NETWORK SECURITY FRAMEWORK: ROBUSTNESS STRATEGY

Teri Arber, NSA
Deb Cooley, NSA
Steve Hirsch, NSA
Martha Mahan, NSA
Jim Osterritter, NSA

ABSTRACT

As commonly perceived, robustness deals with how systems protect, detect, adapt, recover, and/or reconfigure from anomalies to provide some desired level of security services. This paper is a strategy for the development of a general security mechanism/countermeasure valuation scheme. The general objective addresses the question, *"Given the value of information to be protected and the threat environment, how strong and assured should security mechanism(s) be to provide the desired security service(s)?"* It characterizes the relative strength of mechanisms, which provide security services, and provides guidance in selecting these mechanisms. It describes a process that, when completed in a later release of the Network Security Framework (NSF) will provide guidance in assessing the degree of robustness (defined as level of security mechanism strength, along with appropriate assurances) recommended in a particular INFOSEC solution. The process described in this paper may be applied to all components of a solution, both products and systems, to determine the robustness of configured systems as well as of their component parts. It applies to COTS, GOTS, and hybrid solutions. The actual robustness of an overall network solution must take into account the implications of composing layered mechanisms and also incorporate an overall assessment of vulnerabilities and residual risks. This paper is an update to Section 4.4 (Robustness Strategy) of Release 1 of the NSF.

1.0 INTRODUCTION

The *Robustness Strategy* provides a philosophy and initial guidance for selecting the strength of security mechanisms and the security assurance provisions that may be needed for a particular value of information and potential threat level. Note that the Robustness Strategy is not intended to provide universal answers to needed strength or assurance; it is not intended as a "cook book". It should be understood that the final selection of mechanisms, and the level of strength and assurance that is needed will result from an Information Systems Security Engineering (ISSE) activity, and a resultant risk management process that addresses the specific situation of a specific user, mission, and environment.

1.1 Purpose

The Robustness Strategy describes a process that, when completed in a later release of the NSF, will provide guidance in assessing the *degree of robustness*. Robustness is defined as level of security mechanism strength and assurances recommended (considered "good enough") in an INFOSEC solution. At the current stage of development, the Strategy deals primarily with these levels within individual security services and mechanisms based on information of a given value, in a particular (static) threat environment. As discussed below, this is not a complete answer. The process is not intended to provide an endorsement or credential for specific products, nor is it intended to serve as a "cookbook" answer for the robustness of solutions; rather, it offers security engineering guidance to developers, integrators, and risk managers as input to risk management. Users of the NSF can employ the Robustness Strategy for:

- Providing guidance to help developers and integrators assess (1) what strength of mechanism(s), (2) what levels of assurance (in development methodology, evaluation, and testing), and (3) what criteria are recommended for a particular configuration meant to protect information of a particular value with a specific intelligence life in a specific, static threat environment.
- Defining product requirements for different customer scenarios (value of information, threat, configuration, etc.) e.g., as described in the NSF.

- Providing feedback to security requirements developers, decision-makers, customer representatives, customers, etc.
- Constituting developmental requirements when a security solution does not exist.
- Working with academia to foster research in the network security arena, and to educate future engineers, architects, and users in network security technology.
- Performing subsequent risk assessments made necessary by reconfiguration of the system/network under review or by a change in threat or value of information.

As technology in general and INFOSEC threats in particular evolve, so will countermeasures need to evolve, and with them the corresponding application guidance. This paper is a strategy for the development of a valuation scheme for general security mechanisms or countermeasures. Rather than directly defining security requirements, which need to be met, it characterizes the relative strength of mechanisms, which provide security services, and provides guidance in selecting these mechanisms. There is no concept of official compliance with the Robustness Strategy in terms of approving a solution. It is a *strategy*, an aid to "getting you there", as opposed to a prescriptive solution (where nominal compliance assures acceptability).

Trained Information Systems Security Engineers (ISSEs) [ISSEH] support customer organizations in defining and applying security solutions to address their Information Assurance (IA) needs. Working with a customer from initial contact through solution acceptance, an ISSE helps ensure that the customer's security needs are appropriately identified and that acceptable solutions are developed. Within the context of the Network Security Framework Robustness Strategy, an ISSE helps the customer assess the value of his information/assets and the security threat within the operational environment, identify security services necessary to provide appropriate protection, and provide guidance on the characteristics of specific security mechanisms which provide those services.

2.0 OVERVIEW OF THE GENERAL PROCESS

The Robustness Strategy is intended to be applied in the context of the development of a security solution and to be consistent with NSF System Security Methodology Chapter, which describes the overall process. An integral part of that process is to determine the recommended strength and degree of assurance of proposed security services and mechanisms that become part of the solution set. The strength and assurance features serve as a basis for the selection of the mechanisms, and as a means to evaluate products that implement those mechanisms. This paper provides guidance for determining the recommended strength and assurance.

