Special Publication 800-36

Guide to Selecting Information Technology Security Products

Recommendations of the National Institute of Standards and Technology

Timothy Grance
Marc Stevens
Marissa Myers

NIST Special Publication 800-36

COMPUTER SECURITY

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

October 2003

Acknowledgements

The authors, Timothy Grance of NIST, and Marc Stevens and Marissa Myers 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. We also gratefully acknowledge and appreciate the many comments we received from readers of the public and private sectors, whose valuable insights improved the quality and usefulness of this document. The authors would like to specifically acknowledge some key organizations whose extensive feedback substantially contributed to the development of the document. These organizations include: National Archives and Records Administration, Environmental Protection Agency, Department of Treasury, Small Business Administration, Tennessee Valley Authority, and Corbett Technologies. The authors would also like to acknowledge Ron Ross, Marianne Swanson, Tim Polk, Vincent Hu, John Wack, Murugiah Souppaya, Ramaswamy

Executive Summary

The selection of IT security products is an in

Identification and Authentication

Access Control

Intrusion Detection

Firewall

Public Key Infrastructure

Malicious Code Protection

Vulnerability Scanners

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, policies, and procedures; and operational issues such as daily operation, maintenance, and training.

Product considerations should include total life-cy

TABLE OF CONTENTS

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Manageme

Many IT security products are readily available for purchase in the commercial market. This guide will assist the reader in choosing IT security products that meet their organization's requirements.

This guide seeks to help organizations make informed decisions when selecting IT 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 IT 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 during the selection process.

1.3 Scope

This guide covers the selection of IT 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 IT security program or the optimal set of products that should be implemented. This guide covers many IT security product categories, but it is not exhaustive in its coverage. For instance, the issue of obsolescence is not addressed. Issues concerning one IT security product category may also be applicable to other product categories not described in this document. While covering broad IT security product categories, this guide does not attempt to be exhaustive in either coverage or depth of the many and varied products in the market place.

For information on the overall system security requirements analysis process and methods for incorporating security into IT procurements, see NIST Special Pub.98 0 0 10.98 27ating security

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 roles are listed as a guide. Depending on the organization's needs, a person may be assigned one of the roles listed below or a combination of roles relevant to IT security needs. In some small organizations, a single individual may hold multiple roles.

2.1 IT Security Program Manager

The IT Security Program Manager is responsible for developing enterprise standards for IT security. This individual plays a leading role in introducing an appropriate, structured methodology to help identify, evaluTg174 Tm(IT security)Tj10op9oAT0op874 522.65891 Tm(35 0 0 10.98 220.9221

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 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.

to guide decisions that are consistent with the organization's architecture and a well-established business case.

Organizational Questions

These questions are applicable to all information systems (for example, identification of all components, impact on system of emerging technologies, and use of appropriate contract language).

Is the product necessary to adequately mitigate risk?

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 organization determined the sensitivity of the data to be protected?

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

Have security requirements been identified and compared against product specifications?

When selecting products, organizations need to consider the threat environment and the security functions needed to cost-effectively mitigate the risks to an acceptable level. Organizations should give consideration to acquisition 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*. However, agencies should consider their overall requirements and select products accordingly. In the case of cryptographic modules, when agencies have determined the need to protect information via cryptographic means, they may only select CMVP validated cryptographic modules. See http://csrc.nist.gov/cryptval/ for a validation list for cryptographic standards.

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)?

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

Has the impact on the enterprise operational environment where this product will operate been considered?

Have security reviews included requirements for support, plug-in components, or middleware?

Product Considerations

These questions are applicable to all information systems (for example, total life-cycle cost and acceptance testing).

If the product has been evaluated under a CC scheme, validation test reports can be examined to avoid duplication of tests already performed as part of the independent evaluation process.

Does interfacing the new product with the existing infrastructure introduce new vulnerabilities or interdependencies?

What is the frequency of product failures and adequacy of corrective actions?

Vendor Considerations

These questions are applicable to all information system vendors (for example, long-term viability).

Will the selection of a particular product limit the future choices of other IT security 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?

How does the vendor handle software and hardware maintenance, end user support, and maintenance agreements?

Does the vendor have an associated security or configuration guide for the product? Does the vendor use or make reference to NIST, consortia, or other consensus-based checklists, security configurations/settings or benchmarks.

5. IT Security Products

The following categories of security products represent common technological elements helpful in securing IT systems and supporting infrastructure. This list is not all-inclusive and will change over tim

with nonprogrammable logic. The chip connection is made by either direct physical contact or remotely via a contactless electromagnetic interface.

Certificates. The public key certificate associates a certificate holder’s identity with his public key. (See Section 5.5, Public Key Infrastructure, for further details)

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

5.1.3 Environment Questions

Smart Card Specific [4]

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? ƒsy

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?

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?d tem

Product Considerations

Which of the following access control method(s) does the product support and which is needed:

- Internet Protocol (IP) address based
- User identity-based
- Group based
- Role based (user authenticated and assigned a role, with access controlled based on that role).

