
Financial Services Security Laboratory



Application Security Products Profile

Technical Contact Information

If further information regarding technical content is required, please contact:

BITS Financial Services Security Lab

Tel: (202) 289-4322

Fax: (202) 289-3562

bits@fsround.org

**Originating
Author:**

Lynch Davis, Senior Consultant, **Predictive Systems, Inc.**, *Global Integrity*TM
Information Security

Profile Leader

Workgroup Chair: **Eric Guerrino**, CISSP, SVP/Data Security, **The Bank of New York**

BITS Security Lab Application Security Products Profile working group members (primary contributors/organizations identified in bold):

Representative	Organization	Representative	Organization
Gregory Blair	Fortis, Inc./Assurant Group	Jill Flory	Goldman Sachs Group, Inc.
Mary Jane Bolling	Capital One Financial Corporation	Jon Fox	USAA
Jim Brown	M&I Data / Metavante Corporation	Gene Fredriksen	Raymond James Financial, Inc.
Mark Chamberlain	Nationwide	Al Meyer	Harris Bankcorp, Inc.
Pat Christensen	Department of the Navy	Jim Ramsay	First Union Corporation/ Wachovia Corporation
Brian Cregg	Allfirst Financial, Inc.	Don Richmond	Raymond James Financial
Ron Dinehart	IBJ Whitehall Financial Group	Jim St. Clair	Department of the Navy
Landy Dutton	Regions Financial Corp.	Jeffrey Stempora	State Farm Mutual Insurance Companies
Brian Ekkebus	Northern Trust Corporation	John Walsh	Allfirst Financial, Inc.

Profile Feedback

If you have comments regarding this profile, please send an email to BITS@fsround.org. Include the profile name, your name, e-mail address, telephone, and FAX number, and whether you would like to be contacted.

Application Security Products Profile – Version Control History

Note: **Bold** in Version/Date column indicates a public release

Version / Date	Changes
0.90 – 0.92 (Jun – Dec 2000)	◆ DRAFT – Collaboration on Initial Draft (Predictive Systems / Profile Leader / BITS)
1.00 – 1.02 (Jan – Mar 2001)	◆ DRAFT – Financial Services Workgroup Review
1.02 – 1.03 (Mar - May 2001)	◆ DRAFT – Financial Services / Technology Provider Workgroup Review
1.03 (May 2001)	◆ DRAFT – Public Comment
1.04 (September 2001)	◆ DRAFT – Version to be submitted to the LGC for approval for testing to begin
1.05 (October 2001)	◆ FINAL- Initial published version available for testing
1.06 (February 2002)	<ul style="list-style-type: none"> ◆ FINAL – Revised published version available for testing ◆ <i>Section 5 (Subclasses)</i>: Section 5.2 in version 1.05 was split into 5.2 Application-content Filtering and 5.3 Internet-Content Filtering. ◆ <i>Section 5.2</i>: Reworded specific criteria for clarity in section.

Table of Contents

1. INTRODUCTION.....	1
1.1 OVERVIEW	1
1.2 BACKGROUND	1
1.3 MANDATORY AND DESIRED CRITERIA	2
1.4 BOUNDARIES AND UNDERLYING PLATFORMS.....	3
1.5 TEST PLANS AND PROFILES	3
1.6 COMMON TERMS USED IN THIS PROFILE.....	4
2. CRITERIA FOR THE ADMINISTRATION AND OPERATION OF APPLICATION SECURITY PRODUCTS.....	5
2.1 SECURITY FEATURES.....	5
3.0 PRODUCT FUNCTIONALITY.....	15
4.0 SCALABILITY.....	16
3. REQUIRED FUNCTIONAL CRITERIA FOR ALL APPLICATION SECURITY PRODUCTS	17
3.1. INTRODUCTION	17
3.2 ADMINISTRATION	17
3.3 EVENT LOGGING AND ALERTING.....	18
3.4 PRODUCT CONFIGURATION	18
4. DESIRED FUNCTIONAL CRITERIA FOR ALL APPLICATION SECURITY PRODUCTS	19
4.1 INTRODUCTION	19
4.2 PRODUCT CONFIGURATION	19
5. FUNCTIONAL CRITERIA FOR APPLICATION SECURITY PRODUCT SUBCLASSES	21
5.1. INTRODUCTION	21
5.2. FUNCTIONAL CRITERIA FOR APPLICATION-CONTENT FILTERING SECURITY PRODUCTS.....	21
5.3. FUNCTIONAL CRITERIA FOR INTERNET-CONTENT FILTERING SECURITY PRODUCTS	22
5.4. FUNCTIONAL CRITERIA FOR EMAIL SECURITY PRODUCTS	24
APPENDIX A: INDUSTRY STANDARDS.....	27
APPENDIX B: BIBLIOGRAPHY	28
APPENDIX C: GLOSSARY OF TERMS.....	29

1. Introduction

1.1 Overview

This product profile defines the security requirements that will be included in the BITS Security Lab's technical analysis of Application Security products. The primary purpose of these software products is to improve security of electronic mail and Internet access facilities by scanning and filtering incoming code and other content. Currently, this profile addresses products that provide such features by means of a gateway or proxy approach. It does not at this time address products that operate at the user's desktop. However, it is anticipated that the latter will be addressed by this profile in a subsequent release.

Additionally, this profile class does not include products that have a primary purpose of authentication, access control or enhanced operating system or network security. The profile lists the security-related criteria that *apply to the features and functionality* normally found in application security products.

The criteria have been derived and expanded from the BITS Security Lab's Master Security Criteria (MSC¹). The Master Security Criteria defines the basic set of security features, functionality, usability and scalability requirements that apply to many different product categories. Note that there may be some requirements in this document that may not be reflected as requirements in the MSC. Section 2 of this document maps the criteria from the MSC related to the Operation and Administration of products in this profile's product class, designating each as "required" or "desired." The MSC is a necessary accompanying reference for Section 2.

