Dependable and Secure Computing for DOD Systems: Needs, Architecture, Challenges and Partnerships

Tom Bracewell
Systems Architecture Design and Integration Directorate
Raytheon Integrated Defense Systems     Arlington, VA
bracewell@raytheon.com

3rd ITI Workshop on Dependability and Security:
Opportunities and Challenges in Building an Overarching Community
Coordinated Science Laboratory
University of Illinois     Urbana, Illinois
December 5, 2006
Competition Sensitive
DOD Needs in Dependable and Secure Computing

- Mission assurance in information warfare
  - Operate through cyberattack
  - Lifecycle survivability

- Domains
  - Net-centric systems
  - Information systems

- System and network needs
  - Intrusion tolerant systems
  - Self-healing networks
  - Trusted dynamic coalitions
  - Situation awareness in systems of systems

Intelligence, Surveillance and Reconnaissance
DDG-1000 Total Ship Computing Environment

Computing environment for next-generation combat ships

- Layered architecture
- Automated fire control
- Support for net-centric warfare
Industry Challenges

• Architecture
  – Integrating “point solutions” from research
  – Combining security, dependability, performance
  – Scalability, adaptability, “ilities”
  – Successful reuse with predictable results
  – Developing common architectures

• Process
  – Engineering disciplines and methods
  – Validation, verification and measurement
  – Requirements and certification

Challenge: transforming technologies into effective systems
**Common Architecture**

**Architecture Principles**

**Operate Through Attack**

1st & 2nd generation - Basic protections
- Redundancy
- Static diversity

3rd generation security
- Isolation/containment
- Sensor correlation
- Graceful degradation
- Adaptive response

4th generation - Self-regeneration

**Lifecycle Survivability**
- Forensics, cognition
- Application communities
- System communities

**Other Principles**
- Harden security infrastructure
- Application transparency
- Design to weak assumptions
Operational Concept

Common Architecture

Haystackon
Integrated Defense Systems

Avoid/Remove Vulnerabilities
(Design, Removal, Blocking, System Communities)

Prevent Intrusions
(Access Controls, Cryptography, MLS)

Detect Intrusions, Limit Damage
(Firewalls, Intrusion Detection, Virtual Private Networks, PKI)

Operate Through Attacks
(Redundancy, Diversity, Graceful Degradation, Deception, Wrappers, Proof-Carrying Code)

Restore System
(Diagnosis, Learning, Reconfiguration, SW Rejuvenation, Reflection)

Conduct Forensics
(Auditing, Pattern Recognition, Cognition)

Lifecycle Survivability

Operate Through Attack
<table>
<thead>
<tr>
<th></th>
<th>Current Approach</th>
<th>Proposed Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Remove vulnerabilities</strong></td>
<td>Reactive; manual Manual</td>
<td>Learn and adapt (cognition) Share solutions (communities)</td>
</tr>
<tr>
<td><strong>Prevent intrusions</strong></td>
<td>Block known attacks</td>
<td>Recognize new attacks Share situation awareness</td>
</tr>
<tr>
<td><strong>Detect intrusions, Limit damage</strong></td>
<td>Detect some attacks Manual responses</td>
<td>Correlate sensor inputs Use measured responses Learn best responses Isolate and observe attacker</td>
</tr>
<tr>
<td><strong>Operate through attack</strong></td>
<td>None</td>
<td>Gracefully degrade Maintain critical applications Auto-reconfigure</td>
</tr>
<tr>
<td><strong>Recovery</strong></td>
<td>Manual</td>
<td>Self-regenerate</td>
</tr>
<tr>
<td><strong>Forensics</strong></td>
<td>Manual post-mortem</td>
<td>Reason about attacks Develop new policies</td>
</tr>
</tbody>
</table>
Building Partnerships

Opportunities to jointly pursue

– New research programs
– Seedling projects
– University directed research
– Externships / internships
– Cooperative research fellowships
– Graduate and certificate programs
– Long term partnerships