability of mission critical information. This guide, NIST Special Publication 800-36, *Guide to Selecting Information Technology (IT) Security Products*, first defines broad security product categories and specifies product types within those categories. It then provides a list of characteristics and pertinent questions an organization should ask when selecting a product from within these categories.

The selection of IT security products follows the risk management process of identifying the most effective mix of management, operational, and technical controls. A security program should include an appropriate mixture of security controls: management, operational, and technical. The specific blend of security controls an organization employs is tied to the mission of the organization and the role of the system within the organization as it supports that mission. Risk management is the process used to identify an effective mixture of controls. Once the necessary controls are identified, IT security products can then be identified to provide for these controls using the considerations and questions discussed in this document.

The guide will help the reader make sense of the IT security product market, and will assist in choosing IT security products that meet an organization's requirements. It should be used with other NIST publications to develop a comprehensive approach to managing, satisfying, and verifying an organization's computer security and information assurance requirements, including

+ NIST Special Publication 800-30*, Risk Management Guide for Information Technology Systems*

+ NIST Special Publication 800-27, *Engineering Principles for Information Technology Security: A Baseline for Achieving Security*

+ NIST Special Publication 800-23*, Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Test/Evaluated Products*

+ NIST Special Publication 800-4A, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Official.*

Depending on the product category, other NIST Special Publications may be relevant:

+ NIST Special Publication 800-41*, An Introduction to Firewalls and Firewall Policy*

+ NIST Special Publication 800-32*, Introduction to Public Key Technology and the Federal PKI Infrastructure*

+ NIST Special Publication 800-31, *Intrusion Detection Systems*.

The following computer security product categories are covered in this document, with a discussion of the types of products, product characteristics, and environment considerations for each category:

- Identification, Authentication, and Authorization
- Access Control
- Intrusion Detection
- Firewall
- Public Key Infrastructure
- Virus and Malicious Code Protection
- Forensics
- Media Sanitizing.

In addition to a specific discussion of these product categories, the document recommends the following general considerations when selecting IT security products:

- Organizational considerations should include identifying the user community; the relationship between the security product and organization's mission; the sensitivity of the data; the organization's security requirements and security plan, policies, and procedures; and operational issues such as daily operation, maintenance, and training.
- Product considerations should include determining total life-cycle support, ease-of-use, scalability, and interoperability requirements; identifying test requirements; reviewing known vulnerabilities; testing and implementing relevant patches; reviewing product specification with respect to existing and planned organizational program, policies, procedures, and standards; identifying security critical dependencies on other products; and investigating the new product's interface with the existing infrastructure.
- Vendor considerations should include whether the selection of a particular product will limit future security choices; vendor experience; and vendor history in responding to security flaws in its products.

TABLE OF CONTENTS

1. Introduction

1.1 Authority

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

These guidelines are for use by federal organizations that process sensitive information. They are consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Appendix III.

This document may be used voluntarily by nongovernmental organizations. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the OMB, or any other federal official.

1.2 Purpose and Limitations

A secure information infrastructure ensures confidentiality, integrity, and availability of mission critical information. Information technology (IT) security products are an integral component in the design, development, and maintenance of this secure infrastructure. It is important that IT security products operate as they were intended to provide a foundation for this secure infrastructure.

The confidence that security products work as intended is the basis for the concept of security assurance. Varying degrees of assurance are supported through methods such as conformance testing, security evaluation, and trusted development methodologies. Assurance is not, however, a guarantee that the products work as intended in an operational (i.e. installed) environment. National Institute of Standards and Technology (NIST) Special Publication 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, provides recommendations to organizations that process sensitive information for the acquisition and use of security-related IT products.

This guide builds upon Special Publication 800-23 by describing several categories of IT security products and their characteristics. It also provides a set of questions that should be considered when procuring these products. This guide does not provide an exhaustive list of all IT security product categories as the commercial marketplace for IT security products is constantly changing. However, the questions provided in this guide can easily be modified for an organization's particular needs.

This guide should also be used in conjunction with Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, in developing the full set of security controls necessary for an organization to protect and secure its infrastructure.

Vast amounts of IT security products are readily available for purchase in the commercial market. This guide will help the reader make sense of this IT security product market and assist in choosing IT security products that meet an organization's requirements.

This guide seeks to help organizations make informed decisions when selecting computer security products. The categories of products listed here include operational controls such as intrusion detection and technical controls such as firewalls. This guide should be used with other NIST publications to develop a comprehensive approach to the management of an organization's computer security and requirements. The guide first defines broad security product categories and then specifies product types within those categories. This guide explains and provides a list of characteristics and pertinent questions an organization should ask in the selection process.

1.3 Scope

This guide covers the selection of computer security products to be used as operational or technical security controls. It should be used after a risk assessment has been performed and the need for security controls established. This guide does not discuss how an organization should develop its overall computer security program or the optimal set of products that should be implemented. This guide covers many computer security product categories, but it is not exhaustive in its coverage.

For information on the overall system security requirements analysis process and methods for incorporating computer security in IT procurements, see NIST Special Publication 800-4, *Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials*. For information on performing a risk assessment, see NIST Special Publication 800-30. For information on all security controls for an IT system, see NIST Special Publication 800-27, *Engineering Principles for Information Technology Security: A Baseline for Achieving Security*.

1.4 Audience

This guide is written to help an organization during the various stages of the computer security product life cycle. It can be used as a tool by—

- IT Security Officers in conducting the IT risk assessment and building the business case for the procurement of IT security products.

- Chief Information Officers (CIO) and Chief Technology Officers (CTO) in establishing product procurement policy and ensuring that security has been appropriately considered in the selection process.

- IT directors, program managers, and system owners in understanding the types of available security products, what they should consider when making a selection decision, and what factors they should use for evaluating a security product.

Although this document can be used by a number of people in an organization, it will be most useful for those who will be developing and maintaining a secure IT infrastructure.

1.5 Document Structure

This document is organized into five sections:

- Section 1 provides an introduction and describes the people who may benefit from security product guidance.

- Section 2 describes the roles and responsibilities of IT security procurement officials.

- Section 3 provides an overview of security controls, outlining the steps an organization should take before selecting security products.

- Section 4 describes general product selection considerations.

- Section 5 describes security products, specific characteristics that should be considered when selecting a product, and associated environmental questions specific to a particular security product.

2. Roles and Responsibilities

Product selection involves numerous people throughout an organization. Each person involved in the process, whether on an individual or group level, should understand the importance of security in the organization's information infrastructure. Each organization may involve several subordinate organizations during the IT product selection process. The following personnel are listed as a guide. Depending on the organization's needs, one may include all of the personnel listed below or a combination of particular positions relevant to IT security needs. In some small organizations, a single individual may hold multiple roles.

2.1 IT Security Program Manager

IT security program managers are responsible for developing enterprise standards for IT security (i.e., single sign-on, remote access, userid creation). They play a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize IT security risks to the organization. They coordinate and perform system risk analyses, analyze risk mitigation alternatives, and build the business case for the acquisition of appropriate security solutions (including IT security services) that help enable mission accomplishment in the face of real-world threats. These IT security program managers also support senior management in ensuring that security management activities are conducted as required to meet the needs of the organization.

2.2 Chief Information Officer

The CIO is responsible for the organization's IT planning, budgeting, investment, performance and acquisition. As such, the CIO provides advice and assistance to senior organization personnel in procuring the most efficient and effective security product to fit the IT security architecture.

2.3 IT Investment Board (or equivalent)

The IT investment board (or its equivalent) is responsible for managing the capital planning and investment control process defined by the Clinger-Cohen Act of 1996 (section 5). This board can set the investment criteria for security product selection in a qualitative and quantitative environment. The board can review benefits and risks for procuring a particular product and can be involved in examining alternative approaches.

2.4 Program Manager (owner of data) / Procurement Initiator

The program manager represents programmatic interests during the security product acquisition process. Program managers play an essential role in security product selection because of their involvement in strategic planning initiatives and are intimately aware of functional system requirements.

2.5 Acquisition Team

The acquisition team is normally composed of representatives from program, technical, and contracting areas of the organization. It provides a balanced perspective of cost and schedule considerations. Further, the team ensures that security performance and investment objectives have been created and met successfully. Long- and short-term security needs must be considered during the security product selection. Information technology and information resource management personnel provide technical expertise to program management and contracting officers involved in security product selection. They ensure that performance and engineering measures are met.

2.6 Contracting Officer[1]

The contracting officer is the person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

2.7 Contracting Officer's Technical Representative

The Contracting Officer's Technical Representative (COTR) is a qualified Government employee appointed by the Contracting Officer to act as their technical representative in managing the technical aspects of a particular contract.

2.8 IT System Security Officer

The IT System Security Officer is responsible for ensuring the security of an information system throughout its life cycle.

[1] Federal Acquisition Regulation Section 2.101

3. Selecting Proper Security Controls

A security program, whether at the organization or at the system level, should include an appropriate mixture of security controls: management, operational, and technical as described in NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*. Management controls are techniques that are normally addressed by management in the organization's computer security program — focusing on managing the computer security program and risk. Operational controls focus on controls that are operated by people as opposed to a technology or systems. Operational controls often rely on technical expertise, management controls, and technical controls. Technical controls emphasize the security controls that the computer system executes. These controls should be consistent with the operational context and management controls.

Reliance on technical controls alone will be insufficient without complementary management or operational controls. For example, an organization can install a robust firewall; however, if it allows unrestricted dialup access directly to the network, the organization will have significant vulnerabilities.

The number and type of appropriate security controls and their corresponding IT security products may vary throughout a particular system's development and procurement life cycles. The relative maturity of an organization's security architecture may influence the types of appropriate security controls. The blend of security controls is tied to the mission of the organization and the role of the system within the organization as it supports that mission.

Risk management is the process used to identify an effective mix of management, operational, and technical security controls to mitigate risk to a level acceptable to the responsible senior official. Although it may be tempting to simply pick a product off the shelf, using a risk management process to choose the most effective blend of controls enhances an organization's security posture. A risk management process, as described in NIST Special Publication 800-30, comprises three main phases: risk assessment, risk mitigation, and risk evaluation and assessment.

In the risk assessment phase, an organization analyzes identified threats and vulnerabilities in terms of likelihood of occurrence and expected loss, and determines the impact on its ability to fulfill its mission and/or business objectives. The outcome of this action will be a statement of the anticipated type and amount of damage a threat could cause if a vulnerability were to be exploited successfully. This ensures that security requirements are prioritized and specific to the architecture.

In the risk mitigation phase, the organization identifies the types of controls that could be employed to reduce the level of risk as determined in the risk assessment, to an acceptable level. As mentioned above, these solutions may include management, operational, or technical controls. These controls may require the use of an IT security product For instance, firewall and intrusion detection products can help limit the threats that can impact an organization's IT infrastructure. Once an organization has decided to implement a security product, it should evaluate existing technologies in the context of its own security architecture to determine the best option.

Once the necessary controls are identified, IT security products can then be identified to provide for these controls. In addition, it is important to perform a cost-benefit analysis when selecting security products.[2] As part of the cost-benefit analysis, a life-cycle cost (LCC) estimate for the status quo and each alternative identified should be developed. In addition to LCC estimates, benefits associated with each alternative should be identified and, to the extent practicable, quantified in terms of dollar savings or cost avoidance.

