Adaptive System Security Policies

IMPACT
• Optimized survivability to network-based attacks
• Improved protection from insider attacks
• Support for network-wide intrusion response

NEW IDEAS
• Extensions to the Intruder Detection and Isolation Protocol (IDIP) to enable adaptable response decisions that optimize system survivability
• Support for both local and global policies for intrusion response
• Integration of control capabilities and global policy management into the discovery coordinator

SCHEDULE
Proof of Concept Demonstration

1997  1998  1999

Adaptive Policies Defines
System-Level Demonstration

Global Policy Distribution

Optimized Containment/Monitoring Decisions for System Survivability