Discussion of Standards, Metrics and Models for SwA

NDIA Summit on Software Assurance – EID Break-out Workshop

September 7-8, 2005

Arlington, VA

Ken Hong Fong
Chuck Johnson
OUSD(AT&L), Defense Systems
Systems Engineering/Enterprise Development
ekenneth.hongfong@osd.mil; (703) 695-0472
chuck.johnson.ctr@osd.mil; (703) 602-0851 X123

Mitch Komaroff
OASD(NII) ODCIO
mitchell.komaroff@osd.mil
703-602-0980 x146

Notional SwA Artifact Attributes

Artifact Attributes	Description	Metric (1-5)
Functionality	Applications and services achieve intended functionality absent unintended behaviors	
Computing Resource Separation	All application and data processes operate in their own memory space and are not vulnerable to buffer and processing memory overflow, unintended data and instruction code interaction or data and code corruption	
Error and Exception	No predictable errors or exceptions are left unhandled.	
Discrete Functionality	Code objects and modules implement minimal discrete functionality per object/module with no unnecessary functionality	
Hardware isolation	High level language source code implementation is absent of machine level functionality	
Code Transparency	Critical code functionally and behaviorally transparent.	
Requirements & Risk Management	Software Assurance Requirements are established as identified in a formal risk and vulnerability analysis process	
Hierarchical Conformance	At the highest level, i.e., 5, resists control or subversion from external forces, and at lower levels complies with established control regimens of higher level devices	
Networking and Integration Risk Management	Software function not corrupted by unintended interaction across network and integrated system boundaries.	

Notional SwA Process Attributes

Process Attributes	Description	Metric (1-5)
SwA IA	A mature, well understood, standards based process in use in the program for validating conformance with defined Software Assurance requirements and measures. An example might be conformance to a "SwA tuned" CC Protection Profile for the Target of Evaluation's component type and function. A reference model might be similar to NIAP Validated Protection Profiles.	E.g., an EAL level commensurate with a required (notional) SwA criticality level (TBD)
Developer Quality	A defined range of developer control activities in place and validated at a level commensurate with the defined SwA threshold. E.g., a notional "SwA level 3" may map to a minimum required CMM/I level 4 ("Quantitatively Managed"	E.g., CMMI levels mapped to (notional) SwA criticality level
Supplier Integrity and Transparency	A defined Supplier Assurance Level is assigned as threshold commensurate with the defined SwA criticality level	E.g., SAL threshold mapped to (notional) SwA criticality level
Required Technical Maturity Levels	A defined level of desired technical maturity is required for components designated "critical"	E.g., TRL threshold at Level 7 for "critical" components
SE process maturity	A mature, well formed, understandable SE plan has been prepared and accepted that fully accounts for SwA capabilities in an ISSE context	E.g., a SEP has been submitted, reviewed, and accepted by MDA rep for SwA considerations

Notional SwA Target Levels

Assurance Attributes	Description	Example
Level 5	Product has been designed and developed to not only meet functional objectives but also meet specific security and assurance targets, and was developed under controlled conditions, by trusted agents. When called for, this product can control lower assured products in its hierarchical functional chain, and is safe from corruption and influence from external forces	Type 1 Crypto logical devices, High-Low Network Guards
Level 4	A commercial Level 3 product that has been augmented with specially designed and trusted components or ancillary devices to increase the assurance that the underlying component is both controlled and less vulnerable from fragile design or latent defects	An Iridium Satcom phone with the NSA approved security sleeve, a NIPR Guard based upon commercial software operated on a secure OS kernel
Level 3	A fielded commercial product that is designed and developed in accordance with basic security tenets, conforms to normative rules of partitioning and behavior, and has been developed by U.S. vendors with control and transparency of origin	Microsoft XP OS
Level 2	A commercial product that has been developed or influenced by foreign vendors or workers but is otherwise a Level 3 device	SAP
Level 1	A product of undeterminable source, design or pedigree	Shareware

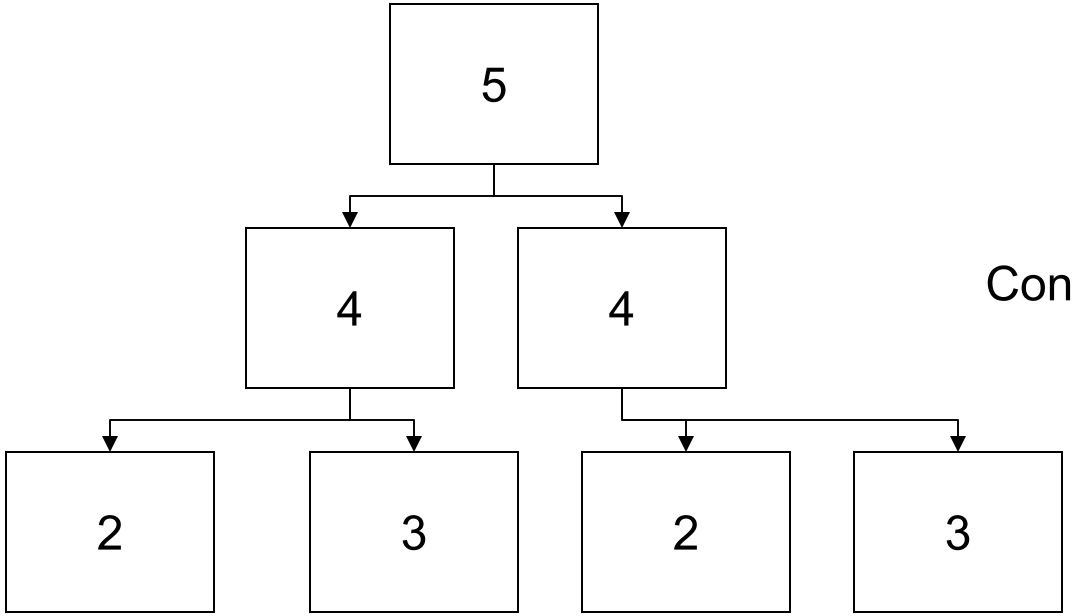
Notional Sensitivity Analysis Measures

Failure Modes for Sensitivity Analysis	Impact of Failure	Example
Level 5	**Component has been subverted and is actively working against the capability**	**Inappropriate data transmission**
Level 4	**Component demonstrates some malicious behavior**	**Propagates worms and viruses**
Level 3	**The component affects other parts of the systems through poor behavior, partial or unpredictable functional failure**	**Data or network flooding with intent to deny**
Level 2	**The device fails completely**	**Locks in off position**
Level 1	**The device performs in a degraded mode, but otherwise does not affect the system**	**Non-essential features fail but main functions continue**

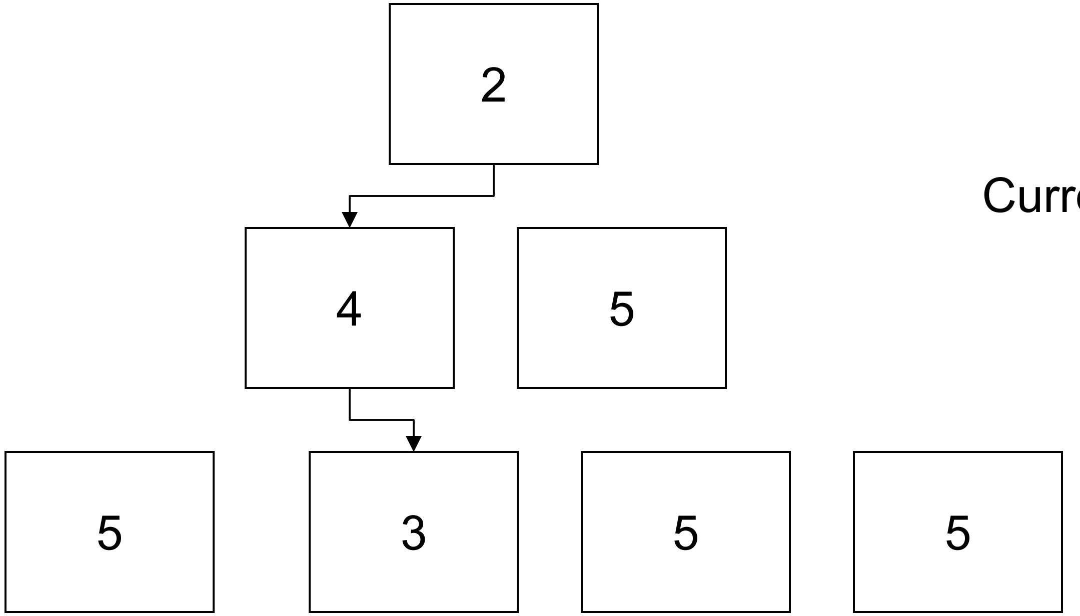
Notional SwA Cumulative Measures

Cumulative Assurance Attributes	Artifact Assurance levels	Process Assurance levels*
Level 5	5	5
Level 4	3	4
Level 3	3	3
Level 2	3	2
Level 1	1	1

* Score resulting from a formula TBD defined by system attributes TBD that combine process attributes



Conceptual



Current

NIAP Validated Protection Profiles

http://niap.nist.gov/cc-scheme/pp/index.html

Anti-Virus	Key Recovery PP	Public Key Infrastructure/ Key Management Infrastructure PP	Switches and Routers PP
Biometrics PP PP	Miscellaneous PP PP	Remote Access PP	System Access Control
Certificate Management PP	Mobile Code PP	Secure Messaging PP	Database Management System PP
Firewalls PP	Multiple Domain Solutions PP	Security Management	Virtual Private Network PP
Guards PP	Network Mgmt	Sensitive Data Protection	Wirelss Local Area Network PP
Intrusion Detection System / Intrusion Prevention System PP	Operating System PP	Single-Level Web Server PP	
	Peripheral Switch PP	Smart Cards PP	

Notes:

PP = There is a ***Validated U.S. Gov't PP*** available for this technology category of product type. However, it should not be inferred that every product listed within this technology category necessarily meets the PP. You can be redirected to the PP page for the given technology by clicking on the red or black PP icon.

PP = There is a ***draft U.S. Gov't PP*** available for this category of product type. However, it should not be inferred that every product listed within this product type necessarily meets the PP. Draft PPs can be invarious stages of development, i.e., being written or vetted, or in evaluation in a NIAP CCEVS CCTL. You can be redirected to the PP page for the given technology by clicking on the red or black PP icon.

PP **= There is a *Validated non-U.S. Gov't PP*** available for this technology category.

CC EAL Levels

EAL1: Functionally Tested	EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious [...] including independent testing against a specification, and an examination of the guidance documentation provided. [...] An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.
EAL2: Structurally Tested	EAL2 requires the cooperation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time [...] applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.[..].
EAL3: Methodically Tested and Checked	EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.
EAL4: Methodically Designed, Tested and Reviewed	EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line. EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to
EAL5: Semiformally Designed and Tested	EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, will not be large. EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security
EAL6: Semiformally Verified Design and Tested	EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks. EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.
EAL7: Formally Verified Design and Tested	EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.
Source: http://en.wikipedia.org/wiki/Evaluation_Assurance_Level	

CMM maturity Levels

Source: http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02tr012.pdf

Maturity Level	Staged Representation Maturity Levels
1	Initial
2	Managed
3	Defined
4	Quantitatively Managed
5	Optimizing

The **Capability Maturity Model** (CMM) is a method for evaluating and measuring the maturity of the software development process of organizations on a scale of 1 to 5. The CMM was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University in Pittsburgh. It has been used extensively for avionics software and for government projects since it was created in the mid-1980s. The Software Engineering Institute has subsequently released a revised version known as the **Capability Maturity Model Integration** (CMMI).

The purpose of CMM Integration is to provide guidance for improving [an] organization's processes and [its] ability to manage the development, acquisition, and maintenance of products or services. (Source: http://en.wikipedia.org/wiki/CMMI)

Technology Readiness Levels

Source: http://en.wikipedia.org/wiki/Technology_Readiness_Level

Technology Readiness Level	Description
1. Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins with to be translated into applied research and development. Example might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. The application is speculative and there is no proof or detailed analysis to support the assumption. Examples are still limited to paper studies.
3. Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that the pieces will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of 'ad hoc' hardware in a laboratory.
5. Component and/or breadboard validation in relevant environment	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include 'high fidelity' laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is well beyond the breadboard tested for TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high fidelity laboratory environment or in simulated operational environment.
7. System prototype demonstration in a operational environment	Prototype near or at planned operational system. Represents a major step up from TRL 6, requiring the demonstration of an actual system prototype in an operational environment, such as in an aircraft, vehicle or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and 'flight qualified' through test and demonstration	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system 'flight proven' through successful mission operations	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. In almost all cases, this is the end of the last "bug fixing" aspects of true system development. Examples include using the system under operational mission conditions.