Once all options are weighed in the cost-benefit analysis, the security product selection is made, and implementation of the product can follow.

[2] There may be cases where the cost of a product is relatively low or the benefit is somewhat obvious, i.e. a virus scan product. In these situations, the rigor of a cost-benefit analysis may be reduced.

4. General Considerations

In addition to the topics discussed in the previous chapters, some other important factors should be considered by organizations when acquiring security products. Independent, third-party testing and evaluation of IT products gives consumers greater confidence that the security features in those products work as advertised by the vendor. Testing and evaluation also provides a way to demonstrate product compliance with organization security requirements and public security standards. NIST Special Publication 800-23 provides guidance on security assurance and the use of tested/evaluated products, and should be consulted by organizations selecting security products for their IT systems and networks.

Two prominent security testing and evaluation programs are now in place to assess the security features and assurances of commercial off-the-shelf (COTS) products: (1) National Information Assurance Partnership[1] (NIAP) Common Criteria (CC) Evaluation and Validation Scheme (CCEVS) and (2) NIST Cryptographic Module Validation Program[2] (CMVP). The NIAP CCEVS employs a network of private sector, accredited testing laboratories to independently evaluate commercial security products in a variety of key technology areas against a set of security requirements and specifications from the international standard, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15408, *Common Criteria for IT Security Evaluation*. The CMVP, also using independent, accredited, private-sector laboratories, focuses on security conformance testing of cryptographic modules against Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, and related federal cryptographic algorithm standards. In both programs, a government body validates the results of the testing and evaluation processes to ensure that the security standards are being applied correctly and consistently.

Above and beyond the confidence gained by consumers acquiring security products tested and evaluated under the NIAP CCEVS and NIST CMVP, there is another very important benefit derived from using these programs. The evidence produced during the product testing and evaluation process (available in different forms depending on the program) can be used by systems integrators to build more secure systems and networks. System certifiers can also use this evidence to more effectively assess the security of an IT system in its operational environment in support of system accreditation.

As stated in NIST Special Publication 800-23, particular attention should be given to products that provide the needed security capabilities and have been evaluated under either program. The following set of questions is product independent and should be considered when forming a decision and selecting any product. These questions are organized into three categories: those that apply to the organization, those that apply to the vendor, and those that apply to the product or its operation.

Organizational Questions

- Is the anticipated user community identified? How many and what type of users does the organization anticipate will use the security product?

[1] See http://niap.nist.gov
[2] See http://csrc.nist.gov

- Is the relationship between this security product and the organization's mission performance understood and documented?

- Has the sensitivity of the data the organization is trying to protect been determined?

- Are the organization security requirements supported by the security plan, policies and procedures?

- Have identified security requirements been compared against product specifications?

- Has appropriate procurement language been used for the specific product under selection?

- Have operational issues, such as daily operation, maintenance, contingency planning, awareness, and training, and documentation been considered?

- Have policies been developed for the procurement and use of evaluated products as appropriate? When selecting products, organizations need to consider the threat environment, the security functions needed to cost-effectively mitigate the risks to an acceptable level. Organizations should give substantial consideration to procurement and deployment of IT security products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. Examples of these specifications include protection profiles based on ISO/IEC 15408, the *Common Criteria for IT Security Evaluation*.

- Is communication required across a domain boundary (implies the need for a boundary controller; e.g., sub-system of firewall, intrusion detection system, and/or routers)?

- Are the system components (hardware or software) required for this product identified?

- Is the security product consistent with physical security and other policy requirements?

Product Considerations

- Have total life-cycle support, ease-of-use, scalability, and interoperability requirements been determined? The total life cycle covers "cradle to grave" and hence includes security product disposal requirements.

- Have test requirements, for acceptance and integration testing, and configuration management been developed? If the product has been evaluated under the NIAP-CCEVS or CMVP, validation test reports can be examined to avoid duplication of tests already performed as part of the independent evaluation process.

- Have known product vulnerabilities been addressed by reviewing the relevant vulnerabilities for a product? Known vulnerabilities for some products can be found using the NIST ICAT Vulnerability Search Engine (http://icat.nist.gov).[3]

- Have all relevant patches been tested and implemented?

[3] ICAT is a search engine for an industry standard set of virtually all known vulnerabilities (http://cve.mitre.org) containing links to vulnerability and patch information.

- Have CC protection profiles (PP) been reviewed, when available (http://www.commoncriteria.org/protection_profiles/pp.html), to identify PPs that express security requirements applicable to the organization's needs in the anticipated threat environment? If existing protection profiles are not adequate, consider the usefulness of similar protection profiles as a starting point for examining products that might satisfy requirements applicable to the new environment.

- CC and FIPS 140-1/FIPS 140-2 program Validated Products lists should be reviewed to ensure that evaluated products are used whenever feasible. Products independently tested and validated under NIAP-CCEVS (or mutually recognized) or CMVP provide an organization with some level of security assurance that the security functions of the product work as specified. In general, third party testing and evaluation can provide a significantly greater basis for customer confidence than is available from unevaluated products. Note, however, that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements and vendor reliability, may be neither useful nor cost effective. Organizations should consider their overall requirements and select the best products accordingly.

- Have CC or FIPS 140-1/FIPS 140-2 validated products been revalidated when new releases of the product are issued?

- Have product specifications been reviewed with respect to existing and planned organizational programs, policies, procedures, and standards? Examples include an organization's

  - Web policy

  - Public key infrastructure (PKI) program and policy

  - Smart card program

  - Network interconnection and approval policy.

- Does the product have any security critical dependencies on other products? For example, an operating system (OS) or cryptographic module?

- Does interfacing the new product with the existing infrastructure introduce new vulnerabilities?

Vendor Considerations

- Will the selection of a particular product limit the future choices of other computer security or operational modifications and improvements? (Note: The change and pace of technology may make it difficult to estimate the impact to an organization's future security architecture.)

- Does the vendor have experience in producing high quality IT security products?

- What is the vendor's "track-record" in responding to security flaws in its products?

5. Computer Security Products

The following product categories of security products represent common technological elements helpful in securing infrastructure. This list is not all-inclusive as what constitutes common product types and may change over time. New products are introduced, and obsolete products are removed from the market constantly.

Each security product category discussion consists of four sections. The first is a general discussion of the security capability that this product category provides. The second describes the types of products that are available. Next, general product characteristics are provided. Finally, environmental questions are listed to help further refine the product requirements and assist in product selection.

Specific product vendors or products are not listed. These guidelines are vendor independent and not a review of specific products.

5.1 Identification, Authentication and Authorization

NIST Special Publication 800-12 defines *identification* as the means by which a user provides a claimed identity to the system. Authentication is the means of establishing the validity of this claim. . Authorization is the process of defining and maintaining the allowed actions. Identification and authentication establishes the basis for accountability and the combination of all three enables the enforcement of identity-based access control.

The user's identity can be authenticated using the following mechanisms:

- Requiring the users to identify themselves by something they have (e.g., token)
- Requiring the user to provide something he/she alone knows (e.g., password)
- Sampling a personal characteristic (e.g., fingerprint).

Identification and authentication (I&A) can be assured through electronic means. One example includes the use of public key technology, where a public key certificate is signed by a Certificate Authority (CA). This method provides a unique digital identity for the certificate holder. The public key certificate associates a certificate holder's identity with his public key. A cryptographic protocol allows the certificate holder to prove to the relying party that he possesses the corresponding private key. A relying party uses the certificate to determine the certificate holder's true public key, and proof of the possession of the private key to authenticate that a person is the certificate holder.

The principal forms of authentication include static, dynamic, and multiple factor.

Static. Static authentication reuses a specific authenticator (e.g., static password). This type of authentication only provides protection against attacks in which an imposter cannot obtain the authenticator. The strength of the authentication process is highly dependent on the difficulty of guessing or decrypting the authenticator values and therefore how well they are protected in transit and while stored on the system.

Dynamic. Dynamic authentication uses cryptography or other techniques to create one per-session authenticator. A dynamic authenticator changes with each authentication session between the claimant and verifier. Dynamic authentication typically does not provide protection against "man-in-the-middle" attacks (imposter is inserted in the transmission path) and session stealing (imposter alters the content of information between the claimant and verifier after they have established an authenticated session unless traffic is encrypted).

Multiple Factor. Multiple-factor authentication requires two or more types of authentication techniques and is another type of static authentication. One example is the use of a password along with a smart card token.

Authorization mechanisms fall into four major categories:

Local: Local authorization is performed for each application and machine to which a user requires access. The mechanisms of the local operating system and applications are employed to setup and maintain the authorizations for that machine or application.

Network: _Authorization is performed at a central, authorization server, providing access to a user's account from one or more workstations on the network. The key here is that the access is to a single user account. If the user requires multiple accounts, then each is a separate authorization and handled in like manner to multiple users.

Single Sign-on: Single sign-on employs a central authorization server to enable a user to authenticate one time and achieve access to multiple applications, machines, and domains operating with a variety of authentication mechanisms (for example, a Kerberos implementation within a heterogeneous Windows 2000 and Unix network). The central server contains identifier/authenticator pairs for each domain the user needs to access and performs an authentication on behalf of the user for each resource the user is authorized to access. The central server establishes and maintains, as individual actions, the authorizations at each application, machine, or domain that the user is allowed to access.

Single Log-on: Single log-on is similar to single sign-on with the exception that the central server authentication mechanism is the mechanism used by all the applications, machine, and domains with which the user needs to interact. Rather than store identifier/authenticator pairs for each verification, the one-time verification is accepted by all resources as the only verification needed. Additionally, the authorizations are maintained at the central server and the individual applications, machines, and domains query the central location to determine whether a specific access is authorized. Single log-on eliminates the need for authorization at each resource and for individual authentications to each resource.

5.1.1 Types of Products

Any product that provides an authentication capability beyond passwords and other basic techniques is said to have some level of robustness. Some examples of authentication products that provide varying levels of robust authentication are provided below. The level of authentication robustness needed by the IT system should be determined in the sensitivity assessment that established the need for authentication as a security control.

Security Tokens. Security tokens are used to allow access first to a computer and then to a network. Tokens come in various forms—from Personal Computer Memory Card International Association (PCMCIA) cards to smart cards and software.

PCMCIA Security Tokens. These tokens can offer a full suite of security services in portable format on a small card. Three types of PCMCIA cards exist:

- **Type I cards**—used primarily for adding additional read-only memory (ROM) or random access memory (RAM) to a computer
- **Type II cards**—used for input/output (I/O) devices, such as data/fax modems, local area networks (LAN), and mass storage devices
- **Type III cards**—used for devices whose components are thicker, such as rotating mass storage devices.

PCMCIA cards can protect secret values reasonably well while still leaving room for additional physical tamper protection mechanisms. Disadvantages include a requirement for a PCMCIA card reader. Although prevalent on laptop computers, card readers are not common in desktop computers. The added expense of purchasing a card reader for every desktop workstation may be cost prohibitive.

Smart Card Tokens. Smart cards are credit-card size plastic cards with an embedded computer chip. The chip can be either a microprocessor with internal memory or a memory chip with nonprogrammable logic.