The process should be applied to all components of a solution, both products and systems, to determine the robustness of configured systems as well as of their component parts. It applies to Commercial Off-The-Shelf (COTS), Government Off-The-Shelf (GOTS), and hybrid solutions. As indicated above, the process provides insight to security requirements developers, decision-makers, ISSEs, customers, and others involved in the solution life cycle. Clearly, if a solution component is subsequently modified, or threat or value of information levels change, there needs to be a reassessment of risk with respect to the new configuration.

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

3.0 DETERMINING THE DEGREE OF ROBUSTNESS

We define the *degree of robustness* as the level of strength and assurance recommended for potential security mechanism(s). In order to determine this level for a given security service in a particular application, the customer (and ISSE) should consider the value of the information to be protected (in relation to the operational mission) as well as the perceived threat environment. Guidelines for determining these values are provided below.

It should be noted that the Robustness Strategy focuses specifically on individual security services and mechanisms. The actual robustness of an overall network solution will need to extend the perspective of

individual solutions. It must take into account the implications of composing layered mechanisms and also incorporate an overall assessment of vulnerabilities and residual risks, as discussed in NSF System Security Methodology Chapter.

Many customers, in support of their mission, have a need to protect information (or an information system) which, if compromised, could adversely affect the security, safety, financial posture, and/or infrastructure of the organization. Five levels of information value have been defined:

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

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

The following threat levels were derived from various relevant works (e.g. [SMI96]) and discussions with subject matter experts throughout the ISSO. Seven levels of threat have been defined:

- **T1:** Inadvertent or accidental events (e.g., tripping over the power cord).
- **T2:** Passive, casual adversary with *minimal* resources who is willing to take *little* risk (e.g., listening).
- **T3:** Adversary with *minimal* resources who is willing to take *significant* risk (e.g., unsophisticated hackers).
- **T4:** *Sophisticated* adversary with *moderate* resources who is willing to take *little* risk (e.g., organized crime, sophisticated hackers, international corporations).
- **T5:** *Sophisticated* adversary with *moderat*e resources who is willing to take *significant* risk (e.g., international terrorists).
- **T6:** *Extremely sophisticated* adversary with *abundant* resources who is willing to take *little* risk (e.g., well-funded national laboratory, nation-state, international corporation).
- **T7:** *Extremely sophisticated* adversary with *abundant* resources who is willing to take *extreme* risk (e.g., nation-states in time of crisis).

Table 3-1 Degree of Robustness

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

After a determination is made regarding the value of information to protect and the threat environment, the ISSE can provide guidance on how strong a security mechanism should be to protect that information as well as guidance on the assurance activities that should be performed. Table 3-1 indicates the minimal Strength of Mechanism Level (SML) and Evaluation Assurance Level (EAL) [CC] recommended to provide protection of

information or information systems of a given value (V1-V5) against a given adversary threat level (T1-T7). Section 4.0 defines the SMLs and Section 5.0 defines the EALs.

4.0 STRENGTH OF MECHANISM

Strength of Mechanism Level is presented by a series of tables focusing on specific security services. At the current stage of development, the Strategy is still being formulated, and the tables are not considered complete or adequately refined. There are a number of additional security mechanisms that are not detailed in the tables but which may be appropriate to provide some security services. Further, the Strategy is not intended to imply that it alone will provide adequate information for the selection of whatever mechanisms may be desired (or sufficient) for any particular situation. As indicated earlier, an effective security solution will only result from the proper application of ISSE skills to specific operational and threat situations. The Strategy does offer a methodology for structuring a more detailed analysis. The security services itemized in these tables have several related supporting security services that may result in recommendations for inclusion of additional security mechanisms and techniques.

For each service, recommended guidance for each of the three SML levels is given for a variety of mechanisms that provide the overall service. In some cases, a group of mechanisms will be required to provide the necessary protection. It should also be noted that an ISSE, in conjunction with a customer, could decide to use a stronger or weaker mechanism than is recommended depending on the environment. It is the intent of the Strategy to ensure that mechanisms across services at the same strength level provide comparable protection, in that they counter equivalent threats. The selection of mechanism(s) from the service tables is an independent event, in the sense that one mechanism does not necessarily require another. Higher strength mechanisms don't necessarily embody features of lower strength mechanisms (i.e., security functions don't necessarily accumulate at higher strength levels). Table entries are preliminary estimates based on consultation with subject matter experts, and are likely to be revised based on technology evolution, threat assessment, and costing development.