1.2 Background

In legacy mainframe environments, strong computer security is achieved primarily through operating system controls. There are also numerous software-based products that enhance the management and effectiveness of operating system security. However, as newer business applications have migrated to the client/server and Internet/intranet environments, operating system security controls are frequently bypassed. Much of a business's most sensitive information is now held in distributed e-mail and Internet/intranet servers throughout the enterprise. Business rules are scattered through multiple software applications, and Application Security products have evolved for inter-application communication and data transfer. Users are given

¹ See Appendix B for complete reference to the MSC version used as the basis for this document.

access to these systems and their sensitive data any time and from anywhere through web browsers and custom front-end applications. Applications are written by programmers with time and performance constraints and frequently with a limited knowledge of or concern for securing their application data. For these reasons, numerous software security products are now available to enhance the protection of the contents of these data repositories. This BITS Security Lab product profile addresses the security requirements for those applications that add security to systems such as e-mail systems and Internet/intranet servers. This profile addresses products within this class that are *server-based* (i.e. gateways, proxy servers, etc). Consideration for *client-based* application security products is under review and may involve a new product security profile, placement of these products within a planned product security profile, or future enhancement of this specific security profile.

1.3 Mandatory and Desired Criteria

Each criterion will be identified as being *required* or *desired*². A product will get the *BITS Tested Mark* only if it meets all the *Required* criteria within Section 2 “Criteria for the Administration and Operation of Application Security Products,” Section 3 “Required Functional Criteria for All Application Security Products” and the appropriate subclass of Section **Error! Reference source not found.** “**Error! Reference source not found.**” In other words, a product will not merit a *BITS Tested Mark* if it misses a single required criterion. Please note that the BITS Financial Services Security Lab employs a “Pass/Withdrawal” testing process.

In this document, *required* criteria use the verb “shall,” while *desired* criteria use the verb “should.”

The criteria identified in this profile as *desired* are not required for the *BITS Tested Mark*, but compliance with these criteria will be noted in the final Test Report. *Desired criteria are recognized by the financial services industry as advantageous and may become requirements in the future.*

1.4 Boundaries and Underlying Platforms

A number of criteria outlined in this document may be addressed through security features of any system component, rather than the Application Security product itself. Rather than requiring all security functionality to be provided by the stand-alone system, the criteria and process allow for the product to rely on an underlying platform (e.g., operating system) or supporting components for specific security requirements. To support this approach, the process allows the Technology Provider and the Testing Lab to define the “boundaries” of the test environment, which delineates the system to be tested. It is anticipated that this boundary will include the product itself, the underlying platform, and any relying application or system. It is important to note, however, that the criteria will be applied equally to all components within that boundary.

Example: A product in this profile’s product class relies on the underlying operating system to provide scalable functionality. This configuration may be sufficient to meet the criteria within the profile for scalability. If, however, during the testing of the product (within this agreed-to testing boundary³ and test plan), a vulnerability or issue is found in the operating system software that renders the system non-compliant with any of the test plan’s criteria test cases, the product will not earn the *BITS Tested Mark* unless the vulnerability or issue is addressed. This determination will be made regardless of the fact that the vulnerability may be in another vendor’s product, since it has been defined and agreed to as part of the test environment within the “boundary.”

Additionally, if the system uses any cryptographic algorithm not identified in “Appendix A: Industry Standards,” then the system shall be configurable to also allow the use of an acceptable algorithm in place of the unlisted algorithm. Systems that do not have this flexibility will be disqualified from the BITS validation process.

1.5 Test Plans and Profiles

It is important to note that actual testing of individual products will be conducted against a test plan produced from this profile. Each product undergoing testing will have a specific test plan developed. *It is possible that certain criteria will be implemented differently, and thus tested differently, in two similar products.*

Systems will be tested within a standard configuration and stand-alone environment that will include *the product itself, any agreed-to supporting products, supporting platform and user interfaces.*

³ Reference: BITS Lab Testing Services Agreement (and Schedule A, Product Testing Schedule)

1.6 Common Terms Used in this Profile

In this section, we will list definitions of terms that are important or frequently used in the remainder of the profile. See “Appendix C: Glossary of Terms” for a complete listing of terms used.

TERM	DEFINITION
access control	<i>A mechanism for limiting use of some resource to authorized users. [1]</i>
audit	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
authentication	<i>The process of reliably determining the identity of a communicating party. [1]</i>
authenticator	<i>The method, material or credential used to create and/or implement authentication bindings, such as a password, PIN number, token seed, smart card seed, etc.</i>
confidentiality	<i>The property of not being divulged to unauthorized parties. [1]</i>
integrity	<i>The quality of being uncorrupted (message integrity refers to the state of a message not being modified while in transit; file integrity refers to the state of files not being modified while in storage). [2]</i>
log file	<i>A file that lists actions that have occurred. [2]</i>
Master Security Criteria (MSC)	<i>BITS Security Lab criteria used to generate product-specific criteria. The criteria in this document fall into categories outlined in the Security Criteria Overview, and will be used to develop the individual Product Security Profiles. MSC version 3.0 will be referenced for this profile.</i>
non-repudiation	<i>The property of a scheme in which there is proof of who sent a message that a recipient can show to a third party and the third party can independently verify the source. [1]</i>
privileged user	<i>A user of a computer or system who is authorized to bypass normal access control mechanisms, usually to be able to perform system management functions. [1]</i>
product administrator	<i>In the scope of this profile, a user with higher privilege at the product's configuration level (may or may not be the same as the system administrator).</i>
Security Criteria Overview (SCO)	<i>A document outlining the general concepts of the BITS Security Lab criteria and items included in the individual product test plans. (see Appendix B).</i>
system	<i>Within the scope of this profile, the totality of the product and the mediation device (if any) that need to be tested.</i>
system administrator	<i>In the scope of this profile, an individual (user) with higher privileges at the operating system level.</i>
user-ID	<i>A number or name unique to a particular user of a computer or group of computers which share user information (the operating system, represents the user in data structures, e.g., the owner of a file or process, the person attempting to access a system resource).</i>

2. Criteria for the Administration and Operation of Application Security Products

2.1 Security Features

For each of the categories listed below, this section lists the minimal functionality in terms of security features expected in products of that category. This section lists the security criteria from the Master Security Criteria document that are common to all products and specifically apply to the administration and operation of most Application Security products. The criteria are categorized according to the following major sections in the Master Security Criteria.

