Lifecycle Models for Survivable Systems

Rick Linger

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense
© 2000 by Carnegie Mellon University
Survivability Concepts
Survivability Defined

Survivability is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.

No amount of security can guarantee systems will not be penetrated

Survivability focus is on mission continuity under adverse conditions
The “Three Rs” of Survivability

Resistance
• capability to deter attacks

Recognition
• capability to recognize attacks and damage

Recovery
• capability to provide essential services during attack and recover full services after attack
Survivable Network Analysis

**SYSTEM:** Essential services
- Essential service usage scenarios
  - Essential architecture components

**ENVIRONMENT:** Intrusion strategies
- Intrusion usage scenarios
  - Compromisable architecture components

- Architecture softspots
- 3Rs analysis
- Survivability Map recommendations
Survivability Impact on Traditional Development Life Cycle
# Survivability Impact - 1

<table>
<thead>
<tr>
<th>Lifecycle Activities</th>
<th>Key Survivability Elements</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Definition</td>
<td>Analysis of mission criticality and consequences of failure</td>
<td>Estimation of cost impact of denial of service attacks</td>
</tr>
<tr>
<td>Concept of Operations</td>
<td>Definition of system capabilities in adverse environments</td>
<td>Enumeration of critical mission functions that must withstand attacks</td>
</tr>
<tr>
<td>Project Planning</td>
<td>Integration of survivability into lifecycle activities and work products</td>
<td>Identification of defensive coding techniques for implementation</td>
</tr>
<tr>
<td>Requirements Definition</td>
<td>Definition of survivability requirements from mission perspective</td>
<td>Definition of access requirements for critical system assets during attacks</td>
</tr>
<tr>
<td>System Specification</td>
<td>Specification of essential service and intrusion scenarios</td>
<td>Definition of steps that compose critical system transactions</td>
</tr>
</tbody>
</table>
## Survivability Impact - 2

<table>
<thead>
<tr>
<th>Lifecycle Activities</th>
<th>Key Survivability Elements</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Architecture</strong></td>
<td>Integration of survivability strategies into architecture definition</td>
<td>Creation of network facilities for replication of critical data assets</td>
</tr>
<tr>
<td><strong>System Design</strong></td>
<td>Development and verification of survivability strategies</td>
<td>Correctness verification of data encryption algorithms</td>
</tr>
<tr>
<td><strong>System Implementation</strong></td>
<td>Application of survivability coding and implementation techniques</td>
<td>Definition of methods to avoid buffer overflow vulnerabilities</td>
</tr>
<tr>
<td><strong>System Testing</strong></td>
<td>Treatment of intruders as users in testing and certification</td>
<td>Addition of intrusion usage to usage models for statistical testing</td>
</tr>
<tr>
<td><strong>System Evolution</strong></td>
<td>Improvement of survivability to prevent degradation over time</td>
<td>Evolution of architecture in response to changing threat environment</td>
</tr>
</tbody>
</table>
Survivability Impact on Contemporary Development Life Cycle
Contemporary Life Cycle

Iteration of customer requirements, COTS market capabilities, and system architecture

Architectures and Engineering Cycle

Iteration 1 Iteration 2 Iteration 3 Iteration 4

Life cycle of continuous system evolution

© 2000 by Carnegie Mellon University
### Survivability Impact

- Reconcile mission survivability with COTS capabilities
- Assess COTS vendors for survivability focus
- Evaluate survivability of COTS products
- Achieve survivability in system integration
- Treat architecture as survivability integrator
- Maintain survivability as COTS products evolve