The chip connection is made by either direct physical contact or remotely via a contactless electromagnetic interface. These two categories of smart cards are termed contact and contactless.

A contact smart card requires insertion into a smart card reader with a direct connection to a conductive micromodule on the surface of the card (typically, gold plated). It is via these physical contact points that transmission of commands, data, and card status takes place.

A contactless card requires only proximity to a reader. Both the reader and the card have antenna, and it is via this contactless link that the two communicate. Most contactless cards also derive the internal chip power source from this electromagnetic signal.

Two additional categories that are derived from the contact and contactless cards are Hybrid cards and Combi cards. A Hybrid card has two chips, each with its respective contact and contactless interface. The two chips are not connected; however for many applications, this Hybrid serves the needs of consumers and card issuers who need both contact and contactless functionality. The Combi card is in a single chip card with a contact and contactless interface. With Combi cards, it is now possible to access the same chip via a contact or contactless interface, with a very high level of security.[4]

Certificates. Methods such as certificates use PKI to authenticate digital signatures. (See Section 5.5, Public Key Infrastructure, for further details.)

[4] http://www.scia.org/knowledgebase/default.htm

Authentication Protocols. These protocols are used to determine who is accessing a resource. Examples include the following:

- **RADIUS**. Using the Remote Authentication Dial-In User Service (RADIUS) protocol, a remote client can exchange authentication, access control, accounting, and device configuration information with a RADIUS server. The RADIUS server can authenticate a user or a device from its database or user I&A parameters.

- **TACACS+**. Terminal Access Controller Access Control System + (TACACS+) protocol enables a network resource to offload the user administration to a central server.

Biometrics. Biometrics are used for physical access control, electronic access control, and monitoring devices. An organization's choice of biometric control depends on the security level required, enrollment success rates, and costs incurred.

Biometrics is a method used to identify and authenticate an individual based on personal characteristics. Examples of personal characteristics include fingerprints, face, retina, iris, speech, handwriting, hand geometry, and wrist veins.

All biometrics use a similar procedure to generate templates for comparison. This process involves two phases: enrollment and matching. In the enrollment phase, the user presents a biometric trait, which is captured, extracted, and converted into a mathematical code for storage. When the user wishes to access the system, the user presents the biometric trait a second time to be compared and matched with the original template. Systems can match in two ways: verification or recognition. In verification systems, the second image is compared with the baseline original template to verify the person's claimed identity. When a user submits the biometric in recognition systems, the system searches the entire database for a matching original template. One benefit of verification matching is the ability for remote authentication. The original template is encrypted and stored in the user's token (e.g., smart card). In this case, the remote authentication device does not need access to the database; it need only extract the presented biometric trait and match it to the template decrypted from the token to perform the authentication.

Errors produced by biometrics products can be categorized as either type I or type II. Type I errors are referred to as "accept in error." This type of error is the one of most concern as an imposter could be accepted by the system. Organizations that are considering a system with a high type I error rate should consider using additional security products to complement the biometric product. Type II errors are referred to as "deny in error." These errors usually add inconvenience to those who use them as deny access by legitimate users.

Biometrics can also be combined with passwords, personal identification numbers (PIN), and cards to further increase accuracy and security.

5.1.2 Identification and Authentication Product Characteristics

- Capability of requiring users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.

- Capability of internally maintaining the identity of all active users and as necessary be able to link defined security-relevant actions to specific users.

- Capability of supporting organization password policies, including length, complexity, and lifetime.
- Advanced capabilities, such as antispoofing and allowing the use of tokens such as smart cards.
- Provisions for efficient identification (ID) of users and password or token management.
- A secure I&A management capability that stores and transmits I&A data in encrypted form.
- Ability to log defined security events and sends alerts messages to the appropriate security administrators.

5.1.3 Environment Questions

Smart Card Specific

Organizational Considerations

- How many individuals in the organization will use the product?
- How will the organization issue the cards?
- Will the organization use an automated database system to enter user-specific information onto the cards, or will manual processes be applied? Where will the database reside?
- Who will control the cards?
- Will readers be distributed to ensure that the implementation will be effective?
- Does the organization plan to use the card as the sole means of authentication?

Product Considerations[5]

- What major functions will the card be expected to perform?
- What kind of data will the card be used to store?
- What are the memory requirements for the card?

Biometric Specific

Organizational Considerations

- How many individuals does the organization seek to use the product and what is the distribution of biometric characteristics in the enrolled population?

[5] NIST Interagency Report 6887, Government Smart Card Interoperability Specification (GSC-IS), v2.0 defines an architectural model for interoperable smart card service provider modules.

- What areas does the organization plan to protect with the product—physical access, electronic access, or as a monitoring device?
- What levels of funds are available for deploying biometrics?
- Is the organization more concerned with false positives (incorrectly admitting an unauthorized person) or false negatives (incorrectly denying access to an authorized person), and how much error is tolerable?

Product Considerations

- How well does the product automate enrollment, verification, and identification?
- Is the enrolled template stored locally on a card or in the reader, or is the enrolled template stored remotely in a central database? Are the communication paths between the offered template and enrolled template protected?
- Is biometric information encrypted between the device and the host?
- Does either the enrolled template or threshold change with each successful verification?
- Does the system log accepted and failed attempts?
- Can end users enroll themselves?
- Does the application support remote enrollment?
- Does the application support remote access?
- Is the application interoperable with smart cards?
- Can the user protect individual files/folders/partitions on the hard disk?

5.2 Access Control

Access control ensures that all access to resources is authorized where necessary. Access control protects confidentiality and integrity and supports the principles of legitimate use, least privilege, and separation of duty.

A primary objective of an operating system is to manage the system resources. Access control measures for computer systems focus on assurances that sufficient management, operational, and technical controls are implemented to protect sensitive data and system or network components commensurate with risk. Access control simplifies the task of maintaining enterprise network security by reducing the number of paths that attackers might use to penetrate system or network defenses.

Access control systems grant access to information system resources to authorized users, programs, processes, or other systems. Access control may be managed solely by the application, or it may use controls on files. The system may put classes of information into files with different access privileges. Controlling access can be based on any or a combination of the following:

- User identification
- Role memberships
- Group membership
- Other information known to the system.

By controlling who can use an application, database record, or file, an organization can help to protect that data. Particular importance should be paid to controlling who is allowed to enable or disable the security features or to change user privileges.

Users need to ensure that secure applications sufficiently manage access to data they maintain. The access control process includes any or all of the following: knowing who is attempting access, mediating access according to some processing rules, auditing user actions, and managing where or how data is sent.

5.2.1 Types of Products

Access Control Lists. Access control lists (ACL), which are often combined into larger technology packages, are used for authorizing access to network resources. Lists can be administered offline and then distributed to various routers and other network devices. Lists also may be stored online locally or accessed from a central server.

An access control product may use the following mechanisms for achieving its security objects:

Traffic Filters. Access controls can be enforced effectively at the data packet layer. A filter can block any packet that does not conform to security policy rules. Filters can be assigned to incoming or outgoing traffic. Filtering can be based on source and destination addresses, protocol types, and information from other fields within the packets unless the contact is encrypted.

Policy Filters. Policy filters can be used to set up access control policies on routers. Policy filters, which operate to and from routing tables, can be used to specify the routers or networks from which updates will be accepted.

Role-Based Access Control. Because ACLs can be cumbersome when used to enforce enterprise-level security policies, role-based access control (RBAC) has emerged as a promising feature of many database management, security management and network operating system products. The essential advantage of RBAC products is that they allow system administrators to assign individual users into roles. The role identifies users as members of a specific group, based on their capabilities, work requirements, and responsibilities in the organization. Access rights, or security privileges, are then established for each role; a user may belong to multiple roles, which provide the appropriate level of access for their requirements. Thus, the RBAC structure empowers administrators with a tool to regulate which users are given access to certain data or resources, without limiting them the “all or nothing” tradition of an ACL.

5.2.2 Access Control Product Characteristics

- Can support risk-based granularity of control (e.g., access rights assigned by paragraph, page, or file/message)

- Can allow simultaneous profile/rule assignment to a list of user accounts
- Can define access privileges for each user
- Can prevent unauthorized forwarding of information
- Can provide for a central administration console for management and enforcement of security policies across distributed systems, if the product will be managed centrally
- Can self-protect against outside attack
- Can provide support for sophisticated rules checking
- Can support content filtering (e.g., objectionable content, malicious code, viruses)
- Is extensible to add cryptographic algorithms and add/modify filters
- Can track access and encrypt log files.

5.2.3 Environment Questions

Organizational Considerations

- The organization should determine via risk assessment what system assets must be protected and to what level, such as individual Web pages system/network components (e.g., applications, databases, “legacy” systems, devices, and connections) and remote user connections. If a network is involved, what is its operational paradigm—that is, unicast (point-to-point network, such as Ethernet), multicast, or broadcast? An organization’s answer will determine the type of access control product.
- What is the current infrastructure? Some products require the purchase of third-party applications, such as Relational Database Management Systems (RDBMS) (for storage of security databases) and Java server pages. The cost and complexity of the setup may be higher if these third-party applications are not already present.
- Role-based access control is most effective when roles closely reflect the actual hierarchy of the organization for which it will be used. For example, a senior human resources administrator may require assignment to multiple roles, whereas a clerk might only need the access associated with a single role.
- For sensitive security rules data, should user access scripts, password data, etc., be stored in encrypted form or via some protection mechanism?
- What is the sensitivity of the protected network versus external network(s)? Is a trusted OS/trusted guard suggested?
- What is the direction of flow for which access control is required? Is it inbound/outbound or only inbound?
- Is there a single “super administrator” or support for delegation of authority to “subadministrators” with limited responsibility (e.g., user subsets or resource subsets)?

Product Considerations

- Which of the following access control method(s) does the product support and which is needed:
  - Internet Protocol (IP) address based
  - Individual user based (authentication: support for simple or strong?)
  - Group based
  - Role based (user authenticated and assigned a role, with access controlled based on that role)
  - Sophisticated/granular rules based.
- If the product supports access control based on defined rules, what is the granularity of the rules supported: access control per user, group, or role?
- What attributes or conditions of access are supported (e.g., type of transaction performed, time frame/frequency of transaction type, or physical/IP address origination)?
- Can the product limit specific transaction types (execution, creation, reading, writing, deletion and renaming) for a particular file or device types system wide or on selected components?
- Where is integration required—for example, types of applications, operating systems, etc.?
  - Some products support only Web applications or Web-enabled legacy applications, and then only certain applications without workarounds or modifications to application output.
  - What are the organization's existing user account directories and security databases?
  - To what level of granularity do the system's objects (e.g., files, directories/folders, components) need to be protected?
  - Can the access control product protect individual devices (e.g., floppy disks, compact disks–read-only memory [CD-ROM], serial and parallel interfaces, and system clipboard)?
- What is the logging capability for audit purposes?
- What is the complexity of installation, configuration, and use of the product's system administration function?
  - Does the product provide for easy definition and editing of access control rules, and of user/group permissions/accounts?
  - Does the product support remote administration?

  - Does it have a Hypertext Markup Language (HTML)/browser-based administrative interface or other graphical user interface (GUI)?

- Can the product support the enterprise's PKI/token/certificate authentication method?