1. Identification
2. Authentication
3. Authorization
4. Confidentiality
5. Data Integrity
6. Audit
7. Data Disposal
8. System Integrity
9. Security Administration
10. Guidance
11. Non-repudiation

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.1: Identification⁴		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
2.1.1	Required	
2.1.2	Required	
2.1.3	Required	
2.1.4	Required	
2.1.5	Required	
2.1.6	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.2: Authentication⁵		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
Subsection 2.2.1: General Mechanism Requirements		
2.2.1.1	Required	
2.2.1.2	Required	
2.2.1.3	Required	
2.2.1.4	Required	<i>Authentication of product to product administrator before this user gives password</i>
2.2.1.5	Required	

⁴ "identification" is defined as: The system shall have the capability of associating a user with an unambiguous identifier (e.g., user-ID) by which the said user shall be held accountable for the actions and events initiated by that user.

⁵ "Authentication" is identified as: The system shall offer features to verify the claimed identity of a user before allowing system access to the said user.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
<p>MSC Section 2.2: Authentication⁵</p> <p>Note: Criteria in this section are applicable to the <u>administration and operation of the product</u>, unless otherwise identified in the "Comment or Rationale" column.</p>		
2.2.1.6	Required	
2.2.1.7	Required	
2.2.1.8	Required	
<p>Subsection 2.2.2: Knowledge and Possession-based Mechanism Requirements</p>		
2.2.2.1	Required	
2.2.2.2	Required	
2.2.2.3	Required	
2.2.2.4	Required	
2.2.2.5	Required	
2.2.2.6	Required	
2.2.2.7	Required	
2.2.2.8	Required	
2.2.2.9	Required	
2.2.2.10	Required	
2.2.2.11	Required	
2.2.2.12	Required	
<p>Subsection 2.2.3: Personal Characteristics-Based Mechanism Requirements (DESIRED)</p> <p>Note: The classification of "DESIRED" for this entire subsection indicates the product submitted for evaluation may not need to comply with the criteria in this section. However, if the product is claiming to provide the capability it is <u>not</u> an optional section; it must fully comply with all criteria in this subsection (2.2.3).</p>		
2.2.3.1	Required (if claimed)	<i>See note accompanying 2.2.3 above</i>
2.2.3.2	Required (if claimed)	<i>See note accompanying 2.2.3 above</i>
2.2.3.3	Required (if claimed)	<i>See note accompanying 2.2.3 above</i>

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.3: Authorization⁶		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
2.3.1	Required	
2.3.2	Required	
2.3.3	Required	
2.3.4	Required	
2.3.5	Required	
2.3.6	Required	
2.3.7	Required	
2.3.8	Required	
2.3.9	Required	
2.3.10	Required	
2.3.11	Required	<i>In the context of this profile, the term "roles" implies "groups."</i>
2.3.12	Required	
2.3.13	Required	
2.3.14	Required	
2.3.15	Required	
2.3.16	Required	
2.3.17	Required	
2.3.18	Required	

⁶ "Authorization" is identified as: The system shall offer features to support the following restrictions: no user shall be allowed access to the system without Identification and Authentication; no user shall be allowed access to a resource (e.g., transaction, data, process, etc.) of the system unless specifically authorized to do so.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.3: Authorization⁶		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless otherwise identified in the "Comment or Rationale" column.		
2.3.19	Required	
2.3.20	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.4: Confidentiality⁷		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.4.1	Required	
2.4.2	Required	
2.4.3	Required	
2.4.4	Required	
2.4.5	Required	
2.4.6	Required	
2.4.7	Required	
2.4.8	Required	
2.4.9	Required	
2.4.10	Required	
2.4.11	Required	
2.4.12	Required	
2.4.13	Required	

⁷ "Confidentiality" is identified as: The system shall offer features to ensure that sensitive information shall be communicated and stored in a way such that only authorized users are allowed access.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.4: Confidentiality⁷		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.4.14	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.5: Data Integrity⁸		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.5.1	Required	
2.5.2	Required	
2.5.3	Required	
2.5.4	Required	
2.5.5	Required	
2.5.6	Required	
2.5.7	Required	
2.5.8	Required	
2.5.9	Required	
2.5.10	Required	

⁸ "Data integrity" is identified as: The system shall offer features to ensure that either: the data shall not be modified or altered without authorization in either storage or in transit; or any unauthorized modification of data shall yield an auditable security-related event.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.6: Audit⁹		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.6.1	Required	
2.6.2	Required	
2.6.3	Required	<i>Within the context of this profile, the product should have the <u>capability</u> to record all identified events (MSC v3, 2.6.3.1 – 11) as well as allowing the administrator to selectively enable/disable recording of the event.</i>
2.6.4	Required	
2.6.5	Required	
2.6.6	Required	<i>Within the context of this profile, notifications are not limited to email.</i>
2.6.7	Required	<i>Within the context of this profile, notifications are not limited to email.</i>
2.6.8	Required	
2.6.9	Required	
2.6.10	Required	
2.6.11	Required	
2.6.12	Required	

⁹ "Audit" is identified as: The system shall offer features to support the following functions: maintain a history file (also called an Audit Log) that records all security-related events pertinent to establishing an audit trail for a "post-mortem" analysis of a suspected security breach; ensure integrity of the audit log; generate customized audit reports; protect audit log(s) from unauthorized access; support administrator-selectable alerts for specified security-related events; support audit records of administrative events.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.7: Data Disposal¹⁰		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.7.1	Required	
2.7.2	Required	
2.7.3	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.8: System Integrity¹¹		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.8.1	Required	
2.8.2	Required	
2.8.3	Required	
2.8.4	Required	
2.8.5	Required	
2.8.6	Required	
2.8.7	Required	
2.8.8	Required	
2.8.9	Required	

¹⁰ "Data disposal" is identified as: The system shall ensure that there is no residual data exposed to unauthorized users as resources are allocated to those data objects or released from those data objects.