The strength referred to below is a *relative* measure of effort (cost) required, defeating the mechanism, and is not necessarily related to the cost of implementing such countermeasures. All things equal especially cost, the “highest” strength mechanism should always be chosen. There are three Strength of Mechanism Levels defined:

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

4.1 Mechanisms Supporting Security Management

Recommended mechanisms for establishing needed security management are depicted in Table 4-1. The degree of awareness and/or control with respect to the following will identify the SML target:

- ***Compromise Recovery***, in addition to achieving a secure initial state, secure systems must have a well-defined status after failure, either to a secure failure state or via a recovery procedure to a known secure state.
- Poor ***System Administration*** is a leading cause of security weaknesses and vulnerabilities. It is the first line of defense in enforcing the security policy. See the NSF Non-Technical Security Countermeasures Section for more information on system security administration.
- ***Training*** is what operators and users need to obtain to learn about security features and system operation. Knowledgeable users are more likely to exercise due care in protecting information assets (increased risk of insider attack is dealt with via personnel security).
- The ***OPSEC*** process is a coordinated multidisciplinary five-step activity involving, identification of critical information, threat identification and analysis, vulnerability identification and analysis, risk assessment,

and adoption of countermeasures. Each use of the process is tailored to a specific activity of concern, whose totality is examined for potential disclosure to specific adversaries, upon which to base directly pertinent countermeasures. Consult with the Interagency Operation Support Staff (IOSS) for case by case consideration.

- ***Trusted Distribution*** is a calculated/controlled method for distributing security critical hardware, software, and firmware components, both originals and updates, that provides protection of the system from modification during distribution, and for the detection of any changes.
- ***Secure Operations*** is the level of standard operating procedures for security protection at the appropriate classification, sensitivity, and/or criticality of the data and resources that are being handled or managed. This includes security doctrine.
- ***Mechanism Management***, certain security mechanisms (e.g., cryptographic algorithms) have ancillary support needs (e.g., key management).

Table 4-1 Security Management Mechanisms

	Compromise Recovery	System Administration	Training	OPSEC	Trusted Distribution	Secure Operations	Mechanism Management
SML1	informal plan	see[NSF98] for non-technical countermeasures	training available at user discretion	implement OPSEC at user's discretion	direct vendor purchase	informal plan of operation	procedural, user's discretion
SML2	detailed plan that is reviewed and approved	see[NSF98] for non-technical countermeasures	formal training plan	OPSEC training required, implement at user's discretion	certificate of authenticity, virus scan, validation	formal plan of operation	procedural, reminders, user's discretion
SML3	detailed plan that is reviewed and approved	see[NSF98] for non-technical countermeasures	Knowledge/skill certification required	OPSEC training required, implementation required	protective packaging, checksums, validation suite	detailed, formal plan of operation	automated support

4.2 Mechanisms Supporting Confidentiality

Confidentiality is the protection of information against disclosure to unauthorized entities or processes. Possible security mechanisms for this security service are depicted in Table 4-2 and can be obtained by single columns that are listed or by a combination of these columns:

Table 4-2 Confidentiality Mechanisms

	Cryptographic Algorithm		Physical Security	Technical Security		Anonymity	
	Effective Key Length	Key Management		Anti-Tamper	TEMPEST	TRANSEC	Cover & Deception
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length	comparable to [5200.1-R]	[FIPS140] level 1 or 2	comply with applicable EMI/EMC FCC standards or portions of [NT1/92]	low power unit	TBD
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length,160+ hash key length	comparable to [5200.1-R]	[FIPS140] level 3 or 4	[NT1/92]	commercial spread spectrum signal techniques	TBD

	Cryptographic Algorithm		Physical Security	Technical Security		Anonymity	
	Effective Key Length	Key Management		Anti-Tamper	TEMPEST	TRANSEC	Cover & Deception
SML3	Due to the complicated nature of this level, please consult with an NSA ISSE.	SMI Cat Z of [NSF98], also consult with an NSA ISSE.	comparable to [5200.1-R]	[FIPS140] level 4 or better	[NT1/92]	cryptographic spread spectrum signal techniques	TBD

- If ***Cryptographic Algorithm*** is chosen, the management of keying material needs to be considered along with the effective length of the key, which includes the strength of the underlying cryptographic algorithm. Effective length is defined as the nominal key length reduced by the effect of any attacks that are published (known) about that cryptographic algorithm (assuming correct implementation). The supporting Key Management Security Management Infrastructure (SMI) Categories are defined in the Security Management Infrastructure Chapter of the NSF.
- ***Physical Security*** includes the tangible security mechanisms such as guards, locks, and fences. The idea is to build a physically secure enclave, providing guards and high walls.
- ***Technical Security*** is a protection mechanism for hardware. Tampering is the unauthorized modification that alters the proper functioning of an information security device or system in a manner that degrades the security or functionality it provides. Anti-Tamper mechanisms detect such alterations. TEMPEST is the investigation, study, and control of compromising emanations from telecommunications and Automated Information System (AIS) equipment.
- ***Anonymity*** is the desire for a user to remain unknown during a virtual transaction. Some applications might be Internet voting and Internet cash. This area is relatively immature and is currently addressed by the TRANSEC and Cover & Deception disciplines. TRANSEC mechanisms provide various degrees of covertness to avoid detection, identification and exploitation. Cover can be provided through mechanisms such as anonymous remailers, "onion routing" or "web anonymizers", and currently have no differentiated levels.