- Is the product limited to supporting certain kinds of security rules/user account databases/directories (e.g., Lightweight Directory Access Protocol [LDAP]-only, X.500-only, or specific RDBMS brand name)?

  - Will the product work with current directories (e.g., LDAP, X.500) to store rules logic and user account information, or does it use a proprietary database or third-party RDBMS (if so, which ones)?

  - If the former, are any changes needed to the directory schema to accommodate additional security content? If the latter, is the database bundled with the system, or must it be purchased separately?

  - How transparent is the security rules/user account database made to the systems administrator by the security administrative application?

  - Does an import feature exist that enables the database to automatically import user account information from existing directories?

  - If the organization will be using existing account directories with the product, what are the performance and security implications if directories are regularly shadowed/replicated?

- Can the product interoperate with security domains and databases on other systems?

- Is support for remote user access required?

- What support does the product provide for laptops/notebooks, personal digital assistants (PDA), and IP-based phones?

- Is the product centralized (e.g., central security server) or distributed (e.g., agent based, client proxy based)? Are changes required to servers or clients? If the product is agent based, will all systems in the organization require agents?

- Is the product integrated with an intrusion detection system (IDS) and/or firewall to enable automated (preprogrammed) access changes (e.g., intruder lockout) based on perceived potential hacker events?

- Are there mechanisms for immediate dissemination and implementation of access right changes?

- What is the requirement for support of component-level redundancy (with hot switchover to backup in case of failure) and scalability to accommodate growing enterprise/user base?

- Is there support for predeployment testing and verification of access rules?

- Are any standard application programming interfaces (API) provided for extensibility and integration with other tools (e.g., C++, C, and Java)? Must APIs be purchased from or custom developed by the vendor?

- Are other security functions provided (e.g., virus scanning, integrity controls, user, and password management)?

- Can the product encrypt and decrypt the transmission of files and directories? Will the product allow secure socket layer (SSL) encryption between a client browser and a security server so that no encryption is required on the backend systems being protected?

5.3 Intrusion Detection

Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of *intrusions,* defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by any of the following: attackers who access systems from the Internet, authorized system users who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them. IDSs are software or hardware products that automate the intrusion monitoring and analysis process.

The implementation of an IDS might be valuable in mitigating perceived risks for the following reasons:

- Prevention of problem behaviors by increasing risk of discovery and punishment for system intruders

- Detection of attacks and other security violations that are not prevented by other security measures

- Detection of preambles to attacks (network probes and other tests for existing vulnerabilities)

- Documentation of the existing threat to the organization

- Quality control for security design and administration

- Provision of useful information about methods used in intrusions.

There are two different approaches to analyzing events to detect attacks: misuse detection and anomaly detection. Either or both of the approaches could be used in an IDS product.

Signature-Based Detection[6]. This approach identifies authorized users' misuse of computing resources. Such activity may include visiting unauthorized Internet sites, navigating around a system to areas that have been explicitly identified as "off-limits," or using an application for activity unrelated to work. Misuse detection systems typically rely on comparison against a predefined pattern of events that describe a known attack. These patterns are called signatures.

Anomaly Detection. Anomaly detection assumes that all intrusive activities deviate from the norm. These tools typically establish a normal activity profile and then maintain a current

[6] Signature-based detection is sometimes referred to as misuse detection. Misuse detection is more explicitly defined as detecting insiders who abuse privileges given them.

activity profile of a system. When the two profiles vary by statistically significant amounts, an intrusion attempt is assumed.

NIST Special Publication 800-31, *Intrusion Detection Systems*, provides a more complete description and discussion of the important issues that should be considered when acquiring an IDS.

5.3.1 Types of Products

Three common types of IDS products are network based, host based, and application based.

Network-Based IDS. These IDSs detect attacks by capturing and analyzing network packets. Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts.

Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network. These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console. Because the sensors are limited to running the IDS, they can be more easily secured against attack. Many of these sensors are designed to run in “stealth” mode, making it more difficult for an attacker to determine their presence and location.

Host-Based IDS. Host-based IDSs operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the OS. Furthermore, unlike network-based IDSs, host-based IDSs can more readily “see” the intended outcome of an attempted attack, because they can directly access and monitor the data files and system processes usually targeted by attacks.

Host-based IDSs normally use information sources of two types: operating system audit trails, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system; therefore these trails are more detailed and better protected than system logs. Some host-based IDSs are designed to support a centralized IDS management and reporting infrastructure that can allow a single management console to track many hosts. Others generate messages in formats that are compatible with network management systems.

Application-Based IDS. Application-based IDSs are a special subset of host-based IDSs that analyze the events transpiring within a software application. The most common information sources used by application-based IDSs are the application’s transaction log files.

The ability to interface with the application directly, with significant domain or application-specific knowledge included in the analysis engine, allows application-based IDSs to detect suspicious behavior due to authorized users attempting to exceed their authorization. This is because such problems are more likely to appear in the interaction among the user, the data, and the application.

5.3.2 Intrusion Detection Product Characteristics

Desired characteristics of an effective IDS areas follows:

- Should run continually
- Should be fault tolerant
- Should resist subversion
- Should impose minimal overhead on the system
- Should observe deviations from normal behavior
- Should be easily tailored to the system in question
- Should cope with changing system behavior over time as new applications are being added
- Should be difficult to fool
- Should be easily maintained
- Should be based on proven systems that provide periodic IDS signature updates
- Should be able to log events to a secure location and be able to send alert messages to the appropriate security administrators
- Logs should be accessible for review on a daily basis from a secure location.

5.3.3 Environment Questions

Organizational Considerations

- Is the system compatible with the organization's current security architecture?
- Can the system identify insider attacks?
- Does the organization want to use the output of its IDS to determine new security requirements?
- Does the organization want to use the IDS to maintain managerial control (nonsecurity related) over system or network usage
- What is the budget for acquisition and life-cycle support of intrusion detection hardware, software, and infrastructure?

Product Considerations

- Is the product sufficiently scalable for your present and projected environment?
- Has the product been tested—against functional requirements and against attack?
- What is the level of expertise required by operators of the product?
- Is the product designed to evolve as the organization grows?

  - Can the product adapt to growth in security administrator expertise?
  - Can the product adapt to growth and change of the organization's systems infrastructure?
- What are the general support requirements for the product?
- What support will the vendor provide for product installation and configuration support?
- What is the vendor commitment for ongoing product support?
  - Are subscriptions to signature updates included?
  - How often are subscriptions updated?
  - How quickly after a new attack is made public will the vendor ship a new signature?
  - Are software updates included?
  - How quickly will software updates and patches be issued after a problem is reported to the vendor?
  - Are technical support services included, and if so, what is the vendor's commitment to timely response?
  - What alternatives does the vendor offer for contacting technical support (e.g., e-mail, telephone, online chat, and Web-based reporting)?
  - Are there any guarantees associated with the IDS?
  - What training resources does the vendor provide as part of the product?
  - What additional training resources are available from the vendor and at what cost?

5.4 Firewall

Network firewalls are devices or systems that control the flow of network traffic between networks employing differing security postures. A firewall acts as a protective barrier because it is the single point through which communications pass. Internal information that is being sent outside a network passes through a firewall as it leaves a network. Incoming data can enter the network only through the firewall. This section is drawn from NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*. This publication provides details of firewalls and firewall product selection that are beyond the scope of this document.

In most modern applications, firewalls and firewall environments are discussed in the context of Internet connectivity and the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. However, firewalls have applicability in network environments that do not include or require Internet connectivity. For example, many corporate enterprise networks employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or personnel department. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas. The inclusion of a proper firewall or firewall environment can therefore provide an additional layer of security that would not otherwise be available.

Although firewalls afford protection of certain resources within an organization, there are some threats that firewalls cannot protect against: connections that bypass the firewall; new threats that have not yet been identified; and viruses that have been injected into the internal network. It is important to remember these shortcomings because considerations will have to be made in addition to the firewall solution to counter these additional threats and provide a comprehensive security solution.

5.4.1 Types of Products

NIST Special Publication 800-41 describes eight kinds of firewall platforms: packet filter firewalls, stateful inspection firewalls, application proxy gateway firewalls, dedicated proxy firewalls, hybrid firewall technologies, network address translation, host based firewalls, and personal firewalls/personal firewall appliances.

Packet Filter Firewalls. The most fundamental type of firewall is called a packet filter. Packet filter firewalls are routing devices that include access control functionality for system addresses and communication sessions. The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a ruleset.

Packet filter firewalls have two main strengths: speed and flexibility. Packet filter firewalls can be used to secure nearly any type of network communication or protocol. This simplicity allows packet filter firewalls to be deployed into nearly any enterprise network infrastructure. Note that their speed, flexibility, and capability to block denial-of-service and related attacks make them ideal for placement at the outermost boundary with an untrusted network.

Packet filter firewalls possess several weaknesses:

- Because packet filter firewalls do not examine upper-layer data,[7] they cannot prevent attacks that employ application-specific vulnerabilities or functions.

- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited. Packet filter logs normally contain the same information used to make access control decisions (source address, destination address, and traffic type).

- Most packet filter firewalls do not support advanced user authentication schemes.

- They are vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing.

- Finally, s a result of the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

Consequently, packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources are not important.

[7] Above layer 3 in the Open Systems Interconnect (OSI) model: Transport (4), Session (5), Presentation (6), and Application (7).

Because current firewall technology includes many features and functionality, it is difficult to identify a single firewall that contains only packet filter features. The closest example would be a network router employing coded ACLs to handle network traffic.

Stateful Inspection Firewalls. Stateful inspection evolved from the need to accommodate certain features of the TCP/IP suite that make firewall deployment difficult. When a TCP (connection-oriented transport) application creates a session with a remote host system, a port is also created on the source system. This port receives network traffic from the destination system. Packet filter firewalls must permit inbound network traffic on all return packets from the destination system for connection-oriented transport to occur. Opening this many ports creates an immense risk of intrusion by unauthorized users who may employ a variety of techniques to abuse the expected conventions. Stateful inspection firewalls solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding client port. This "state table" is then used to validate any inbound traffic. The stateful inspection solution is more secure because the firewall tracks client ports individually rather than opening all inbound ports for external access.

In essence, stateful inspection firewalls add Layer 4 (transport) awareness to the standard packet filter architecture. Stateful inspection firewalls share the strengths and weaknesses of packet filter firewalls, but because of the state table implementation, stateful inspection firewalls are generally considered to be more secure than packet filter firewalls.

A stateful inspection firewall also differs from a packet filter firewall in that stateful inspection is useful or applicable only within TCP/IP network infrastructures. Stateful inspection firewalls can accommodate other network protocols in the same manner as packet filters, but the actual stateful inspection technology is relevant only to TCP/IP. For this reason, many texts classify stateful inspection firewalls as representing a superset of packet filter firewall functionality.

Application-Proxy Gateway Firewalls. Application-proxy gateway firewalls are advanced firewalls that combine lower layer access control with upper layer (Layer 7–Application Layer) functionality. All network packets that traverse the firewall must do so under software (application-proxy) control.

Application-proxy gateway firewalls have numerous advantages over packet filter firewalls and stateful inspection packet filter firewalls. First, application-proxy gateway firewalls usually have more extensive logging capabilities resulting from the firewall being able to examine the entire network packet rather than only the network addresses and ports.