¹¹ "System integrity" is identified as: The system shall offer features to support the following functions: perform integrity checks for system functions; retain the security parameters after the occurrence of events such as system restart, disaster recovery, arrival of sensitive dates related to the Y2K issue, etc.; provide the back-up capability to restore the system, when necessary, to a well-defined state (such as the need to undo modifications to a file or to undo transactions); ensure that security features are always invoked and may not be bypassed unless authorized and configured to do so.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.8: System Integrity¹¹		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.8.10	Required	
2.8.11	Required	
2.8.12	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.9: Security Administration¹²		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.9.1	Required	
2.9.2	Required	
2.9.3	DESIRED	<i>Products are server based. Data is not necessarily processed in real-time. Within the context of this profile, "lockout" denotes "disconnect."</i>
2.9.4	DESIRED	<i>Products are server based. Data is not necessarily processed in real-time. Within the context of this profile, "lockout" denotes "disconnect."</i>
2.9.5	Required	
2.9.6	Required	

¹² "Security administration" is identified as: The system shall offer features to selectively authorize a highly privileged user (a security administrator) to perform day to day activities such as: activate protective features (e.g., the login feature); customize (i.e., override, if appropriate) vendor-provided defaults; monitor suspected activities related to a potential security breach; detect security violation incidents promptly, isolate and investigate the problem, and securely recover the system; Generate security audits when needed; and manage user accounts.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.9: Security Administration¹²		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
2.9.7	Required	
2.9.8	Required	<i>In the context of this profile, "override" means "modify."</i>
2.9.9	Required	
2.9.10	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.10: Guidance¹³		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the "Comment or Rationale" column.		
NEW	DESIRED	<i>NEW CRITERIA¹⁴: The product should document any and all modifications performed by the product. This includes modifications to itself and to other components of the system.</i>
2.10.1	Required	
2.10.2	Required	
2.10.2.1	Required	
2.10.2.2	Required	

¹³ "Guidance" is identified as: The vendor shall supply the following product support capability: a cogent security-related document for administration (e.g., a "Security Administration Guide") that would be made available as a hard copy or an electronic file, as an entity unto itself, and not fragmented throughout the reference manuals; a cogent user guide for security functions that would provide guidance for configuring the product's security features and maintaining security on an ongoing basis.

¹⁴ All criteria identified as "New Criteria" in this section will be reviewed by the Financial Services MSC Committee for possible inclusion in a future release of the MSC.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
2.10.2.3	Required	
2.10.2.4	Required	
2.10.2.5	Required	
2.10.2.6	Required	
2.10.2.7	Required	
2.10.2.8	Required	
2.10.2.9	Required	

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
MSC Section 2.11: Non-repudiation¹⁵		
Note: Criteria in this section are applicable to the <u>administration and operation of the product</u> , unless specifically identified in the “Comment or Rationale” column.		
NOTE: The classification of “DESIRED” here means that if the product submitted for evaluation does not provide non-repudiation functions, then it need not comply with the criteria in this section. However, if the product submitted for evaluation claims to provide non-repudiation functions, it must fully comply with items 2.11.1 – 2.11.3.		
2.11.1	Required	See NOTE above.
2.11.2	Required	See NOTE above.
2.11.3	Required	See NOTE above.

3.0 Product Functionality

This section of the criteria refers to the primary functionality of the product and how it is affected by security. For products whose primary functionality is not security (e.g., applications, databases, operating systems, etc.), this section will test how that functionality is impacted by the security features of the product, as described in Section 2 of the Criteria. However, for those products whose primary functionality is security-related (e.g., authentication systems, network security

¹⁵ “Non-repudiation” is identified as: The system shall have the capability of preventing users from successfully denying actions and events of users acting in the role of a sender or receiver.

products, authorization systems, etc.), the “functionality” criteria will address the main purpose of the product. In the cases of these product profiles, the “functionality” section of the criteria will often be as detailed, if not more so, than the “security features” section. Furthermore, since the Product Profiles address a wide variety of products within a class, it is permissible for the Profile to contain functionality criteria specific to a “subclass” of products (e.g., the Authentication Systems profile might contain criteria specific to biometrics systems, smart cards, PKI, etc.).

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
3.1	Required	
3.2	Required	

4.0 Scalability

Scalability criteria shall specify minimum limitations in terms of traffic/use parameters of volume, frequency or time. These criteria are used to assess the degree to which security service objectives are met, at or near system capacities or *across multiple platforms*. The focus of the testing shall be to verify vendor claims of the scalability of the product in a standard configuration. The criteria are applied in tests that are designed to stress the product design and to determine that the product retains security functionality as the offered traffic exceeds stated system capacities.

MSC REFERENCE	REQUIRED, DESIRED OR N/A	COMMENT OR RATIONALE
4.1	Required	

3. Required Functional Criteria for All Application Security Products

3.1. Introduction

This section will list the required criteria for the functional areas that are common to all products in this profile. Product subclasses will have additional and unique functionality for which additional required criteria will be listed separately in Section 5.

Rationale statements will be applied where appropriate.

3.2 Administration

<i>CRITERIA</i>		<i>RATIONALE</i>
3.2.1	The product shall allow the product administrator to specify threshold parameters to control and/or limit the generation of alerts.	<i>For example, send an alarm when incoming mail volume from a certain sender exceeds the threshold.</i>
3.2.2	The product shall allow the administrator to exclude certain users or groups of users from the filtering process.	<i>Products need to be configurable and flexible to specify the default processing to occur, but administrators need to be able to make exceptions to the rules, based on business needs and unique requirements of certain users or classes of users. For example, the default specification may be to block ActiveX, but certain developers may need access to a site that provides support services using ActiveX components. This may be provided using user account identifiers or IP addressing.</i>
3.2.3	The product shall support centralized policy management for permit/deny rules, configuration parameters, and distribution so that multiple instances of the product can be centrally managed.	