4.3 Mechanisms Supporting Integrity

In Table 4-3 we have four mechanisms that will help in obtaining integrity either singly or in combination with others. When taken in the context used here, *integrity*, as a security service, means the protection of information against undetected, unauthorized modification, or undetected destruction of information.

Table 4-3 Integrity Mechanisms

	Cryptographic Algorithm		Physical Security	Signature Checksum	Redundancy
	Effective Key Length	Key Management			
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat. X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length	comparable to [5200.1-R]	parity, or commercial checksum, hash and, signature with SML1 algorithm	not applicable
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length, 160+ hash key length	comparable to [5200.1-R]	cryptographic checksum, hash, and signature with SML2 algorithm	redundant data path with 100% correct comparison
SML3	Due to the complicated nature of this level, please consult with an NSA ISSE.	SMI Cat Z of [NSF98], also consult with an NSA ISSE.	comparable to [5200.1-R]	cryptographic checksum, hash and signature with SML3 algorithm	multiple data paths with 100% correct comparison

- A ***Cryptographic Algorithm***, in an error extension mode, will emphasize the error and should be used in conjunction with a detection mechanism (e.g., parity or human review).
- ***Physical Security*** is described under Confidentiality (4.2) above.
- ***Signature/Checksum*** provides data integrity by digitally signing data. Typically, the data requiring protection is used to calculate a smaller value such as a parity, checksum or hash. This value can then be digitally signed.

- ***Redundancy*** is the availability of multiple methods to obtain the same information.

4.4 Mechanisms Supporting Availability

Availability is also known as service assurance. In order to ensure availability of data, the system must employ both preventative as well as recovery mechanisms. This security service is quantified in Table 4-4 and can be obtained by a combination of the services as appropriate for the applications.

- ***TRANSEC*** is used to overpower potential jammers. A strong enough signal is provided for this anti-jam capability. TRANSEC can also be used to hide a signal to avoid jamming. Note: Because of the real time nature of exploitation, it may not be necessary to use an SML3 algorithm strength to meet the SML3 level for this mechanism.
- ***Anti-Tamper*** is described under Confidentiality (4.2) above.
- ***Physical Security*** is described under Confidentiality (4.2) above.
- ***Redundancy*** or Redundant paths should be available so as to allow information flow without violating the site security policy. This might include bypassing any problem areas, including congested servers, hubs, cryptography, etc.
- ***Data Recovery*** is the ability to recover data that may otherwise be unavailable due to the loss of key, storage media, etc.

Table 4-4 Availability Mechanisms

	TRANSEC	Anti-Tamper	Physical Security	Redundancy	Data Recovery
SML1	high power	[FIPS140] level 1 or 2	comparable to [5200.1-R]	bypass channel available	informal archival plan, user backs up own key or data
SML2	commercial spread spectrum signal techniques	[FIPS140] level 3 or 4	comparable to [5200.1-R]	backup data path, hot spare	formal archival plan, central back- ups
SML3	Cryptographic spread spectrum signal techniques	[FIPS140] level 4 or better	comparable to [5200.1-R]	multiple data paths, multiple hot spares	formal archival plan, central, offsite back-ups

4.5 Mechanisms Supporting Identification and Authentication (I&A)

Identification and Authentication is one aspect of Access Control (as, ultimately, all security services are). There usually is a need for a process that enables recognition of an entity within, or by, an AIS. Along with that, a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information is needed. These are the attributes of Identification and Authentication that are listed in Table 4-5. We categorize these attributes as follows:

- ***Identification*** or System Identification (SID) in particular is one way a system might recognize the "entity" (which may be a person). Biometrics might be used to ID a living person.

Table 4-5 Identification and Authentication Mechanisms

	Identification		Human to Machine Authentication		Peer to Peer Authentication			
	System IDs (SIDs)	Biometrics	Passwords Pins Challenge/ Response	Tokens	Certificates	Cryptographic Algorithm		Personnel Security
						Effective Key Length	Key Management	
SML1	Uniqueness	not applicable	have one	badge/key static	bind w/SML1 cryptographic algorithm	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat. X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length	commercial hiring practices
SML2	uniqueness and minimum character length	use one Biometric	minimum effective length – TBD	memory device, updated periodically	bind w/SML2 cryptographic algorithm	80+ bits symmetric key length, 160+ exponent 1024+ modulus public	SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length, 160+ hash	equivalent of SECRET clearance