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.358486ehTj10.98 0 0 10.98 377.9954099(dj10.98 0 0 10.98 122.cl/IPthe

Is the product limited to supporting certain kinds of security rules/user account databases/directories (e.g., Lightweight Directory

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?

Can the system protect against unauthorized access by use of an image versus presentation of an actual biometric object (i.e., presentation of a picture of an iris/retina versus presentation of the actual eye)?

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 perform unauthorized actions, 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. Intrusion detection systems (IDS) are software or hardware products that assist in the intrusion monitoring and analysis process.

The implementation of an IDS might be valuable for the following reasons:

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

Detect attacks and other security violations that are not prevented by other security measures

Detect preambles to attacks (network probes and other tests for existing vulnerabilities)

Document the existing threat to the organization

Quality control for security design and administration

Provide useful information about methods used in intrusions.

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

Signature-Based Detection[7]. This approach identifies events or sets of events that match with a predefined pattern of events that describe a known attack. These patterns are called signatures. Signatures may include system states, or accessing system areas that have been explicitly identified as “off-limits.”

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 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.

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

5.3.1 Types of Products

Three common types of IDS products are network based, host based, and application based. Each type of product may optionally offer intrusion prevention capabilities.

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.

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 determine exactly which processes and user accounts 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.

Intrusion Prevention. Intrusion detection systems often have intrusion prevention capabilities. This means that not only can they detect an intrusive activity, but they can also attempt to stop the activity, ideally before it reaches its targets. Intrusion prevention is much more valuable than intrusion detection because intrusion detection simply observes events without making any effort to stop them. Unfortunately, intrusion prevention can also cause operational issues because if the detection of incidents is not accurate, then it may block legitimate activities that are incorrectly classified as malicious. Any organization that wants to utilize intrusion prevention should pay particular attention to detection accuracy when selecting a product.

Another consideration involving intrusion prevention is architecture-related. IDS products may be simply monitoring activity, or they may actually be “in-line”, which means that activity must pass

and Firewall Policy. This publication provides details of firewalls and firewall product selection that are beyond the scope of this document.

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 simp 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. 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.

(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 layered defense 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.

Centrally Managed Distributed Firewalls. The goals for host-based firewalls and personal firewalls/appliances can also be achieved using centrally managed distributed firewall products. All of these firewall types provide firewall capability in every protected computer. Centrally managed distributed firewalls are centrally controlled but locally enforced. A security administrator defines and maintains security policies, not the end-users. This places the responsibility and capability of defining security policies in the hands of a security professional who can properly lock down the target systems. A centrally managed system is scalable because each system does not have to be administered separately. A properly executed distributed firewall system includes exception logging. More advanced systems include location intelligence so that the appropriate policy is enforced depending on the context of the connection.

Centrally managed distributed firewalls can be either software- or hardware-btrally

-

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?

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

How vulnerable is the firewall to attacks via the ne]twork against the firewall itself?
If the firewall runs on an individual host for which all users are not trusted system administrators, how vulnerable is it to tampering by a user logged into the operating system running on the protected hosts?

Does the system require end-users to configure and maintain security policies, security professionals to individually manage policies per host, or is the configuration centrally managed?

- If centrally managed, how is this function secured?
- If centrally managed, are remote systems with VPN connections covered by this feature?

Can the firewall support hot-standby/failover/clustering?

What type of NAT is supported?

Is firewall “chaining” possible (to distribute filtering functions across a series, for better performance)?

Is 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?

Is the product SNMPv3 capable?

5.5 Public Key Infrastructure

The interconnectivity of networks and the Internet support opportunities for government and business to conduct electronic transactions. 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 a PKI 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
>
> PKI information can be found 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 pr0.98 425 Tm( )Th Tm(relies on the c269ed 10.m(8 00 0.0006 Tw 10.98( )Th Tm(reli//p whichovide

p

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 those applications. 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. FIPS 140-2 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 another 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 keys, 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 certificate revocation list (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 per0.00101 Tc 0.0004 Tw 10.90.28944009 Tw 10.98 0 0.76I2nce revosed ities 10.98 0 0 10.98 249.912.15633. 10.98 0

The organization should determine how difficult it is to migrate from one PKI product to another.

What is the projected growth of the organization?

What physical security measures are required to ensure the integrity of a central PKI solution?

Product Considerations

Is the product compatible and interoperable with other PKI products/service providers?

Are there proprietary interface dependencies?

What is the ease of supporting applications (e.g., virtual private networks, access control, secure e-commeID 435.98 1 0 10.98 174.65rce, s 653.58044 Tm(m)Tj11.9883 0 110.98 174.65arm(ard6 653.5804

connections, PDAs and other removable devices so that viruses can be intercepted before they are stored on the hard drive.

Integration with e-mail, Web, FTP, instant messaging and other applications that may transport malicious code should be transparent but effective.