3.3 Event Logging and Alerting

<i>CRITERIA</i>		<i>RATIONALE</i>
3.3.1	The product shall log each event that it has been configured to detect or alert.	<i>To provide forensics for prevention and prosecution, the product shall log, minimally, time of violation, source, nature of violation and related user session information.</i>
3.3.2	The product shall log time of violation, source, nature of violation and related user session information.	<i>Provide forensics for prevention and prosecution.</i>
3.3.3	The product shall proactively alert administrators of events that it has been configured to detect or alert on.	<i>The product shall enable administrator configurable security related event logging and an alert capability associated with logged events.</i>

3.4 Product Configuration

<i>CRITERIA</i>		<i>RATIONALE</i>
3.4.1	The product shall come configured in its default state that provides the greatest level of security.	<i>Administration should have the ability to choose the appropriate level of security upon installation.</i>
3.4.2	The product shall provide centralized configuration capabilities and shall provide an authorized administrator the capability to automatically propagate changes to all or selected nodes.	
3.4.3	The product shall not interfere with the operation of (a) other clients or applications or (b) the host system.	<i>The product should not interfere or alter the successful operation of existing components such as: web servers, firewalls, load balancers, SSL, etc.</i>

4. Desired Functional Criteria for All Application Security Products

4.1 Introduction

This section will list the optional criteria for the functional areas that are common to all products in this profile. Some subclasses of products will have additional, unique, functionality for which additional optional criteria will be listed separately in Section 5.

Rationale statements will be applied where appropriate.

4.2 Product Configuration

<i>CRITERIA</i>	<i>RATIONALE</i>
4.2.1 DESIRED: The product should support the ability to deploy the product in a fault-tolerant or high-availability configuration.	
4.2.2 DESIRED: The product should provide the administrator the ability to define the fail-over state.	<i>How a product is configured and how it is integrated into an environment can determine the effect a failure will have on security. Failure of the product may leave current or pending sessions in an "open" state, leading to loss of security, or in a "closed" state, leading to a loss of availability. The organization needs the ability to specify the fail-over state based on its assessment of the associated risks and the business requirements.</i>
4.2.3 DESIRED: The product should integrate with third-party systems management tools.	<i>For example, this capability can facilitate centralized proactive alert monitoring and administration simplicity/consistency, etc. Note: Although this is primarily an operational issue, it is desired within products in this class to support various enterprise management tools. In the context of this profile, "management tools" are considered "commonly available enterprise management systems," typically using common industry-standard interfaces and protocols, such as SNMP.</i>
4.2.4 DESIRED: The product should support the capability of remote logging of various audit events and maintain integrity of the remote log.	<i>Recognizing it is easy to compromise the integrity of remote logging of audit events, the desired functionality of this criterion encourages products to maintain integrity of this data via various, secure and standards-</i>

<i>CRITERIA</i>	<i>RATIONALE</i>
	<p><i>based mechanisms.</i></p> <p><i>Also, it is understood that this capability may impose risks. However, this criterion is considered a desirable feature of products in this product classification. Enterprises would base the decision to use this desired capability on a variety of corporate business and risk factors.</i></p>

5. Functional Criteria for Application Security Product Subclasses

5.1. Introduction

For each of the subclasses listed below, this section lists the minimal functionality in terms of functional criteria expected in products of that subclass.

Application-Content Filtering Security Products

These are products that provide validation of application layer protocols, the analysis and control of application requests and the prevention of unauthorized activity for the protection of Internet application servers.

Internet-Content Filtering Security Products

These are products that provide server-based content filtering, virus scanning, malicious code scanning and/or encryption for the protection of Internet client systems (e.g. a web browser).

Email Security Products

These are products that provide server-based filtering, virus scanning, malicious code scanning and/or encryption for email systems.

5.2. Functional Criteria for Application-Content Filtering Security Products

<i>CRITERIA</i>		<i>RATIONALE</i>
5.2.1	The product shall allow the administrator to specify the actions to take when a request is found to violate a specified security policy.	<i>The administrator needs the flexibility to specify what action should be taken, depending on the policy specification. For example, after the system tests the message and is found to violate a specified policy, the application could (1) log the failure, (2) generate appropriate alerts, and (3) permit the message to pass through to its designed destination, or (4) block or quarantine the message for security reasons.</i>
5.2.2	The product shall allow the administrator to configure the notification message sent to users when a request is blocked for security reasons.	

CRITERIA		RATIONALE
5.2.3	The product shall protect application logic and business rules. The product shall not allow unauthorized user behavior and application usage.	<i>Only allow users to execute application code for its intended purposes. Prevent parameter tampering, manipulation of hidden fields, Trojan-Horses, etc.</i>
5.2.4	The product shall prevent unauthorized manipulation of application data.	<i>Protect information residing on the client system from unwarranted or unexpected access or modification</i>
5.2.5	The product shall provide the capability to customize application enforcement rules.	<i>Allow administrators to define application policy enforcement.</i>
5.2.6	The product shall isolate individual user-sessions to prevent users from accessing another user's information	<i>Only allow users to follow intended application path and access their own information.</i>
5.2.7	The product shall have the capability to prevent execution of damaging commands via the application.	<i>Prevent cross-site scripting, injection of executable code in text fields, stealth commands, etc.</i>

5.3. Functional Criteria for Internet-Content Filtering Security Products

CRITERIA		RATIONALE
5.3.1	The product shall scan active code in raw, compressed or encapsulated forms.	
5.3.2	The product shall offer the ability to run mobile code ¹⁶ in a safe "sandbox" ¹⁷ to check for unexpected execution time activity.	
5.3.3	The product shall offer facilities to quarantine or prevent the execution of suspicious or unknown code types.	
5.3.4	The product shall have the ability to	

¹⁶ Within the context of this profile, "mobile code" will refer to any code that cross-networks and executes on a destination (typically, non-specific platform) system. This can include, but is not limited to, code created with Java, Javascript, VBScript, ActiveX and application macros (MS-Word, MS-Excel).

¹⁷ Within the context of this profile, "sandbox" will refer to a restricted area of the web browser allocated specifically to an applet. This provides a limited-access environment, to the user's system resources, for the execution of non-trusted code (i.e. applets).