	Identification		Human to Machine Authentication		Peer to Peer Authentication			
	System IDs (SIDs)	Biometrics	Passwords Pins Challenge/ Response	Tokens	Certificates	Cryptographic Algorithm		Personnel Security
						key length	key length	
SML3	uniqueness, minimum character length, minimum distance (e.g., Hamming)	use one Biometric with a liveness test	minimum effective length - TBD	CIK, updated every time	bind w/SML3 cryptographic algorithm	Due to the complicated nature of this level, please consult with an NSA ISSE.	SMI Cat Z of [NSF98], also consult with an NSA ISSE.	equivalent of TOP SECRET clearance

- ***Human to Machine Authentication*** could be alphanumeric phrases, like passwords, PINs or challenge/response exchanges that are memorized by a human or used with a token calculator (e.g. challenge/response). Also, physical devices such as hardware tokens have this utility (e.g., a credit card type physical entity).
- ***Peer to Peer Authentication*** can be certificates that identifies and authenticates the "entity". Along with that certificate is the similar SML cryptographic algorithm that "binds" it to the entity with a digital signature. Authentication is obtained by a different party (a separate, but knowledgeable entity) and given to another. Within this area there could exist a cryptographic algorithm (as discussed under Confidentiality above), and Personnel Security, where a security clearance is obtained for a particular person to reduce the risk of an insider attacking the system.

4.6 Mechanisms Supporting Access Control

Beyond I&A, Access Control can be thought of as the "super service" encompassing all security services. In the context of network security, access control is concerned with limiting access to networked resources (hardware and software) and data (stored and communicated). The primary goal here is to prevent unauthorized use, and unauthorized disclosure or modification of data by unauthorized entities. A secondary goal is to prevent an Availability or Denial of Service attack. Several mechanisms that can be used to help provide the Access Control service are shown in Table 4-6, and include the following parameters:

- ***Anti-Tamper*** is described under Confidentiality (4.2).
- ***Mandatory Access Control (MAC)*** is where authorized access to data is automatically imposed by the system through the use of labels, and binding the labels to the data associated with it. When implementing MAC there is a concern with both the integrity of the label itself, and the strength of binding of the label to the data. In other words, if SML2 is required for MAC, the integrity of the label must also be provided with SML2, and the function (possibly a cryptographic algorithm) binding the label to the data must also be SML2. Other implementation concerns include making the labeling non-bypassable and fail-safe.
- ***Discretionary Access Control (DAC)*** is different from MAC in that the owner of the data to be accessed (versus the machine) can choose who can and cannot be authorized access to the data. For SML1, this is comparable to setting Unix permission bits (owner/group/world) to grant access. For SML2 & 3, using access control lists (ACLs) further refines the mechanism. ACLs can be more specific to allow certain identities access to information (e.g. specific users within a group can be granted access). Again DAC mechanisms should be non-bypassable (only "changeable" by the owner of the data), fail-safe, and possess the same SML level of integrity associated with the level of DAC required.
- ***Certificates*** are described under I&A (4.5).
- ***Personnel Security*** is described under I&A (4.5).

Table 4-7 Access Control Mechanisms

	Anti-Tamper	Mandatory Access Control	Discretionary Access Control	Certificates	Personnel Security
SML1	[FIPS140] level 1 or 2	not applicable	comparable to Unix permission bits	bind w/SML1 cryptographic algorithm	commercial hiring practices
SML2	[FIPS140] level 3 or 4	labels bound to data having integrity and binding function	access control lists (ACLs)	bind w/SML2 cryptographic algorithm	equivalent of SECRET

	Anti-Tamper	Mandatory Access Control	Discretionary Access Control	Certificates	Personnel Security
		both at the SML2 level			clearance
SML3	[FIPS140] level 4 or better	labels bound to data having integrity and binding function both at the SML3 level	access control lists (ACLs)	bind w/SML3 cryptographic algorithm	equivalent of TOP SECRET clearance

4.7 Mechanisms Supporting Accountability

Accountability can be considered a special case of non-repudiation. The accountability security service is basically holding any entity on a network responsible for its actions on that network. Mechanisms, which can be used to provide the security service of accountability, are shown in Table 4-7, and discussed below:

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

  These should be considered for each SML level, and in SML2 and 3, be detailed in a plan. Of course, as with all mechanisms, consideration should be given to non-circumvention or "non-bypassability", and the effects of failure.
- ***Intrusion Detection*** is still in relative infancy. Intrusion detection is that mechanism which monitors a network and detects either 1) known attacks being mounted against the system or 2) differences in a profiled use of the system. An intrusion detection mechanism has several aspects associated with it. These include whether it is static ([SML1] set up to filter only on known attacks and profiles), dynamic ([SML2] set up to filter on known attacks and profiles, but updateable perhaps through software downloads), or dynamically adaptable ([SML3] this adds the aspect of "artificial intelligence" where the system learns new profiles based on usage). Also, depending on the SML level, a reaction mechanism to a detected intrusion must be either informally (SML1) or formally (SML2 & 3) detailed and implemented.
- ***I&A*** is described under I&A (4.5).