Another advantage is that application-proxy gateway firewalls allow security administrators to enforce whatever type of user authentication is considered appropriate for a given enterprise infrastructure. Application-proxy gateways can authenticate users directly, as opposed to packet filter firewalls and stateful inspection packet filter firewalls, which normally authenticate users based on the network layer address of the system on which they reside. Given that network layer addresses can be easily spoofed, the authentication capabilities inherent in application-proxy gateway architecture are superior to those found in packet filter or stateful inspection packet filter firewalls. Finally, given that application-proxy gateway firewalls are not simply Layer 3 devices, they can be made less vulnerable to address spoofing attacks.

The advanced functionality of application-proxy gateway firewalls also fosters several disadvantages when compared with packet filter or stateful inspection packet filter firewalls.

First, because of the “full packet awareness” found in application-proxy gateways, the firewall is forced to spend significant time reading and interpreting each packet. Therefore, application-proxy gateway firewalls are not generally well suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a dedicated proxy server can be used to secure less time-sensitive services, such as e-mail and most Web traffic. Another disadvantage is that application-proxy gateway firewalls are often limited in terms of support for new network applications and protocols. An individual, application-specific proxy agent is required for each type of network traffic that needs to transit a firewall. Most application-proxy gateway firewall vendors provide generic proxy agents to support undefined network protocols or applications. However, those generic agents tend to negate many of the strengths of the application-proxy gateway architecture, and they simply allow traffic to “tunnel” through the firewall.

Dedicated Proxy Firewalls. Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic, but they do not contain firewall capability. They are typically deployed behind traditional firewall platforms for this reason. In typical use, a main firewall might accept inbound traffic, determine which application is being targeted, and then hand off the traffic to the appropriate proxy server (e.g., an e-mail proxy server). The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery.

Dedicated proxies allow an organization to enforce user authentication requirements and other filtering and logging on any traffic that traverses the proxy server. The implications are that an organization can restrict outbound traffic to certain locations or could examine all outbound e-mail for viruses or restrict internal users from writing to the organization’s Web server. Security experts have stated that most security problems occur from within an organization; proxy servers can assist in foiling internally based attacks or malicious behavior. Simultaneously, filtering outbound traffic will place a heavier load on the firewall and increase administration costs. Many organizations enable the caching of frequently used Web pages on the proxy, thereby reducing firewall traffic. In addition to authentication and logging functionality, dedicated proxy servers are useful for Web and electronic mail (e-mail) content scanning.

Hybrid Firewall Technologies. Recent advances in network infrastructure engineering and information security have resulted in a “blurring of the lines” that differentiates the various firewall platforms discussed earlier. As a result, firewall products currently incorporate functionality from several different classifications of firewall platforms. For example, many packet filter or stateful inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls. Nearly all major firewall vendors have introduced hybridization into their products in some manner; therefore it is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Hybridization of firewall platforms makes the prepurchase product evaluation phase of a firewall project important. Supported feature sets, rather than firewall product classification, should drive the product selection.

Network Address Translation. Network address translation (NAT) technology was developed in response to two major issues in network engineering and security. Network address translation is an effective tool for “hiding” the network-addressing schema present behind a firewall environment. In essence, NAT allows an organization to deploy an addressing schema of its choosing behind a firewall, while still maintaining an ability to connect to external resources through the firewall. Network address translation is accomplished by one of three methods: static, hiding, and port.

In static NAT, each internal system on the private network has a corresponding external, routable IP address associated with it. This particular technique is seldom used, because of the scarcity of available IP address resources.

With hiding NAT, all systems behind a firewall share the same external, routable IP address. Thus, with a hiding NAT system, many systems behind a firewall will still appear as only one system. This type of NAT is fairly common, but it has one glaring weakness: it is impossible to make resources available to external users once they are placed behind a firewall that employs it. Port address translation is not required to use the IP address of the external firewall interface for all network traffic; another address can be created for this purpose. With port address translation, it is possible to place resources behind a firewall system and still make them selectively accessible to external users.

In terms of strengths and weaknesses, each type of NAT has applicability in certain situations, with the variable being the amount of design flexibility offered by each type. Static NAT offers the most flexibility, but as stated earlier, static NAT is not always practical given the shortage of IP version 4 addresses. Hiding NAT technology was an interim step in the development of NAT technology, but it is seldom used because port address translation offers additional features beyond those present in hiding NAT while maintaining the same basic design and engineering considerations. Port address translation is often the most convenient and secure solution.

Host-based Firewalls. Firewall packages are available in some OSs or as add-ons; they can be used to secure only the individual host. Internal servers should be protected and should not be assumed to be safe from attack because they are behind a main firewall. Host-based firewall packages typically provide access-control capability for restricting traffic to and from servers running on the host, and some limited logging is usually available. Although a host-based firewall is less desirable for high traffic, high-security environments, in internal network environments or regional offices they offer greater security usually at a lower cost. A disadvantage to host-based firewalls is that they must be administered separately; after a certain number, it becomes easier and less expensive to simply place all servers behind a dedicated firewall configuration.

Personal Firewalls/Personal Firewall Appliances. Securing personal computers (PC) at home or remote locations is now as important as securing them at the office; many personnel telecommute or work at home and operate on organization- or agency-proprietary data. Home users dialing an Internet service provider (ISP) may have limited firewall protections available to them because the ISP has to accommodate potentially many different security policies. Therefore, personal firewalls have been developed to provide protection for remote systems and to perform many of the same functions as larger firewalls. These products are typically implemented in one of two configurations.

The first configuration is a personal firewall, which is installed on the system it is meant to protect; personal firewalls usually do not offer protection to other systems or resources. Likewise, personal firewalls do not typically provide controls over network traffic that is traversing a computer system — they protect only the computer system on which they are installed.

The second configuration is a personal firewall appliance, which is in concept similar to a traditional firewall. In most cases, personal firewall appliances are designed to protect small networks such as networks that might be found in home offices. These appliances usually run on specialized hardware and integrate some other form of network infrastructure components in addition to the firewall itself, including the following: cable modem wide area network (WAN) routing, LAN routing (dynamic routing support), network hub, network switch, Dynamic Host Configuration Protocol (DHCP) server, Simple Network Management Protocol (SNMP) agent, and application-proxy agents.

In terms of deployment strategies, personal firewalls and personal firewall appliances normally address connectivity concerns associated with telecommuters or branch offices. However, some organizations employ these devices on the organizational intranet, practicing a defense-in-depth strategy.

Management of the device or application is an important factor when evaluating or choosing a personal firewall or personal firewall appliance. Ideally, a personal firewall or personal firewall appliance should enable the organization or agency to enforce its defined security posture on all systems that connect to its networks and systems. In the case of telecommuters, this means that a personal firewall or personal firewall appliance should enforce a policy at least as restrictive as end-users would experience if they were behind the corporate or agency firewall in the office.

5.4.2 Firewall Product Characteristics

- A firewall environment should be employed to perform the following general functions:
  - Filter packets and protocols
  - Perform stateful inspection of connections
  - Perform proxy operations on selected applications
  - Log traffic allowed and denied by the firewall
  - Provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed
- The firewall should be able to filter packets based on the following characteristics:
  - Protocol (e.g., IP, Internet Control Message Protocol [ICMP])
  - Source and destination IP addresses
  - Source and destination ports (which identify the applications in use)
  - Interface of the firewall that the packet entered

- The proxy operations should, at a minimum, be operable on the content of Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP) traffic.

- A list of evaluated products is maintained by the National Information Assurance Partnership at http://csrc.nist.gov/niap.

5.4.3 Environment Questions

Organization Considerations

- Organizations should use firewalls to secure their Internet connections and their connections to other networks. At remote locations, users should use personal firewalls and firewall appliances to secure their connections to the Internet and ISPs.

- Organizations should view firewalls as their first line of defense from external threats; internal security must still be a top priority. Internal systems must be patched and configured in a timely manner.

- Organizations must monitor incident response team reports and security Web sites for information about current attacks and vulnerabilities. The firewall policy should be updated as necessary. A formal process should be used for managing the addition and deletion of firewall rules.

- Organizations should recognize that all systems administration, especially firewall administration, requires significant time and training. Organizations should ensure that their administrators receive regular training so as to stay current with threats and vulnerabilities.

Product Considerations

- What protocols are supported and/or filtered? Do they include the network-layer (packet/protocol filtering with ACLs), the application-layer (protocol/content filtering [virus checking, active code blocking]), or both?

- Is the product a fully featured application-layer firewall or a firewall router with an ACL-driven packet filter?

- What types of ACLs are supported? Do they include basic (standard and static extended) or advanced ACLs?

- What are the basic ACL criteria: per interface, per network-layer protocol, per IP address and range, and inbound and outbound?

- What type of advanced access control is supported? Do they include context-based access control (CBAC), access by authenticated users only, or application-layer protocol filtering?

- What authentication servers and mechanisms are supported? Do they include TACACS/TACACS+/Extended TACACS, RADIUS, or other?

- What type of network address translation is supported?

- Is firewall “chaining” possible (to distribute filtering functions across a series, for better performance)?
- Are router-to-router authentication supported?
- Is there event logging and auditing?
- Is there router and firewall encryption?
- Is Internet Protocol security (IPSec) support available?
- If SNMP is addressable, does protection exist from an unauthorized administrator?

5.5 Public Key Infrastructure

Many possibilities are made available in the e-business/e-government arena by the interconnectivity of networks and the Internet. To enable these paperless business activities, it is critical to assure that the auditability and legal standing of these electronic transactions are comparable to the paper formats. One method of meeting this requirement is the use of public key technologies and a PKI.

A PKI can be quite complex. Similarly, the strategies for implementing them may range from complete outsourcing of all functionality to building a homegrown PKI from COTS products. The nuances and details of PKI implementation strategies are well beyond the scope of this document. For a detailed treatment of the subject, the following references are highly recommended:

- NIST Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*
- NIST Special Publication 800-32, *Introduction to Public Key Introduction to Public Key Technology and the Federal PKI Infrastructure*
- The Federal Public Key Infrastructure Steering Committee Web site at http://www.cio.gov/fpkisc
- The PKI Web site of the NIST at http://csrc.nist.gov/pki**.**

Discussion of the service aspects of PKI support is addressed in NIST Special Publication 800-35, *Guide to Information Technology Security Services*. This section briefly defines the key concepts of PKI and identifies key criteria for decision making to provide a means for developing an initial purchasing and implementation strategy.

PKI Terms and Introduction. Public key cryptography relies on the concept of a key pair, composed of a private key, which must be kept a secret, and a mathematically related public key. The two basic functions of public key cryptography are as follows:

- **Digital Signatures**. A key holder signs a digital document with his private key, and a relying party can verify that signature with the public key and know with certainty that the document has not been altered in any way since it was signed and that it was signed with the unique private key corresponding to the verification public key.

- **Key Management**. A relying party can use a public key to encrypt or agree to a secret symmetric key to be shared with the private key holder and used in a subsequent message or protocol to encrypt data.