CRITERIA		RATIONALE
	perform content scanning with keyword context intelligence.	
5.3.5	The product shall provide the administrator the capability to define keywords.	<i>In support of content scanning, administrators must have the ability to define keywords to be used (or not used) and not be dependent upon distributions from the Product vendor.</i>
5.3.6	The product shall be able to validate the signature of signed code.	
5.3.7	The product shall block the execution of signed code if the signer is explicitly defined on the “deny” list or is not explicitly defined on the “permit” list subject to a default action for permit and deny.	<i>Although the signature on the signed code may be valid and from a known party, the user should retain the ability to control and execute permission based on the source, and with the flexibility to implicitly or explicitly permit or deny the action.</i>
5.3.8	The product shall provide the ability for the product administrator to define code types and actions to be taken for these code types.	
5.3.9	The product shall provide the product administrator the ability to define both "permit" and "deny" lists of signers.	
5.3.10	The product shall provide the ability for the product administrator to deny or permit communications using access control lists.	<i>Administrators need flexibility in how they control communication. The product should support the ability to control access using IP addresses or subnets, user names, either defined locally or in conjunction with LAN applications such as NT Server and Netware, or by the network interfaces the product is connected to.</i>
5.3.11	The product shall provide the ability for the product administrator to specify “permit” or “deny” as the default action to take when a message fails a policy check or an applicable policy does not exist.	
5.3.12	The product shall allow the administrator to specify the actions to take when a request is found to violate a specified security policy.	<i>The administrator needs the flexibility to specify what action should be taken, depending on the policy specification. For example, after the system tests the message and is found to violate a specified policy, the application could (1) log the failure, (2) generate appropriate alerts, and (3) permit the message to pass through to its designed destination, or (4) block or quarantine the message for security reasons.</i>

CRITERIA		RATIONALE
5.3.13	The product shall allow the administrator to configure the notification message sent to users when a request is blocked or quarantined for security reasons.	
5.3.14	The product shall provide the administrator the ability to retrieve quarantined code.	
5.3.15	DESIRED: The product should protect application logic and business rules. The product should not allow unauthorized user behavior and application usage.	<i>Only allow users to execute application code for its intended purposes. Prevent parameter tampering, manipulation of hidden fields, Trojan-Horses, etc.</i>
5.3.16	DESIRED: The product should prevent unauthorized manipulation of application data.	<i>Protection information residing on the client system from unwarranted or unexpected access or modification.</i>
5.3.17	DESIRED: The product should provide the capability to customize application enforcement rules.	<i>Allow administrators to define application policy enforcement.</i>
5.3.18	DESIRED: The product should isolate individual user-sessions to prevent users from accessing another user's information.	<i>Only allow users to follow intended application path and access their own information.</i>
5.3.19	DESIRED: The product should have the capability to prevent execution of damaging commands via the application.	<i>Prevent cross-site scripting, injection of executable code in text fields, stealth commands, etc.</i>

5.4 Functional Criteria for Email Security Products

CRITERIA		RATIONALE
5.4.1	The product shall scan email and attachments, in raw, compressed or encapsulated forms.	<i>In order to scan and detect malicious code effectively, the product must scan the incoming text stream including encapsulated forms such as post script, and common attachment types, such as Acrobat, script, executable, and Zip files, for virus and malicious code.</i>
5.4.2	The product shall provide the ability to filter or block email content based on policies defined by the product administrator.	

CRITERIA	RATIONALE
5.4.3 The product shall allow the administrator to define appropriate reactions to email that violate policy.	<i>Such reactions might be to quarantine the message, delete message, bounce message and reject connection.</i>
5.4.4 The product shall allow the administrator to define whether or not a notification message should be sent to the sender and/or the receiver when a received email violates the configured policy.	<i>Some products provide the ability to send a notification to the sender that a received message was “repaired”, “rejected”, or “returned”, and whether or not the message was actually forwarded to the recipient. In some cases, the connection itself from the sender may be rejected. The product must provide the administrator the ability to specify what action to take for each policy violation. In some cases, the administrator may desire an alert only when the volume of policy violations exceeds an administrator-specified threshold. For example, an alert may only be wanted when the number of connection attempts from a designated sender exceeds 100 connections per second.</i>
5.4.5 The product shall determine the email attachment type without relying on file extension name. If such a determination cannot be made unambiguously, then the product shall offer facilities to quarantine or prevent the transmission of such attachments based on the security policy specifications	<i>It is not always possible to make an absolutely accurate determination of the attachment type. Some commercially available email security products offer a quarantine function in recognition of this technical reality.</i>
5.4.6 The product shall have the ability to perform content scanning with keyword context intelligence.	<i>Although it is recognized that keyword-in-context scanning is difficult to achieve in practice, products should not claim this ability unless it is effective. For example, context filtering on keyword “breast” should not take action on messages containing “breast cancer institute.”</i>
5.4.7 The product shall provide the administrator the capability to define keywords.	<i>In support of keyword content scanning, administrators must have the ability to define keywords to be used (or not used) and not be dependent upon distributions from the product vendor. Keyword scans should be permitted minimally on the Subject, Sender, Recipient, and message text fields.</i>

Appendix A: Industry Standards

For the purposes of these criteria, the terms “public and widely used or financial industry standards” shall refer to those standards, algorithms, and protocols listed below as well as other relevant standards approved by the following standards organizations: IETF, ANSI X9, ITU-T, ISO, NIST, and IEEE.

Symmetric encryption algorithms	<ul style="list-style-type: none"> • 3DES (ANS X9.52, X9.66) • IDEA • RC4 • RC5 • RIPEM
Asymmetric algorithms (for symmetric key agreement or key transport)	<ul style="list-style-type: none"> • RSA (ANS X9.44) • D-H (minimum 1024-bit modulus – ANSI X9.42) • ECDH (ANS X9.63) • Elliptic Curve
Digital hashing algorithms	<ul style="list-style-type: none"> • SHA-1 (ANS X9.30-2) • MD5
Digital signature algorithms	<ul style="list-style-type: none"> • DSA (ANS X9.30-1) • rDSA (ANS X9.31) (includes RSA) • EC-DSA (ANS X9.62)
Key management standards and protocols	<ul style="list-style-type: none"> • ANS X9.70, ANS X9.73, ANS X9.69, ANS X9.24, ANS X9.77 • CMP • PKCS #7, #10 • IETF PKIX standards
Random number generators	<ul style="list-style-type: none"> • ANS X9.82
Prime number generators	<ul style="list-style-type: none"> • ANSI X9.80
Cryptographic device security	<ul style="list-style-type: none"> • ANS X9.66 • FIPS 140-2
Peer entity authentication	<ul style="list-style-type: none"> • ANS X9.72 • FIPS 196
PIN security	<ul style="list-style-type: none"> • ANS X9.8, ANS X9.86, ANS X9.87
Biometrics management and security	<ul style="list-style-type: none"> • ANS X9.84
Directory standards	<ul style="list-style-type: none"> • X.500 • LDAP v3
TCP/IP integrity	<ul style="list-style-type: none"> • IPsec

The system shall use any of the algorithms listed above or those that are supported by any of the standards organizations listed above. If the system uses any other cryptographic algorithm, then it shall be configurable to also allow the use of an acceptable algorithm in place of the unlisted algorithm.

