Network Mission Assurance
Phoenix Challenge 2002 Conference

Lockheed Martin Advanced Technology Laboratories
Distributed Processing Laboratory
1 Federal Street • A&E Building 3W
Camden, New Jersey 08102

Mike Junod
mjunod@atl.lmco.com
(856) 338-3947

September 12, 2002
• ATL Organization

• Holistic Information Assurance

• Information Assurance Efforts
  — Network Mission Assurance (NMA) Framework
  — Threat Analysis & Prediction (TAP)
  — Cyber Attack Workstation (CAW)
  — Dynamic Trust-based Resource Allocation (DyTR)
  — Intelligent Agents
  — Virtual Network Simulator (VNS)
Over the past five years, ATL has become a major DARPA contractor. Lockheed Martin is a leader in information technology (ITO, ISO, TTO) and has established “military relevance” capability. Government laboratories (15%) provide a transition path from DARPA to the field and a strategic foothold for ACTD, ATD follow-ons.

For commercial work, which accounts for less than 5%, the near term is focused on small, working strategic relationships, while the long term goal is to grow to represent more than 20% of business. Lockheed Martin, with 35% of the work, currently has a 50/50 mix of development vs. services/consulting.
Overall Objectives

• Objectives
  — Dynamically Identify, Protect, and Ensure Survivability and Continued Operation of High Value/Critical Assets (Holistic Vision)
  — Predictively Determine Likely “Attack Campaigns” to Mitigate Major Disruption of High Value Assets & Ensure Critical Infrastructure Survivability

• Research Focus Areas
  — Active Network Management and Adaptive Quality of Service
  — Adaptive, Distributed Resource Allocation & Control
  — Secure Adaptive Agent Framework
  — Attack Knowledge Representation to infer Attack Patterns
  — Faster than Real-Time Exploration of Attacks & Response Effects
  — Dynamic Network Mapping and Exploit Determination in Support of Autonomic Information Warfare Operations
  — Dynamic Trust Assessment
Holistic Information Assurance
Infrastructure Model and Control
- Inspect infrastructure state
- Reflect controls back onto enclave infrastructure

Asset Identification
- Dynamically identify critical assets for mission objectives
- Map critical assets to low level resources

Threat Analysis and Prediction
- Infer patterns from network event observations
- Correlate patterns to likely attack campaigns
- Explore campaign effects on critical assets

Response Coordination
- Analyze campaign effects relative to mission objectives
- Identify and Initiate most effective response

Ensure Survivability of High Value Assets and Continued Operation of Critical Infrastructure Components
Integration alone is not sufficient. You need orchestration!

Core Infrastructure
- Information Model
- Distributed Object Services
- Code and Object Mobility
- Reflective Sensor Control
- Dynamic QoS Manager
- Network Discovery
- Network Resource Mgmt.

Visualization (Tree View)
- Multiple Views
- Sensor Attribute Access

Pluggable IA Capabilities
- Sensors
- Controllers
- Actuators
- Interfaces
Threat Analysis and Prediction

- **Attack Knowledge Base**
  - Attacker Capability Ontology
  - Attack method rules
  - ICAT (public software fault database based on CVE)

- **Use of Protégé, an open-source ontology editor**

- **Representation of attacker capabilities that result from the exploitation of software faults**

**Attack Projection**

- Forecasts the effects of the attack on infrastructure assets
- Takes predicted “next attack step” and simulates the effect upon the infrastructure and critical assets
- Identifies areas of need for close monitoring
Cyber Attack Workstation

Reconnaissance and Attack Tool Automation

- Automate the process of monitoring and attacking network
- Provide library of intelligence gathering, penetration, and denial of service tools for use through single interface
- Allow user with little experience in hacking to test attack mechanisms

Exploit Options

- Define High Level Attack Campaign

Defense Through Understanding of the Offense
Active, dynamic networks have limited or no a priori access allocation

- Adaptively determine trust
- Dynamically allocate resources

DARPA FTN Contract
out of AFRL
EMAA Security Architecture

Agent

• Audit Logging

CommunicationServer

AgentManager

EMAAClassLoader

Secure Class Loader

JVM

Security Manager

Access Controller

Operating System

Hardware

EMAA Framework

Application Specifics

Maximize the security provided by the framework

EMAA Framework

Maximize the security provided by the framework

Application Specifics

0%

100%

- SSL: Remote Host Authentication and Encryption
- Agent authentication
- Sole provider of threads to agents
- Checks agent privileges
- Loads authorized classes
- Establishes permissions for each agent according to policy.