PKI is a systematic means of managing key pairs and associating the names of key holders with their public keys. In a PKI, a trusted CA issues public key certificates to subscribers (e.g., people, organizational entities, or even network devices), typically binding the subscriber's public key to his name and his security and identity attributes. The certificate is digitally signed by the CA, and the public key of the CA is well known to all potential relying parties. Thus, a relying party can verify that he has a subscriber's true public key by verifying the signature on the subscriber's certificate, and then relying on the subscriber's public key in subsequent e-commerce transactions. CAs rely on the services of a Registration Authority (RA) to vouch for the identity of subscribers and to publish certificates and certificate status information to a repository, which is usually a directory accessible via the LDAP protocol.

Subscribers and relying parties use PKI-enabled applications to use PKI in actual e-commerce. These applications, in turn, use PKI clients to perform signing, verification, and key management operations. The digital signature and key management functionality of PKI are used in PKI-enabled applications to achieve authentication, integrity, confidentiality, and nonrepudiation.

5.5.1 Types of Products

Before selecting a CA product, a CA service provider, or PKI clients, an organization should understand the PKI-enabled applications that it wishes to run and the products available for that application. In many cases, it will make sense to select the CA and client type in conjunction with the primary application packages, or to select the applications first and let them drive PKI choices. Once the applications to be supported have been identified and the security policies and requirements associated with them have been defined, the following characteristics will differentiate PKI products.

Key Protection and Cryptographic Modules. The protection afforded private keys is a major factor in establishing the assurance level of a PKI. Agencies should decide what their assurance requirements are and ensure that the kinds of modules needed to achieve that assurance are incorporated in CAs and clients. In most cases, PKI products can use a range of cryptographic modules, but all PKI products do not support all modules. Private keys should always be stored and used in an approved cryptographic module, validated to conform to FIPS 140-2 (140-1 for some older modules). FIPS 140 has four levels of security, 1 to 4, in order of increasing security. The CA cryptographic module should normally be at levels 2 to 4 depending on the sensitivity of the data and transactions being protected. Hardware cryptographic modules are usually more secure than software-based products. In many cases, CAs and RAs will use hardware modules, and subscribers will use software modules, however in some cases many or all subscribers will also use hardware modules.

Cross-Certification and the Federal PKI Architecture. In some cases, organizations will wish to allow their users to use certificates issued by their CA to conduct business with other agencies and organizations. This action requires that the CA be capable of some form of cross-certification, where the CA can issue certificates to other CA's extending trust to that CA, its subscribers, and its associated applications. If this capability is required by the organization, it is critical that the products selected strictly adhere to industry standards. Demonstration of interoperability with a wide variety of CA vendors' products is recommended.

The Federal PKI Bridge CA (FBCA) provides a trust path between PKIs in various agencies. The use of it, however, depends on the use of clients capable of building certification paths of certificates through cross-certificates stored in directories. The FBCA defines certificate policies for four levels of assurance. Technical interoperation with the FBCA is the ability to process certain certificate extensions, including nameConstraint, certificatePolicies, and policyMapping. Agencies wishing to cross-certify with the bridge CA should ensure that the clients, CAs, and directory servers they select can interoperate technically with the Bridge CA and that the products selected support the policy requirements established for the level of assurance. Current policy and interoperability information is available at http://www.cio.gov/fpkisc/documents.

Repositories. CAs typically publish certificates and certificate revocation lists (CRL) to directory servers, and many clients can retrieve the certificates and CRLs they need from directories. Agencies may chose to implement a directory solely for the purposes of PKI, or they may integrate directories into a broad range of applications and services, including PKI. It is easier to build a directory solely for PKI, but also less generally useful.

The LDAP is used by CAs and clients to publish and retrieve certificates and CRLs. Directories are a complex subject in their own right; however, nearly all now support LDAP. A broad consideration of directory issues is beyond the scope of this section; however, agencies implementing PKI should consider their directory plans and needs, and make PKI directory decisions in that broader context.

Key Recovery. Most CA products today offer a key recovery capability for encryption or key management private keys only. (If signature private keys are subject to key recovery, then nonrepudiation is compromised.) Although other key recovery schemes are possible, many CA products offer a feature in which the CA automatically keeps a backup copy of the encryption private key. This copy can be used to recover encrypted data if subscribers lose their key, or are not available to activate their key. Agencies should consider key recovery needs when procuring CA products or PKI-enabled applications that encrypt stored data.

Certificate Status. Certificates may be revoked before they expire. Most CA products can create a list of revoked certificates called a CRL and post it in a repository, and most clients can check such a list. The freshness of this revocation information may be an issue in a PKI; and the CRL features and capabilities of CAs products, services, and clients vary significantly, but support for these features in CA products and clients is not ubiquitous. A wide range of alternative means exists for tracking and managing certificate status in a PKI, each with its own efficiencies and weaknesses. Certificate status and revocation are major issues in the performance and scalability of PKIs and in the assurance level of certificates. The larger the PKI, the more difficult and expensive it is to maintain very fresh status information. High-assurance certificates, however, require a status mechanism that provides fast effective revocation to limit the damage caused by key compromises. Agencies selecting PKI products or services must determine their certificate status requirements. They also must select a system and products that can provide needed status information in a timely manner as the PKI grows in size and scope.

PKI-Enabled Applications. In a sense, the CA, the clients it supports and the entire PKI are "just plumbing." Perhaps the most basic elements to be considered in selecting a CA product or service provider are the applications that are enabled to use the clients supported by the CA. PKI enabled applications and products include the following:

- S/MIME secure E-mail application that can be used to sign and encrypt e-mail. The S/MIME software uses the subscriber's PKI client to perform PKI operations with certificates and keys.

- Web servers and browsers that implement the SSL/Transport Layer Security (TLS) are widely implemented and support not only PKI-based cryptographic authentication of servers and clients but also encryption of traffic in "secure" sessions. Again, the application either relies on a PKI vendor's PKI client or uses a built-in PKI client to perform PKI operations.

- Document-signing products or applications that are used with forms, document management, or workflow products to allow signatures and approvals on electronic documents and to replace signed paper documents.

- Access control that uses certificates and a challenge/signed response protocol to authenticate an identity or privilege for use in access control, and may implement "single sign-on" for a variety or services.

- Products with built-in PKI-enabled access control—for example, firewalls, mail servers, or directory servers. These products often rely on the SSL/TLS protocol.

- File encryption systems that may use public key certificates to manage file encryption keys and to provide for a key recovery capability, if keys are otherwise lost.

5.5.2 PKI Product Characteristics

- The PKI must be designed and implemented in a manner that ensures that the security policies can be enforced.

- The PKI must provide all the functions and capabilities necessary to support the authorized administrators that are responsible for the security management.

- The system should provide for easy key maintenance and secure public and private key backups.

- The selected PKI products must be compliant with applicable federal regulations and policies such as the following:

  – FIPS PUB 140-2: Security Requirements for Cryptographic Modules

  – FIPS PUB 171: Key Management

  – FIPS PUB 46-3: Digital Encryption Standard

  – FIPS PUB186: Digital Signature Standard.

- The PKI must conform to the X.509v3 or PKIX standards. These standards are the basis for most PKI-oriented products. Products not conforming to these standards should be avoided to provide scalability and future interoperability.

5.5.3 Environment Questions

Organizational Considerations

- How critical is the system in meeting the organization's mission?
- What regulations and policies are applicable in determining what is to be protected?
- What threats are applicable in the environment in which the system will be operational?
- What security and cryptographic objectives are required by the system (e.g., integrity, confidentiality)?
- Are users knowledgeable about PKI, and how much training will they undergo?
- The organization should establish assurance objectives to be achieved by the PKI and policies and procedures to support those objectives.
- The process of establishing a complete set of policies to support a PKI can involve addressing numerous difficult issues, including privacy, maintaining assurance (trust) levels, key recovery, and long-term proof of identity and authenticity.
- Interconnection policies with other PKIs should be established.
- Are processes in place to ensure that required assurance levels do not degrade over time?
- Does the vendor or organization have policies for electronically archiving digitally signed documents, possibly for long periods of time?
- The organization must define the coverage of any licenses (e.g., enterprise wide, site specific) and document agreement.
- The organization should determine how difficult it is to migrate from one PKI package to another.

Product Considerations

- Is the product compatible and interoperable with other PKI products/service providers?
- Are there proprietary API dependencies?
- What is the ease of supporting applications (e.g., virtual private networks, access control, secure e-commerce, smart card management, smart cards and hardware, directories, secure messaging, secure forms, and enterprise)?
- Is the product easy to deploy?
- What is the flexibility of administration?
- What is the scalability and portability of installation?

- Does the vendor use interoperable products that fully conform to existing PKI standards?
- Will the organization's PKI accept digital certificates from other PKIs?
- The system should provide for easy key maintenance and secure public and private key backups.
- A determination should be made regarding the maximum number of certificates that the organization would need and whether the service provider could accommodate that number.
- What is the level of effort required for application, database, and OS modification to support system?
- What encryption algorithms and certificate types are supported? Are they user selectable?
    - Is there support for smart cards, PCMCIA tokens, etc.?

5.6 Virus and Malicious Code Protection

Viruses and other malicious code[8] are typically hidden in software and require a host to replicate. Virus and malicious code protection requires strict procedures and multiple layers of defense. Protection includes prevention, detection, containment, and recovery. Protection hardware and access-control software can inhibit this code as it attempts to spread. Most security products for detecting viruses and other malicious code include several programs that use different techniques.

5.6.1 Types of Products

Scanners. Scanners provide precise identification of known malicious code. Scanners search for "signature strings" or use algorithmic detection methods to identify known code. Scanners rely on a significant amount of a priori knowledge about the code.

Integrity Checkers. Integrity checkers detect infections by searching a program or other executable code to determine if it has been altered or changed. Integrity checkers can only flag a change as suspicious; they cannot determine if the change is a genuine virus infection. These programs are usually checksum based. The integrity checking process begins with the creation of a baseline, where checksums for clean executables are computed and saved. Each time the integrity checker is run, it again makes a checksum computation and compares the result with the stored value. Note that several different kinds of checksums are used. Simple checksums are easy to defeat; cyclical redundancy checks (CRC) are better, but can still be defeated. Cryptographic checksums provide the highest level of security.

Vulnerability Monitors. These monitors are designed to prevent modification or access to particularly sensitive parts of the system; consequently, the monitors may block an attack on those parts. This requires considerable information about "normal" system use because PC viruses typically take advantage of system vulnerabilities and do not circumvent any security features. This type of software also requires decisions from the user about permitted operations.

[8] The terms "virus" and "malicious code" are used interchangeably in this section.

Behavior Blockers. These programs contain a list of rules that a legitimate program must follow. If the program breaks one of the rules, the behavior blockers alert the users.

Heuristic Analysis. Heuristic analysis scans a file for suspicious codes and techniques.