Table 4-7 Accountability Mechanisms

	Audit	Intrusion Detection	Identification and Authentication
SML1	informal reaction mechanism	static system with informal reaction mechanism	see I&A table for SML1
SML2	formal reaction plan and strategy	dynamic system with formal reaction mechanism	see I&A table for SML2
SML3	formal reaction plan and strategy	dynamic, adaptive system with formal reaction mechanism	see I&A table for SML3

4.8 Mechanisms Supporting Non-Repudiation

The security service of non-repudiation provides a method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny processing the data. It is quantified in Table 4-8 and can be obtained by a combination of these mechanisms as appropriate for the applications:

- ***Signature*** is used to digitally sign data in such a way that only the sender and receiver could have respectively sent and received the message. The sender signs the original data to prove he sent it. The receiver signs a receipt to prove he received the original data. Validation of these signatures is always required.
- ***Trusted Third Party*** is used to prearrange a method by which a third party may receive the information from the sender and transmit/send it to the receiver in a way that ensures sender and receiver are confident that they are communicating with the correct party.
- ***Accountability*** is described under Accountability (4.7).
- ***I&A*** is described under the I&A (4.5).
- ***Archive*** is the ability to store data so that it can be recovered if necessary.

Table 4-8 Non-Repudiation Mechanisms

	Signature	Trusted Third Party	Accountability	Identification & Authentication	Archive
SML1	sign with SML1 cryptographic algorithm	see I&A Table forSML1 Personnel Security	see Accountability table for SML1	see I&A table for SML1	informal archival plan, user backs up own key or data
SML2	sign with SML2 cryptographic algorithm	see I&A Table forSML2 Personnel Security	see Accountability table for SML2	see I&A table for SML2	formal archival plan, central back- ups
SML3	sign with SML3 cryptographic algorithm	see I&A Table forSML3 Personnel Security	see Accountability table for SML3	see I&A table for SML3	formal archival plan, central, offsite back-ups

5.0 LEVEL OF ASSURANCE

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

Assurance is the measure of confidence in claims made; that the security features and architecture of an automated information system appropriately mediate access and enforce the security policy. The assurance measures referred to in this paper are from the Common Criteria [CC98].

In addition to those addressed in the Common Criteria, there are other assurance tasks that the Common Criteria doesn't discuss. These include Failure Analysis and Test, TEMPEST Analysis and Test, and TAMPER Analysis and Test, among others. If these apply to a particular product or system, then they should be added to the requirements of the appropriate Evaluation Assurance Levels.

6.0 GLOSSARY

Customer: See user.

Effective Key Length: A measure of strength of a cryptographic algorithm, regardless of actual key length.

Interagency OPSEC Support Staff (IOSS): 6411 Ivy Lane, Suite 400, Greenbelt, MD, (301) 982-0323.

Information Systems Security Engineer (ISSE): The ISSE performs the science and art of discovering customer INFOSEC needs, defining, designing, and implementing (with economy and elegance) system solutions that satisfy those needs, safely resisting the forces to which the information systems may be subjected.

[Security] Robustness: A characterization of a security function, mechanism, service, or solution, reflecting whether it is adequately strong or "good enough" to provide the desired information protection (as contrasted with how "good" the function, etc., is).

Security Policy: What security means to the user a statement of what is meant when claims of security are made. More formally, it is the set of rules and conditions governing the access and use of information. Typically, a security policy will refer to the convential security services, such as confidentiality, integrity, availability, etc., and perhaps their underlying mechanisms and functions.

User: The party responsible (or his designee) for the security of the information. The user works closely with the ISSE. Also referred to as the customer.

7.0 REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, CCEB-96/013, Version 1.00, 96/01/31

[4009] NSTISSI No. 4009, National INFOSEC Glossary

[5200.1-R] DoD Reg 5200.1-R, Information Security Program, 1997.

[CC98] Common Criteria for Information Technology Security Evaluation, CCIB-98 (ISO/IEC 15408), Version 2.0, 1998, http://csrc.nist.gov/cc/.

[FIPS140] FIPS PUB 140-1, National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, http://www.itl.nist.gov/div897/pubs/fip140-1.htm.

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

[ISSEH] Information Systems Security Engineering Handbook, Release 1.0, 1994.

[ISSPG] Information System Security Policy Guideline (I942-TR-003, 1994).

[LAING] Laing, Alan, “DoD PKI Level of Protection and The Appropriateness of Proposed Solutions for Various Applications”, 1998, DRAFT.

[NCSC88] National Computer Security Center, Glossary of Computer Security Terms, (NCSC-TG-004-88, 1988).

[NSA120] NSA/CSS Dir. No. 120-1, NSA/CSS Operations Security Program, 1990.

[NSF98] National Security Agency, Network Security Framework, Release 1, 1998,http://www.nsff.org/.

[NT1/92] NSTISSAM TEMPEST/1-92, Compromising Emanations Laboratory Test Requirements, Electromagnetics, 1992.