- Dynamically checks permissions in policy.
### Some of ATL’s Agent-Based Systems

<table>
<thead>
<tr>
<th>Some of ATL’s Agent Systems</th>
<th>Customer</th>
<th>Application</th>
<th>ABS Ingredients</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Robots, Agents, People</td>
<td>DARPA</td>
<td>TBD (Seedling)</td>
<td>Heterogeneous Teams</td>
</tr>
<tr>
<td>• Cooperating Agents for Specific Tasks (CAST)</td>
<td>DARPA, NWDC</td>
<td>Navy Time-Critical Strike, Coalition C2</td>
<td>Info, imagery collection, correlation, dissemination</td>
</tr>
<tr>
<td>• Joint Interagency Task Force - East (JIATF-E)</td>
<td>DARPA</td>
<td>Ship Tracking</td>
<td>Information retrieval, integration</td>
</tr>
<tr>
<td>• Log C2/Agile Commander</td>
<td>CECOM</td>
<td>Plan Monitoring</td>
<td>Sentinels</td>
</tr>
<tr>
<td>• Dismounted Guardian</td>
<td>CECOM</td>
<td>Threat Alerts</td>
<td>Data sharing, distributed</td>
</tr>
<tr>
<td>• Small Unit Ops</td>
<td>DARPA</td>
<td></td>
<td>Fusion</td>
</tr>
<tr>
<td>• LCS - Marine</td>
<td>DARPA</td>
<td>Logistics Requests</td>
<td>Human-computer dialog</td>
</tr>
<tr>
<td>• Joint Logistics/JTL ACTD</td>
<td>DARPA</td>
<td>Logistics Integration</td>
<td>Data integration/mediation</td>
</tr>
<tr>
<td>• Airborne Manned/ Unmanned System (AMUST)</td>
<td>Army AATD</td>
<td>SA for Command on the Move</td>
<td>Data access, sentinels</td>
</tr>
<tr>
<td>• Air Mobility Command, Coalition Operations, etc.</td>
<td>AFRL</td>
<td>Plan Monitoring/ Replanning</td>
<td>Data access, sentinels</td>
</tr>
</tbody>
</table>

**ATL Agent Technology has been Deployed on >20 Programs**
Virtual Network Simulator (VNS)

- Designed to rapidly configure and simulate Army tactical networks
- Focuses on training Information Assurance Manager (IAM) or IA Network Manager (IANM) to react to network attacks
- Interfaces with CECOM’s existing Internet Attack Simulator (IAS)
- Simulates CECOM/s attack taxonomy and C2 Protect tool behaviors

### Instructors Interface
- Configures network training scenarios
- Selects and launches network attacks
- Monitors student performance

### Student Interface
- Initializes network configuration and protection mechanisms
- Monitors network performance and attack alerts
- Responds to attacks using available protection tools

**Internet Attack Simulator**

**Virtual Network Simulator**

**HLA Runtime Infrastructure (RTI)**
VNS Network Monitoring Features

- Alert Messages from the IDS change the borders from light **BLUE** to flashing **RED**
- Links Change Between bright **GREEN** and **RED** to signify changes in traffic density

VNS Network Control Features

- The scan of the router is detected by the IDSs
- Student is able to drill down and investigate
- Student is able to recognize trouble as the attacked links “heat up”
- Student is able to select a router to investigate further
- Student deduces the DoS attack and takes corrective action
Lockheed Martin Booth

Questions?


6. M. Junod, “Cyber Attack Workstation (CAW)”