5.6.2 Virus and Malicious Code Protection Product Characteristics

- Accuracy, ease of use, and administrative and system overhead should be considered in product selection.
- Virus protection products should be procured from vendors that display a history of frequent updates and swift responses to new viruses.
- The product should be able to automatically update virus definitions from remote locations or local files.
- Integration with e-mail systems should be transparent but effective.
- The tool should be able to perform an automatic scan of the hard drive for viruses and to check the memory at the frequency level required by the organization's perceived risk level.
- The tool should be able to protect incoming data from a modem or network connection and intercept a virus before it is stored on the hard drive.
- The tool should be able to protect the boot record and inform the user when a virus is detected.
- The tool should be able to update virus definition files both on-demand and automatically on a pre-set schedule.
- The tool should provide an option to choose scanning preferences and perform on-demand scans.
- The tool should be able to provide real-time protection.
- The tool should be able to scan all files that are opened, created, or downloaded.
- The tool should be able to scan all file types for malicious code and monitor JavaScript and ActiveX components for malicious activity.
- The tool should prompt when an infected file is found and give an option to proceed with an appropriate action.
- The tool should offer a repair feature of any infected files or quarantine files designated as irreparable.
- The tool should be able to restore infected files to the state before they were corrupt.

5.6.3 Environment Questions

Organizational Considerations

- What is the skill level of the users in your organization?
- How effective is the tool?
- Are systems connected to an internal or external network?
- Are system components known to be vulnerable to attack (e.g., email and browser applications)?
- Is transportable storage media brought in from outside sources?

Product Considerations

- Can the user perform an update of virus definition files whenever needed?

Vendor Considerations

- What level of support is available to the end-user?
- Is the vendor able to develop and publish virus signatures in a timely manner? Do vendors develop their own virus signatures, or are the signatures based on published search strings?
- What is the level of documentation needed?

5.7 Forensics

Computer forensics involves the identification, preservation, extraction, and documentation of computer-based evidence.[9] Such information may be hidden from view; thus, special forensic software tools and techniques are required. Forensic software tools and methods can be used to identify passwords, log-ons, and other information that may have been deleted from the computer memory. These tools can also be used to identify backdated files and to tie a diskette to the computer that created it.

The computer forensics process consists of three phases: acquisition, examination, and utilization. Computer forensic investigators must have software tools that can effectively and efficiently accomplish the following tasks:

- Image data
- Create comprehensive file listings
- Identify and recover text located anywhere on the storage media
- View text and image files

[9] http://www.cybercrime.gov describes the Federal Criminal Code as it relates to the search and seizure of computers and the gathering of electronic evidence.

- Assure that recovery methods do not unnecessarily contaminate data evidence or produce artifacts
- Identify compressed data and decompress it
- Identify encrypted files.

5.7.1 Types of Products

Forensic tools can be purchased individually or as a suite. They may be grouped into two categories: evidence preservation and collection tools, and analysis tools. These tools facilitate many different forensic activities, including evaluating system content, file comparisons, transactions, and file deletions.

Evidence Preservation and Collection Tools. These tools preserve the integrity of data that resides on evidentiary computer media and provide an unobtrusive mechanism for making copies of some or all of the original data. Write-protection tools and disk imaging software assist forensic examiners during preservation and copying of evidence.

Analysis Tools. The primary function of forensic analysis tools and products is to assist the examiner in analyzing vast amounts of data. Analysis tools perform the following:

- Recover deleted files
- Recover data not allocated to a specific file or application
- Perform string and pattern matching
- Conduct file identification
- Perform file listing or cataloging.

5.7.2 Forensics Product Characteristics

The needed characteristics of a computer forensic toolset will vary with each application. Some products perform a wide range of forensic tasks, such as text string search, deleted file recovery, free space extraction, hidden data recovery, and others perform only a single task.[10]

5.7.3 Environment Questions

Organizational Considerations

- Does the organization need to analyze evidence from a computer incident?
- Does the organization need to recover data from computers seized as evidence and to present it to law enforcement for investigative use and to prosecutors for use at trial?

[10] The NIST Information Technology Laboratory has two ongoing research projects in computer forensics: National Software Reference Library (NSRL) project and Computer Forensics Tool Testing (CFTT) project (see http://www.nsrl.nist.gov and http://www.cftt.nist.gov).

Product Considerations

- Will the product find data on FAT12 (floppy disks), FAT16 (Win3.x, Win95), FAT32 (Win98), New Technology File System (NTFS) (WinNT), Win2000, Macintosh, Linux, or UNIX file systems?

- Is the product designed to be used with the OS in use at the organization?

- Does the product analyze large hard disk partitions and very large hard drives in use by the organization?

- Does the product have reporting capabilities? Does it have case management and configuration management capabilities?

- Does the product prevent the modification of evidence?

- What media does the product support? (e.g., floppy, CD-ROM, optical, tape, and other drives in use by the organization)?

5.8 Media Sanitizing

With the more prevalent use of increasingly sophisticated encryption systems, an attacker wishing to gain access to an organization' sensitive data is forced to look elsewhere for information. One avenue of attack is the recovery of supposedly deleted data from media or memory. This residual data may allow unauthorized individuals to reconstruct and thereby gain access to sensitive information. Media sanitization tools can be used to thwart this attack by ensuring that deleted data are completely removed from the system or media.

When storage media are transferred, become obsolete, or are no longer usable as a result of damage, it is important to ensure that residual magnetic, optical, or electrical representation of data that has been deleted is no longer recoverable. Sanitization is the process of removing data from storage media, such that there is reasonable assurance, in proportion to the sensitivity of the data, that the data may not be retrieved and reconstructed. Once the media are sanitized, it should be impossible or extremely difficult and time-consuming to retrieve the data. There are several accepted methods for sanitizing media: overwriting, degaussing, and destruction

5.8.1 Types of Products

- **Overwriting**. One method to sanitize media is to use software or hardware products to overwrite storage space on the media with nonsensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) to be erased or deleted but also the entire media, including all addressable locations. The security goal of the overwriting process is to replace sensitive data with nonsensitive random data. Media should be overwritten a minimum of three times using a method based on the information sensitivity contained on the media. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method.

- **Degaussing.** A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can erase. Degaussers have two different mechanisms: strong magnet and electromagnetic. Degaussing can be an effective method for sanitizing damaged media, for sanitizing media with exceptionally large storage capacities, or for quickly sanitizing diskettes. Degaussing is not effective for sanitizing nonmagnetic media, such as optical media.

- **Destruction.** Media also can be sanitized using physical destruction of the media. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverization, shredding, melting, sanding, and acid bath. Physical destruction may be the only appropriate sanitization method for nonrewritable optical media, such as CD-ROM (read only) and Write-Once Read-Many (WORM).

  – *Disintegration, Pulverization, Melting, and Incineration.* These sanitization methods are designed to completely destroy the media. They are typically conducted at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

  – *Shredding.* Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size[11] of the refuse should small enough that there is reasonable assurance in proportion to the sensitivity of the data that the data cannot be reconstructed.

  – *Sanding.* Sanding is the application of an abrasive substance (e.g., an emery wheel, grinder, or disk sander or sanding device) to the media's physical recording surface. The entire media recording surface must be removed completely.

  – *Acid Bath.* The application of acid solutions (e.g., concentrated hydriodic) to the media is typically conducted at an outsourced facility with the specific capabilities to perform these activities effectively, securely, and safely.

- **Memory Sanitization.** Sanitization of memory is determined based on whether the memory is volatile or nonvolatile. Volatile memory, such as RAM chips, requires power to maintain their content. Removing electrical power from the chip will erase or sanitize its contents. Nonvolatile memory, such as forms of Programmable Read-Only Memory (PROM), maintain their contents permanently or until reprogrammed. Sanitization methods vary for specific forms of PROM. These methods include ultraviolet light, PROM programmers using overwriting, and physical destruction. No memory sanitization products are specifically discussed.

5.8.2 Media Sanitizing Product Characteristics

Overwriting

- Can overwrite disks regardless of the OS used to write them originally

- Overwrites an entire physical drive regardless of the types or lack of partitions

[11] Class I shredders, defined by General Services Administration (GSA) Interim Federal Specification FF-S-001169, produce a crosscut residue measuring 1/32-inch + 1/64-inch tolerance by 1/2 inch. Class I shredders are appropriate for the highest level of protection.

- Can overwrite logical file locations
- Notification is provided or recorded when address space cannot be overwritten
- Overwrite method and number or repetitions is configurable
- Provides a capability to verify or inspect the overwrite
- Does not damage the media.

Degaussing

- Tested to verify degaussing capabilities (e.g., Type I, low energy; Type II, high energy)
- Does not damage the media.

Destruction

- Conducted at an approved facility or location, whether performed internally by the organization or outsourced, that has been proved effective, secure, and safe

Shredders

- Crosscut or stripper
- Shred size of refuse meets General Services Administration (GSA) standards based on the sensitivity of the data stored on the media.

Sanding

- Uses an approved abrasive substance, such as an emery wheel, grinder, disk sander, or sanding device
- The entire recording media surface is removed completely.

5.8.3 Environment Questions

Organizational Considerations

- What types (e.g., optical nonrewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the sensitivity of the data stored on the media?
- Will the media be exiting a controlled area?
- Should the sanitization process be conducted internal to the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media?

Product Considerations

- Is the media storage volatile or nonvolatile?
- Is the sanitization method appropriate for the media type, data sensitivity, and organization?

Appendix A–References

National Institute of Standards and Technology. *Special Publication 800-4: Computer Security Considerations in Federal Procurements: A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials* (Draft Update).

National Institute of Standards and Technology. *Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook*. October 1995. http://crsc.nist.gov/publications/nistpubs/index.html

National Institute of Standards and Technology. *Special Publication 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems*. September 1996. http://crsc.nist.gov/publications/nistpubs/index.html

National Institute of Standards and Technology. *Special Publication 800-21: Guidelines for Implementing Cryptography in the Federal Government*. November 1999.

National Institute of Standards and Technology. *Special Publication 800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*. August 2000.

National Institute of Standards and Technology. *Special Publication 800-25: Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*. October 2000.

National Institute of Standards and Technology. *Special Publication 800-27: Engineering Principles for Information Technology Security: A Baseline for Achieving Security*. June 2001

National Institute of Standards and Technology. *Special Publication 800-30: Risk Management Guide for Information Technology Systems*. (Draft).

National Institute of Standards and Technology. *Special Publication 800-31: Intrusion Detection Systems*. August 2001.

National Institute of Standards and Technology. *Special Publication 800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure*. February 2001.

National Institute of Standards and Technology. *Special Publication 800-41: Guidelines on Firewalls and Firewall Policy*. January 2002.

National Institute of Standards and Technology. *Computer Security Laboratory Bulletin: Disposition of Sensitive Automated Information*. October 1992.

United States. *Federal Acquisition Regulation*. September 2001.

U.S. Office of Management and Budget. *Circular A-130, Appendix III: Security of Federal Automated Information Resources*. November 28, 2000.

U.S. Department of Energy, Federal Energy Regulatory Commission. *Information Technology Security Solutions Evaluation and Review*. June 11, 2001.

U.S. Navy Staff Office. *NAVSO Publication 5239-26: Remanence Security Guidebook.*

U.S. Department of Energy. *Clarification to the DOE Manual 5639.6A-1: Clearing, Sanitizing, and Destruction of Automated Information Systems Storage Media, Memory, and Hardware.* December 30, 1996.

Defense Technical Information Center - Information Assurance Technology Analysis Center. *Computer Forensics: Tools & Methodology*, *Critical Review and Technology Assessment Report*. Michael Noblett, Adam Feldman. May 12, 1999.

Defense Technical Information Center - Information Assurance Technology Analysis Center. *Information Assurance Tools Report*, *Intrusion Detection.* June 15, 2001.