[SMI96] SMI Task 1 Team, Threat and Vulnerability Model for Information Security, 1997.

[UIC] National Security Agency Specification for Unified INFOSEC Criteria, 1991.

[FORD] Warwick Ford, *Computer Communications Security,* Prentice Hall PTR, Englewood Cliffs, NJ, 07632, 1994.

Network Security Framework: Robustness Strategy

Teri Arber
Deb Cooley
Steve Hirsch
Martha Mahan
Jim Osterritter

Context

- ✓ Information Assurance Technical Framework (IATF)
- ✓ Definition of Robustness
- ✓ Defense in Depth
  - ➔ Layered Security
- ✓ Defense Information Assurance Program
  - ➔ Information Assurance Solutions (IAS)

Purpose

- ✓ A strategy to:
  - ➔ Provide guidance
  - ➔ Aid in defining solution requirements
  - ➔ Aid in risk management
  - ➔ Stimulate research
- ✓ Can be used for:
  - ➔ Component parts
  - ➔ Configured systems

Assumptions

- ✓ Trained Information System Security Engineer (ISSE) is available
- ✓ The Security Policy is known
- ✓ More than one acceptable solution
- ✓ There will be countermeasure evolution

General Process

- ✓ Determine the Value of Information and Threat Environment
- ✓ Determine the Degree of Robustness
- ✓ Select Security Services
- ✓ Select Security Mechanisms
- ✓ Assess Residual Risk

Information Value

- ✓ Define levels of Information Value by the consequences of violating policy:
  - ➔ V1: Negligible adverse effects
  - ➔ V2: Minimal damage
  - ➔ V3: Some damage
  - ➔ V4: Serious damage
  - ➔ V5: Exceptionally grave damage

Threat Environment

- ✓ Define levels of Threat Environment:
  - ➔ T1: Inadvertent or accidental
  - ➔ T2: Casual adversary, minimal resources, little risk
  - ➔ T3: Adversary, minimal resources, significant risk
  - ➔ T4: Sophisticated, moderate resources, little risk
  - ➔ T5: Sophisticated, moderate resources, significant risk
  - ➔ T6: Very sophisticated, abundant resources, little risk
  - ➔ T7: Very sophisticated, abundant resources, significant risk

Degree of Robustness

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

Strength of Mechanism

- ✓ Series of tables by Security Service
- ✓ Levels of Strength
  - ➔ SML1: Basic strength (third from highest)
  - ➔ SML2: Medium strength (second from highest)
  - ➔ SML3: High strength (highest)

Security Services

- ✓ Security Management
- ✓ Confidentiality
- ✓ Integrity
- ✓ Availability
- ✓ Identification and Authentication
- ✓ Access Control
- ✓ Accountability
- ✓ Non-Repudiation

Level of Assurance

- ✓ Utilize the Common Criteria for security assurance
- ✓ Additions might include
  - ➔ Failsafe design and analysis
  - ➔ Anti-Tamper design and analysis
  - ➔ TEMPEST design and analysis
  - ➔ Process Assurance (SSE-CMM)

Summary

- ✓ This strategy is not a ‘cookbook’
- ✓ It does provide guidance
- ✓ It is a starting point

For More Information

- ✓ Robustness Strategy Team
  - ➔ Teri Arber - tarber@radium.ncsc.mil
  - ➔ Deb Cooley - dcooley@radium.ncsc.mil
  - ➔ Steve Hirsch - sjhirsc@aztech.ba.md.us
  - ➔ Martha Mahan - mmm@suslol.demon.co.uk
  - ➔ Jim Osterritter - josterri@radium.ncsc.mil
- ✓ Network Security Framework
  - ➔ http://www.nsff.org/

Security Management Mechanisms

	Compromise Recovery	System Administration	Training	OPSEC	Trusted Distribution	Secure Operations	Mechanism Management
SML1	Informal plan	See NSF98 for non-technical countermeasures	Training available at user discretion	Implement at user's discretion	Direct vendor purchase	Informal plan of operation	Procedual, user's discretion
SML2	Detailed plan that is reviewed and approved	See NSF98 for non-technical countermeasures	Formal training plan	Training required, implement at user's discretion	Certificate of authenticity, virus scan, validation	Formal plan of operation	Procedural, reminders, user's discretion
SML3	Detailed plan that is reviewed and approved	See NSF98 for non-technical countermeasures	Knowledge/ skill certification required	Training required, implemen-tation required	Protective packaging, checksums, validation suite	Detailed, formal plan of operation	Automated support