Appendix B: Bibliography

MSC *Master Security Criteria (v3.0)*, BITS, October 2001

Appendix C: Glossary of Terms

Definitions provided in this document are provided via references in various books and publications. Several of these references are included at the end of this section.

TERM	DEFINITION
access control	<i>A mechanism for limiting use of some resource to authorized users. [1]</i>
account	<i>In terms of a “user account”, an account is an established relationship between a user and a computer, network or information service.</i>
active attack	<i>An attack which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files. [3]</i>
administrator	<i>Taken in the context of this profile and if used without pre-qualification, this term indicates any user (or group of users) that could be defined as being a system administrator and/or product administrator, typically having privilege beyond the scope of an end-user. See also “end user”, “user” and “product administrator.”</i>
automated Information System (AIS)	<i>Any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware. [3]</i>
application Programming Interface (API)	<i>Typically provided by a software development toolkit.</i>
applet	<i>Typically, a small program not resident on the local system, which, when downloaded, executes from within another application on that local system. For example, dynamically downloaded Java programs that execute within Internet browsers are considered applets.</i>
asymmetric cryptography	<i>A class of cryptographic algorithms that use separate keys for encryption and decryption. [2]</i>
attack	<i>An attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures. [3]</i>
audit	<i>To keep a record of events that might have some security significance, such as when access to resources occurred. [1]</i>
authenticate	<i>To determine that something is genuine. To reliably determine the identity of a communicating party. [1]</i>
authentication	<i>The process of reliably determining the identity of a communicating party.[1]</i>
authenticator	<i>The method, material or credential used to create and/or implement authentication bindings, such as a password, PIN number, token seed, Smart card seed, etc.</i>
authorization	<i>Permission to access a resource.[1]</i>
biometric device	<i>A device that authenticates people by measuring some hard-to-forge physical property, like a fingerprint or the strokes and timing of a signature.</i>
biometrics	<i>Using physical characteristics of users such as fingerprints and retinal impressions to authenticate users. [2]</i>
buffer overflow	<i>This happens when more data is put into a buffer or holding area, then the buffer can handle. This is due to a mismatch in processing rates between the producing and consuming processes. This can result in system crashes or the creation of a back</i>

TERM	DEFINITION
	<i>door leading to system access. [3]</i>
certificate	<i>A message signed with a public key digital signature stating that a specified public key belongs to someone or something with a specified name. [1]</i>
certificate authority (CA)	<i>Something trusted to sign certificates. [1]</i>
certificate revocation list (CRL)	<i>A list containing names of users and roles that are no longer valid within a public key cryptography system.[2]</i>
challenge-response	<i>An authentication mechanism in which the authentication process sends a challenge to a process that requests authentication; the latter is authenticated only if it sends the correct response to the authentication process.[2]</i>
clear text	<i>A message or data that is not encrypted.</i>
client	<i>Something that accesses a service by communicating with it over a computer network. [1]</i>
confidentiality	<i>The property of not being divulged to unauthorized parties. [1]</i>
credential	<i>A letter or certificate given to a person to show that he has a right to confidence or to the exercise of a certain position or authority. [5]</i>
cryptography	<i>The practice of encoding and decoding data.</i>
decrypt	<i>To undo the encryption process. [1]</i>
dictionary attack	<i>Typically an “offline attack” or “brute force attack” ... this is the process of “guessing” passwords, based on a set of key words or characters, until a match is made.</i>
digital signature	<i>A method based on public key encryption to verify identities over a network.</i>
distributed system	<i>Multiple systems and/or processors that are working to support one set of applications or functions, even from geographically disperse locations.</i>
DLL	<i>Dynamic Link Library – Software (executable code or data, such as icons or fonts) used by Microsoft's Windows and IBM's OS/2 to provide services (such as a LAN driver or a distributed filing system) to applications. One memory-resident copy of the DLL can be simultaneously shared by all applications.</i>
DNS	<i>Domain Name System - an Internet service that translates domain names into IP addresses.</i>
dongle	<i>A device that attaches to a computer to control access to a particular application.</i>
end user	<i>Taken in the context of this profile and unless otherwise indicated, this term will be associated with the end-user of the product. See also “user” and “administrator.”</i>
encrypt	<i>To scramble information so that only someone knowing the appropriate secret can obtain the original information (through decryption).</i>
escrow	<i>To hold something in safekeeping. Most uses of the word actually mean keeping the something safe from the owner as opposed to providing any safety for the owner.</i>
group	<i>A named collection of users, created for convenience in stating authorization policy.</i>
hash	<i>A cryptographic one-way function that takes an arbitrary-sized input and yields a fixed-size output. [1]</i>
immutable	<i>Unchangeable. [2]</i>
integrity	<i>The quality of being uncorrupted. Message integrity refers to the state of a message not being modified while in transit. File integrity refers to the state of files not being modified while in storage. [2]</i>