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 inform the user when a virus is detected and prompt the user to select an appropriate action, such as deleting an infected file or attempting to remove the virus from an infected file.

The tool should offer a repair feature of any infected files or quarantine files designated as irreparable.

5.6.3 Environment Questions

Organizational Considerations

running scanners on a regular basis, administrators can also see how effectively they have mitigated vulnerabilities that were previously id

Does the product support all operating system

Identify and recover text located anywhere on the storage media

View text and image files

Assure that recovery methods do not unnecessarily contaminate data evidence or produce artifacts

Identify compressed data and decompress it

Identify files by their contents and file header signatures, not just filenames and file exten59917 Tm(age files)TjETe files

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?

Is the acquisition and analysis of the media performed by the same individual?

Product Considerations

Will the product find data on all applicable file systems (e.g. FAT12 (floppy disks), FAT16 (Win3.x, Win95), FAT32 (Win98), NTFS (WinNT), NTFS5 (Win2000), HFS and HFS+ (Macintosh), Ext2FS and Ext3FS (Linux), UFS (Solaris), FFS (Unix), virtual 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)?

What is the speed of duplication/collection?

Does the product sanitize the destination media prior to duplication/collection?

5.9 Media Sanitizing

With the more prevalent use of increasingly sophisticated encryption systems, an attacker wishing to gain access to an organization’s 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 impractical to retrieve the data. There are several accepted methods for sanitizing media: overwriting, degaussing, and destruction[12].

5.9.1 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

[12] The cost and benefit of a media sanitization method should be understood prior to a final decision. For instance, it may not be cost effective to degauss inexpensive media like diskettes.

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 varietytive m.98 0 0 1 Tw 10.98 0 0 10.98 380.16357h24.81 arizt esetyre

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

Can overwrite logical file locations

Notification is provided or recorded when address space cannot be overwritten

Overwrite method and number of repetitions is configurable (e.g. using static or dynamic data)

Provides a capability to verify or inspect the overwrite

Does not damage the media.

Degaussing[13]

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 appropriate 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

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

The entire recording media surface is removed completely.

5.9.3 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 processed outside a controlled area?

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 (NIST). *Special Publication (SP) 800-12: An Introduction to Computer Security: The NIST Handbook*. October 1995.

NIST Computer Security Laboratory Bulletin: *Disposition of Sensitive Automated Information*. October 1992.

Federal Information Security Management Act of 2002, 44 U.S.C. Chapter 35, Subchapter III. 2002.

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*. N0l>m

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://www.commoncriteria.org >.

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

Appendix B–Acronyms

ACL	Access Control List
CA	Certificate Authority
CC	Common Criteria for IT Security Evaluation (ISO/IEC 15408)
CCEVS	Common Criteria Evaluation and Validation Scheme
CD-ROM	Compact Disk—Read-Only Memory
CIO	Chief Information Officer
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
CRL	Certification Revocation List
CVE	Common Vulnerabilities and Exposures
DBMS	Database Management System
DHCP	Dynamic Host Control Protocol
E-mail	Electronic Mail
Ext2FS	Second Extended File System
FAR	Federal Acquisition Regulation
FAT	File Allocation Table
FBCA	Federal Bridge Certification Authority
FFS	Fast File System
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GSA	General Services Administration
GUI	Graphical User Interface
HFS	Hierarchical File System
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IPSec	Internet Protocol Security
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
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
PKIX	Public Key Infrastructure for X.509 Certificates
PP	Protection Profile
PROM	Programmable Read Only Memory
RA	Registration Authority
RADIUS	Remote Authentication Dial-in User Service
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
UDP	User Datagram Protocol
UFS	Unix File System
WAN	Wide Area Network
WORM	Write-Once Read-Many

Appendix C–Frequently Asked Questions

1.

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 m

Assurance Partnership[2] (NIAP) Common Criteria (CC) Evaluation and Validation Scheme (CCEVS) and (2) NIST Cryptographic Module Validation Program[3] (CMVP). In the case of cryptographic modules, when agencies have determined the need to protect information via cryptographic means they may only select CMVP validated cryptographic modules. See http://csrc.nist.gov/cryptval/ for a validation list for cryptographic standards.

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 security plans, policies and procedures?

Have security requirements been identified and 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?

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

Have security reviews been made for support/plug-in components middleware?

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:

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, 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?

– 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?

What is the frequency of product failures and adequacy of corrective actions?

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:

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?

How does the vendor handle software and hardware maintenance, end user support, and maintenance agreements?

What is the long-term viability of the vendor?

Has the vendor developed a security configuration guide?

Does the vendor have an associated security guide for the product? Does the vendor use or make reference to NIST, consortia, or other consensus-based checklists, security configurations/settings or benchmarks.

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 and authentication

Access control

Intrusion detection

Firewall

Public key infrastructure

Vulnerability scanners

Forensics

Media sanitizing