Confidentiality Mechanisms

	Cryptographic Algorithm		Physical Security	Technical Security		Anonymity	
	Effective Key Length	**Key Management**		**Anti-Tamper**	**TEMPEST**	**TRANSEC**	**Cover & Deception**
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length	compa-rable to [5200.1-R]	[FIP140] level 1 or 2	comply with applicable EMI/EMC FCC standards or portions of [NT1/92]	low power unit	TBD
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length, 160+ hash key length	compa-rable to [5200.1-R]	[FIP140] level 3 or 4	[NT1/92]	commercial spread spectrum signal techniques	TBD
SML3	Due to the complicated nature of this level, please consult with a NSA ISSE.	SMI Cat Z of [NSF98], also consult with a NSA ISSE.	compa-rable to [5200.1-R]	[FIP140] level 4 or better	[NT1/92]	cryptographic spread spectrum signal techniques	TBD

Integrity Mechanisms

	Cryptographic Algorithm		Physical Security	Signature Checksum	Redundancy
	Effective Key Length	**Key Management**			
SML1	40+ bits symmetric key length, 80+ exponent 512+ modulus public key length	SMI Cat. X of [NSF98], 80+ exponent 512+ modulus public key length, 80+ hash key length	comparable to [5200.1-R]	parity, or commercial checksum, hash and, signature with SML1 algorithm	not applicable
SML2	80+ bits symmetric key length, 160+ exponent 1024+ modulus public key length	SMI Cat Y of [NSF98], 160+ exponent 1024+ modulus public key length, 160+ hash key length	comparable to [5200.1-R]	cryptographic checksum, hash, and signature with SML2 algorithm	redundant data path with 100% correct comparison
SML3	Due to the complicated nature of this level, please consult with an NSA ISSE.	SMI Cat Z of [NSF98], also consult with an NSA ISSE.	comparable to [5200.1-R]	cryptographic checksum, hash and signature with SML3 algorithm	multiple data paths with 100% correct comparison

Availability Mechanisms

	TRANSEC	Anti-Tamper	Physical Security	Redundancy	Data Recovery
SML1	high power	[FIPS140] level 1 or 2	comparable to [5200.1-R]	bypass channel available	informal archival plan, user backs up own key or data
SML2	commercial spread spectrum signal techniques	[FIPS140] level 3 or 4	comparable to [5200.1-R]	backup data path, hot spare	formal archival plan, central back-ups
SML3	Cryptographic spread spectrum signal techniques	[FIPS140] level 4 or better	comparable to [5200.1-R]	multiple data paths, multiple hot spares	formal archival plan, central, offsite back-ups

I&A Mechanisms

	System IDs (SIDs)	Biomet-rics	Passwords PINs Challenge/ Response	Tokens	Certificates	Crypto-graphic Algorithm	Personnel Security
SML 1	uniqueness	not applicable	have one	badge/key static	bind w/SML1 cryptographic algorithm	See Confidenti-ality Mechanisms	commercial hiring practices
SML 2	uniqueness and minimum character length	use one Biometric	minimum effective length – TBD	memory device, updated periodi-cally	bind w/SML2 cryptographic algorithm		equivalent of SECRET clearance
SML 3	uniquness, minimum character length, minimum distance(e.g., Hamming)	use one Biometric with a liveness test	minimum effective length - TBD	CIK, updated every time	bind w/SML3 cryptographic algorithm		equivalent of TOP SECRET clearance

Access Control Mechanisms

	Anti-Tamper	Mandatory Access Control	Discretionary Access Control	Certificates	Personnel Security
SML1	[FIPS140] level 1 or 2	not applicable	comparable to Unix permission bits	bind w/SML1 cryptographic algorithm	commercial hiring practices
SML2	[FIPS140] level 3 or 4	labels bound to data having integrity and binding function both at the SML2 level	access control lists (ACLs)	bind w/SML2 cryptographic algorithm	equivalent of SECRET clearance
SML3	[FIPS140] level 4 or better	labels bound to data having integrity and binding function both at the SML3 level	access control lists (ACLs)	bind w/SML3 cryptographic algorithm	equivalent of TOP SECRET clearance

Accountability Mechanisms

	Audit	Intrusion Detection	Identification and Authentication
SML1	informal reaction mechanism	static system with informal reaction mechanism	see I&A table for SML1
SML2	formal reaction plan and strategy	dynamic system with formal reaction mechanism	see I&A table for SML2
SML3	formal reaction plan and strategy	dynamic, adaptive system with formal reaction mechanism	see I&A table for SML3

Non-Repudiation Mechanisms

	Signature	Trusted Third Party	Accountability	I&A	Archive
SML1	sign with SML1 cryptographic algorithm	see I&A Table for SML1 Per-sonnel Security	see Accountability table for SML1	see I&A table for SML1	informal archival plan, user backs up own key or data
SML2	sign with SML2 cryptographic algorithm	see I&A Table for SML2 Per-sonnel Security	see Accountability table for SML2	see I&A table for SML2	formal archival plan, central back- ups
SML3	sign with SML3 cryptographic algorithm	see I&A Table for SML3 Per-sonnel Security	see Accountability table for SML3	see I&A table for SML3	formal archival plan, central, offsite back-ups