Systems Security Engineering

Jennifer Bayuk
Stevens Institute of Technology
www.SERCuarc.org
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

Systems Concepts

System Architecture

Logical Architecture

Allocated Architecture

Physical Architecture
Diagram of System of Interest with inputs and outputs.
1. Functional

2. Interface

3. System-wide – “ilities”

Source: Buede, The engineering design of systems, models and methods, Wiley, 2009
The Vee Model

Modeling Example

Security

perpetrators

enact

Threats

exploit

permit

harm

produce and manage

value

vulnerabilities

systems
Example

Source: Bayuk, SSE Lab Architecture Definition, 2010
Security Systemigram 6

- Security
  - Program Director
    - Security Policy
      - Metrics
        - Risk
      - Assesses
        - Audit
      - Reviews
        - Dictates
        - Observes
      - Requires
        - Report to
      - Facilitates
  - Lab System
    - Lab System
      - Shared Admin IDs
      - Internet Exposure
      - Inexperienced Admins
      - Controls
        - IAM, Firewall manual procedures
        - Logs tripwire
        - Protect
        - Monitor
        - Restores
    - Response
      - Audit trails
      - Provides
        - Faculty and student handbook professional ethics
      - Requires
        - Students, Professors, Admins
      - Decrease
        - Decrease
      - Increase
        - Decrease
      - Reduce
        - Increase
      - Networks
        - Threats
          - Sabotage
          - Authentication bypass
          - Network sniffing
          - Exploit
            - Exploit
            - Disruption
              - Breakage
              - Bad software config missing logs bed user setup
    - Experience
      - Classes
      - Education
      - Research
      - Produce and manage
        - When degraded may reduce
      - When degraded may reduce
      - When degraded may reduce
      - Identify
        - Professors, Admins
      - Enact
        - Employ
      - Thwarts
        - Cheating students disgruntled staff
    - Identify
      - Professors, Admins
    - Employ
      - Identify
Requirements Gathering Example

Source: Bayuk, SSE Lab Architecture Definition, 2010
Input and Output Requirements

Source: Bayuk, SSE Lab Architecture Definition, 2010
Functional Decomposition

Example of architectural influence: Isolate functionality exposed to majority of threats

Source: Bayuk, SSE Lab Architecture Definition, 2010
V and V

- 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 adequately secure?
<table>
<thead>
<tr>
<th><strong>Security:</strong></th>
<th>Something that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Feature:</strong></td>
<td>A system capability that contributes to its security.</td>
</tr>
<tr>
<td><strong>Security Metric:</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Security Framework:</strong></td>
<td>The concept of operations, mission, and environment under which a system operates.</td>
</tr>
</tbody>
</table>
SERC Security Approach

1. Devise System Security Engineering Methods
2. Devise Security Metrics
3. Design Secure Architecture
4. Define Security
5. Analyze System Mission and Purpose in Operational Context
If each SERC member concentrated on one system of interest and could prove something provided more or less security in that context, then we could, in combination, demonstrate the utility of the systems engineering methodology.

Though such an engineering approach may seem like practical application rather than research to some in our community, they may be overlooking the fact that security is not at all well understood, and so any serious investigation of its properties constitutes a research endeavor.