U.S. Critical Infrastructure Assurance Office. *Practices for Securing Critical Information Assets*. January 2000.

U.S. General Services Administration. *A Guide to Planning, Acquiring, and Managing Information Technology Systems*. December 1998.

National Computer Security Center. *NCSC-TG-025, Version-2: A Guide to Understanding Data Remanence in Automated Information Systems*. September 2, 1991.

Summers, Rita C. *Secure Computing: Threats and Safeguards*. McGraw Hill, 2000.

Gartner Group. *Biometrics-Based Recognition for Financial Services*, *Context Overview Report*. December 31, 1998.

Jim Rapoza. *Accessing Control*. eWeek.com. December 4, 2000.

Jim Rapoza. *Access Control Tools Add Site Security*. eWeek.com. July 17, 2000.

Steve Lewis, Steve Wilson, and Martin D'Cruze. *Why do you want web access control anyway?/Interactive scorecard and NetResults: Web access control packages*. Network World. May 28, 2001.

Jay Bellamy. *Knock Knock, Who's There?* InfoSecurity/Secure Computing. March 2001.

Rutrell Yasin. *Access Control Gets Granular*. InternetWeek. January 20, 2000.

The Biometrics Consortium. <http://www.biometrics.org>.

The Common Criteria Project. < http://csrc.nist.gov/cc>.

The Smart Card Industry Association. <http://www.scia.org>.

Appendix B–Acronyms

ACL	Access Control List
API	Application Programming Interface
CA	Certificate Authority
CBAC	Context-Based Access Control
CC	Common Criteria for IT Security Evaluation (ISO/IEC 15408)
CCEVS	Common Criteria Evaluation and Validation Scheme
CD-ROM	Compact Disk—Read-Only Memory
CFTT	Computer Forensics Tool Testing
CIO	Chief Information Officer
CMVP	Cryptographic Module Validation Program
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
CRC	Cyclical Redundancy Check
CRL	Certification Revocation List
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Control Protocol
E-mail	Electronic Mail
FAR	Federal Acquisition Regulation
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GSA	General Services Administration
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
ICMP	Internet Control Message Protocol
ID	Identification
IDS	Intrusion Detection System
I/O	Input/Output
IP	Internet Protocol
IPSec	Internet Protocol Security
IPT	Integrated Product Team
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LCC	Life-Cycle Cost
LDAP	Lightweight Directory Access Protocol
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSRL	National Software Reference Library

NTFS	New Technology File System
OMB	Office of Management and Budget
OS	Operating System
OSI	Open Systems Interconnect
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
PROM	Programmable Read Only Memory
RA	Registration Authority
RADIUS	Remote Authentication Dial-in User Service
RAM	Random Access Memory
RBAC	Role-Based Access Control
RDBMS	Regional Database Management System
ROM	Read-Only Memory
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TACACS+	Terminal Access Controller Access Control System +
TCP	Transfer Control Protocol
TLS	Transport Layer Security
WAN	Wide Area Network
WORM	Write-Once Read-Many

Appendix C–Frequently Asked Questions

1. **Why was this guide written?**

   This guide will help organizations make informed decisions when selecting computer security products. The categories of products listed here include operational controls such as intrusion detection and technical controls such as firewalls. This guide should be used with other NIST publications to develop a comprehensive approach to the management of an organization's computer security and requirements. The guide first defines broad security product categories and then specifies product types within those categories. This guide explains and provides a list of characteristics and pertinent questions an organization should ask in the selection process.

2. **For whom is the guide intended?**

   This guide is written to help an organization during the various stages of the computer security product life cycle. It can be used as a tool by—

   + IT Security Officers in conducting the IT risk assessment and building the business case for the procurement of IT security products.
   + Chief Information Officers (CIO) and Chief Technology Officers (CTO) in establishing product procurement policy and ensuring that security has been appropriately considered in the selection process.
   + IT directors, program managers, and system owners in understanding the types of available security products, what they should consider when making a selection decision, and what factors they should use for evaluating a security product.

   Although this document can be used by a number of people in an organization, it will be most useful to those who will be developing and maintaining a secure IT infrastructure.

3. **Who has a role in product selection?**

   Product selection involves numerous people throughout an organization. Each person involved in the process, whether on an individual or group level, should understand the importance of security in the organization's information infrastructure and the security impacts that their decisions will have. The personnel listed below are a sample guide. Depending on the organization's needs, one may include all of the personnel listed below or a combination of particular positions relevant to IT security needs.

   + IT Security Program Manager
   + Chief Information Officer
   + IT Investment Board (or equivalent)
   + Program Manager (owner of data) / Procurement Initiator
   + Acquisition Team
   + Contracting Officer

- + Contracting Officer's Technical Representative
- + IT System Security Officer

4. What specific security products should an organization select?

This guide does not discuss how an organization should develop its overall computer security program or the optimal set of products that should be implemented, nor are the product categories listed in this guide exhaustive as the commercial marketplace for IT security products is constantly changing. Also, the specific products that are right for each organization will vary based on mission, specific IT infrastructure, security objectives, operational constraints, and so forth.

5. How should an organization go about selecting IT security products?

A security program, whether at the organization or at the system level, should include an appropriate mixture of security controls: management, operational, and technical. The number and type of appropriate security controls and their corresponding IT security products may vary throughout a particular system's development and procurement life cycle. The relative maturity of an organization's security architecture may influence the types of appropriate security controls. The blend of security controls is tied to the mission of the organization and the role of the system within the organization as it supports that mission.

Risk management is the process used to identify an effective mix of management, operational, and technical security controls to mitigate risk to a level acceptable to the responsible senior official. Once the necessary controls are identified, IT security products can then be identified to provide for these controls. In addition, it is important to perform a cost-benefit analysis when selecting security products[1]. As part of the cost-benefit analysis, a life-cycle cost (LCC) estimate for the status quo and each alternative identified should be developed. In addition to LCC estimates, benefits associated with each alternative should be identified and, to the extent practicable, quantified in terms of dollar savings or cost avoidance.

Once all options are weighed in the cost-benefit analysis, the security product selection is made, and implementation of the product can follow.

6. How can an organization gain assurance in the operation of the security features of commercial-off-the-shelf (COTS) products?

Independent, third-party testing and evaluation of IT products can give consumers greater confidence that the security features in those products work as advertised by the vendor. Testing and evaluation also provides a way to demonstrate product compliance with organization security requirements and public security standards. NIST Special Publication 800-23 provides guidance on security assurance and the use of tested/evaluated products, and should be consulted by organizations selecting security products for their IT systems and networks.

Two prominent security testing and evaluation programs are now in place to assess the security features and assurances of commercial off-the-shelf (COTS) products: (1) National Information

[1] There may be cases where the cost of a product is relatively low or the benefit is somewhat obvious, i.e. a virus scan product. In these situations, the rigor of a cost-benefit analysis may be reduced.

Assurance Partnership[2] (NIAP) Common Criteria (CC) Evaluation and Validation Scheme (CCEVS) and (2) NIST Cryptographic Module Validation Program[3] (CMVP).

7. What are the organizational considerations when selecting an IT security product?

The organizational considerations required to support a product purchase are provided in the list of following questions. An organization may or may not have a need to consider all questions. In some cases, a high cost product acquisition may require a more extensive evaluation of organizational considerations.

+ Is the anticipated user community identified? How many and what type of users does the organization anticipate will use the security product?

+ Is the relationship between this security product and the organization's mission performance understood and documented?

+ Has the sensitivity of the data the organization is trying to protect been determined?

+ Are the organization security requirements supported by the security plan, policies and procedures?

+ Have identified security requirements been compared against product specifications?

+ Has appropriate procurement language been used for the specific product under selection?

+ Have operational issues, such as daily operation, maintenance, contingency planning, awareness, and training, and documentation been considered?

+ Have policies been developed for the procurement and use of evaluated products as appropriate? When selecting products, organizations need to consider the threat environment, the security functions needed to cost-effectively mitigate the risks to an acceptable level. Organizations should give substantial consideration to procurement and deployment of IT security products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. Examples of these specifications include protection profiles based on ISO/IEC 15408, the Common Criteria for IT Security Evaluation.

+ Is communication required across a domain boundary (implies the need for a boundary controller; e.g., sub-system of firewall, intrusion detection system, and/or routers)?

+ Are the system components (hardware or software) required for this product identified?

+ Is the security product consistent with physical security and other policy requirements?

8. What are the product considerations?

The following questions apply to the product and should be considered when forming a decision and selecting a product:

[2] See http://niap.nist.gov

[3] See http://csrc.nist.gov

+ Have total life-cycle support, ease-of-use, scalability, and interoperability requirements been determined? The total life cycle covers "cradle to grave" and hence includes security product disposal requirements.

+ Have test requirements, for acceptance and integration testing, and configuration management been developed? If the product has been evaluated under the NIAP-CCEVS or CMVP, validation test reports can be examined to avoid duplication of tests already performed as part of the independent evaluation process.

+ Have known product vulnerabilities been addressed by reviewing the relevant vulnerabilities for a product? Known vulnerabilities for some products can be found using the NIST ICAT Vulnerability Search Engine (http://icat.nist.gov).[4]

+ Have all relevant patches been tested and implemented?

+ Have CC protection profiles (PP) been reviewed, when available (http://www.commoncriteria.org/protection_profiles/pp.html), to identify PPs that express security requirements applicable to the organization's needs in the anticipated threat environment? If existing protection profiles are not adequate, consider the usefulness of similar protection profiles as a starting point for examining products that might satisfy requirements applicable to the new environment.

+ CC and FIPS 140-1/FIPS 140-2 program Validated Products lists should be reviewed to ensure that evaluated products are used whenever feasible. Products independently tested and validated under NIAP-CCEVS (or mutually recognized) or CMVP provide an organization with some level of security assurance that the security functions of the product work as specified. In general, third party testing and evaluation can provide a significantly greater basis for customer confidence than is available from unevaluated products. Note, however, that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements and vendor reliability, may be neither useful nor cost effective. Organizations should consider their overall requirements and select the best products accordingly.

+ Have CC or FIPS 140-1/FIPS 140-2 validated products been revalidated when new releases of the product are issued?

+ Have product specifications been reviewed with respect to existing and planned organizational programs, policies, procedures, and standards?

+ Does the product have any security critical dependencies on other products? For example, an operating system (OS) or cryptographic module?

+ Does interfacing the new product with the existing infrastructure introduce new vulnerabilities?

9. What are the vendor considerations?

The following questions apply to the vendor and should be considered when forming a decision and selecting a product:

[4] ICAT is a search engine for an industry standard set of virtually all known vulnerabilities (http://cve.mitre.org) containing links to vulnerability and patch information.

- Will the selection of a particular product limit the future choices of other computer security or operational modifications and improvements?
- Does the vendor have experience in producing high quality IT security products?
- What is the vendor's "track-record" in responding to security flaws in its products?

10. Which IT security product categories are discussed in this document?

The document discusses the following product categories of security products representative of common technological elements helpful in securing infrastructure:

- Identification, authentication, and authorization
- Access control
- Intrusion detection
- Firewall
- Public key infrastructure
- Virus and malicious code protection
- Forensics
- Media sanitizing