TERM	DEFINITION
key	<i>A quantity used in cryptography to encrypt or decrypt information.</i>
key escrow	<i>The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees. [3]</i>
log	<i>To record an action. [2]</i>
log file	<i>A file that lists actions that have occurred. [2]</i>
MAC	<i>Message Authentication Code – a synonym of message integrity code (MIC). [1]</i>
malicious code	<i>(Also “Malicious Mobile Code”) Mobile code software modules designed, employed, distributed, or activated with the intention of compromising the performance or security of information systems and computers, increasing access to those systems, providing the unauthorized disclosure of information, corrupting information, denying service, or stealing resources. [6]</i>
message digest	<i>An irreversible function that takes an arbitrary sized message and outputs a fixed length quantity. MD2, MD4, and MD5 are message digest algorithms. [1]</i>
multifactor	<i>More than two elements or quantities.</i>
message integrity code (MIC)	<i>A fixed-length quantity generated cryptographically and associated with a message to reassure the recipient that the message is genuine. [1]</i>
(NIST)	<i>National Institute of Standards and Technology.</i>
non-repudiation	<i>The property of a scheme in which there is proof of who sent a message that a recipient can show to a third party and the third party can independently verify the source. [1]</i>
NTP	<i>Network Time Protocol.</i>
OCSP	<i>Online Certificate Status Protocol.</i>
offline attack	<i>An attack performed while offline to the system being attacked (see also “dictionary attack”).</i>
one-time passwords	<i>Passwords that can only be used one time. [2]</i>
operator	<i>In the context of this profile, “operator” maintains similar relationships and functions as “administrator” (see above), given different and/or additional privileges than a typical “end user” of a system.</i>
orthogonal	<i>Having to do with right angles; rectangular. [5]</i>
passive attack	<i>Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data. [3]</i>
password	<i>A supposedly secret string used to prove one’s identity. [1]</i>
personal identification number (PIN)	<i>A short sequence of digits used as a password. [1]</i>
public Key Cryptography Standards (PKCS)	<i>A set of standards first introduced in 1991 by RSA Data Security, Inc., for implementing public key cryptographic algorithms and incorporating them in to applications. [2]</i>
plaintext	<i>Unencrypted data. [3]</i>
pre-authentication	<i>A protocol for proving you know your password before you are allowed access to a high quality secret encrypted with that password. [1]</i>
private key	<i>The quantity in public key cryptography that must be kept secret. [1]</i>

TERM	DEFINITION
privileged user	<i>A user of a computer or system who is authorized to bypass normal access control mechanisms, usually to be able to perform system management functions. [1]</i>
product administrator	<i>In the scope of this profile, this role is associated with a user having higher privilege at the product's configuration level. This user (role) may be the same as the system administrator, but could also be different.</i>
protected path	<i>A mechanism that guarantees a mutually authenticated channel. [4]</i>
public key	<i>The quantity in public key cryptography that is safely divulged to as large an extent as is necessary or convenient. [1]</i>
public key cryptography	<i>A cryptographic system where encryption and decryption are performed using different keys – see Asymmetric key cryptography. [2]</i>
relying party	<i>In the scope of this profile, “relying party” is typically associated with the use of “system” (see below). It is associated frequently with the extent of which a criteria is in scope as in references to an application or component maintaining reliance on another element to support said criteria.</i>
replaying	<i>Storing and retransmitting messages. The word is usually used when implying that the entity doing the reply of messages is mounting some sort of security attack.</i>
repudiation	<i>Denying that you did something or made some statement. [1]</i>
revoke	<i>To withdraw, repeal, rescind, cancel, or annul. [5]</i>
role	<i>A function or office assumed by someone. [5]</i>
security domains	<i>The sets of objects that a subject has the ability to access. [3]</i>
security features	<i>The security-relevant functions, mechanisms, and characteristics of AIS hardware and software. [3]</i>
server	<i>Some resource available on the network to provide some service such as name lookup, file storage, or printing. [1]</i>
sign	<i>To use your private key to generate a digital signature as a means of proving you generated, or approve of, some message.</i>
signature	<i>A quantity associated with a message which only someone with knowledge of your private key could have generated, but which can verified through knowledge of your public key. [1]</i>
spoof	<i>To convince someone that you are some entity X when you are not X, without X's permission. [1]</i>
strong authentication	<i>Authentication performed in such a way that it cannot easily be performed. Examples of strong authentication include one-time passwords, challenge-response mechanisms, and cryptographic authentication. [2]</i>
symmetric key cryptography	<i>A class of cryptographic algorithms in which the same key is used for encryption and decryption. Examples of symmetric key algorithms include DES, IDEA, RC2, and RC4. [2]</i>
system	<i>Within the scope of this profile, “system” is used to imply the totality of the product and the mediation device (if any) that need to be tested. [SCO 2.1.1]</i>
system administrator	<i>In the scope of this profile, an individual (user) having higher privilege at the operating system level.</i>
system restart	<i>To restart a system. May also be referenced as a “warm boot”, whereas the system is restarted from an operational state. Additionally, may also be referenced as a “cold boot”, whereas the system is powered off and then on again.</i>

TERM	DEFINITION
token device	<i>A credit-card sized device that generates authentication tokens, such as one-time passwords. [2]</i>
two-factor authentication	<i>A process in which two pieces of information are required to prove one's identity (such as a password and a smart card). [2]</i>
weak authentication	<i>Typically, this implies the conventional use of passwords.</i>
user	<i>Taken into the context of this profile and if used without pre-qualification, this term indicates any and all users, such as end-user, product user-ID or system user.</i>
user-ID	<i>A number or name which is unique to a particular user of a computer or group of computers which share user information. The operating system uses the uid to represent the user in its data structures, e.g. the owner of a file or process, the person attempting to access a system resource etc.</i>
X.509	<i>A CCITT standard for security services within the X.500 directory services framework. The X.509 encoding of public key certificates has been widely adopted; the other protocol elements of X.509 have not. [1]</i>

Glossary Items are based on the following references:

- [1] Kaufman, C., Perlman R. and Speciner M., *Network Security: Private Communication in a Public World*, Prentice Hall, New Jersey, 1995
- [2] Bernstein, T., Bhimani A., Schultz E., and Siegel C., *Internet Security for Business*, John Wiley & Sons, Inc., New York, 1996
- [3] NSA Glossary of Terms used in Security and Intrusion Detection
- [4] Loscocco Peter A., Smalley Stephen D., Muckelbauer Patrick A., Taylor Ruth C., Turner S. Jeff, Farrell John F., *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments*, 1998
- [5] Guralnik, David Bernard (editor), *Webster's New World dictionary of the American Language*, 1986
- [6] Department of Defense, Memorandum, November 7, 2000, Subject: Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems