Metricon 5.5

Verification versus Validation

Jennifer Bayuk
Cybersecurity Program Director
School of Systems and Enterprises
jennifer.bayuk@stevens.edu
Systems Thinking

The Vee Model

Advantages of the Engineering Approach

1. Manage Complexity
2. Top-down requirements tracing
3. Black box modeling
4. Logical flow analysis
5. Documentation
6. Peer Review
7. Detailed Communication

Traditional Requirements Process

1. Functional

2. Interface

2. System-wide – “ilities”

3. System-wide – “ilities”

Focus on systems security engineering is required to know when it should be placed here.

Security vulnerabilities are frequently introduced here.

Systems engineering literature traditionally places security here.

Source: Buede, The engineering design of systems, models and methods, Wiley, 2009
Today’s Security Requirements
...a charitable interpretation...

Functional – What is necessary for mission assurance?

Nonfunctional – What is necessary for system survival? What is necessary to anticipate changing threat environments?

V and V - What is necessary to ensure requirements are met?

Must include security requirements to support:
   System Mission and Purpose
   System Lifecycle Maintenance

Should address:
   Adaptability, flexibility, agility, redundancy, robustness, scalability….
Verification: Did we build the system right?

Validation: Was the right system built?

Also known as:

Correctness – *Do the security features work?*

Effectiveness – *Is the system secure?*
Systems Engineering Verification Activity

- Identify Verification and Validation Targets
- Define Verification and Validation Approach
- Perform Verification
- Perform Validation
- Provide Verification and Validation Results

Source: ISO 28127
A New Security Approach

• Clear problem statements
• Thorough problem background description including a full literature review
• Clearly defined solution criteria
• Proposed hypothesis formulated to shed light on a solution and how it may be proven or disproven
• Summary of contributions to field and a statement of next steps
A Systematic Look at Security

Security: Something that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.

Security Feature: A system capability that contributes to its security.

Security Metric: Measurement that characterizes an attribute of the system of interest that is proposed to have both face and construct validity in the context of a hypothesis that the system is secure.

Security Framework: The concept of operations, mission, and environment under which a system operates.
Frameworks

- Patterns at system level
- Security is identified with resiliency of mission
- Systemic security features are functional requirements
- Architecture security metrics verify and validate functional requirements

Example: Pipelined monitors

Possible Functional Security Metrics:

- sensor signal-to-noise ratios
- data integrity cross-platform checks
- the type and number of information delivery alternatives available to the end user/operator

New Security Methodology

Devise System Security Engineering MPTs

Devise Security Metrics

Design Secure Architecture

Extract Security Frameworks

Define Security
Common Indexes cannot be expected to exist in different realms and different management domains.
Expectations for linkage must be articulated.

Source: Bayuk, ISACA Training 2009
## Example System Security Verification Processes

<table>
<thead>
<tr>
<th></th>
<th>Input/Output</th>
<th>Configuration Compliance</th>
<th>Peer Review</th>
<th>Completion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Testing</strong></td>
<td>Continuous monitoring</td>
<td>Change control verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Analysis</strong></td>
<td></td>
<td>Automated configuration checking</td>
<td>Segregation of oversight duties</td>
<td>Process metrics</td>
</tr>
<tr>
<td><strong>Inspection</strong></td>
<td>Quality Control</td>
<td>Audit and Assessment</td>
<td>Red/Blue Teams</td>
<td></td>
</tr>
</tbody>
</table>
Presentation Techniques

Facilitates comparison between different types of technology, business units, etc, often used for audit remediation.

Total patched or otherwise automatically verified to be secured via specific tools.

Source: Bayuk, Metricon 3.5, 2008
Validation Criteria

- content validity
- face validity
- criterion validity
- construct validity
Validation

Source: Bayuk, Enterprise Security for the Executive, 2010
Questions? Discussion?

Follow-up:

jennifer@bayuk.com