Major HCI Challenges Supporting the Dependability, Safety and Security of Evolving “On Demand” Enterprise Computing and Communications Services

Arthur S. Robinson S/TDC
O. Sami Saydjari - CDA
First, a word about terminology:

• Enterprises understand the need for continuity in their mission critical services, despite stresses such as imperfections in system hardware, software and human-computer interactions; damage caused by both environmental stresses and physical attacks; and disruptions caused by both internal and external cyber attacks.

• In effect, they understand the need for service dependability, safety and security, but have not yet agreed on a single term encompassing all three attributes.
• We have attempted to use “Enterprise Vulnerability Management” to describe the integrated management of Enterprise dependability, safety and security vulnerabilities, with limited acceptance to date.

• Users appear to be more attracted to terminology such as “Enterprise Survivability”.

• Since there is a major world need for processes that address all threats to mission continuity from an integrated perspective, we are continuing to use all three terms until consensus emerges on how best to describe their integrated effects.
Current System Upgrade Processes Often Do Not Address Important Dependability, Safety and Security Issues

Typical upgrades focus on increasing profits and productivity by increasing demands on:
- Web Enabling
- Collaboration
- Distributed Commerce Transactions
- Outsourcing
- Often without adequately addressing critical system dependability, safety and security issues!
W.G. 10.4 Has Played a Major Role In Identifying the Additional Stress Testing Processes Needed to Assess & Mitigate the Combined Effects of Enterprise Dependability, Security, and Safety Stresses
Approved Certification & Assessment Processes Can Be Used to Drive Enterprise Vulnerability Management (EVM) Planning & Implementation

1. Government Dependability Certification & Accreditation Processes
2. Government Security Certification & Accreditation Processes

- Define Scope/Identify Assets
- Define Vulnerability Management Requirements
- Customize Processes & Assess Vulnerabilities
- Vulnerability Management Roadmap Planning
- Implement EVM Roadmap

Tools for Customization and Documentation of Enterprise Vulnerability Management Processes

Vulnerability Management Case Database

- Identify Critical Enterprise Assets
- Desired/Current States
- Customize & Integrate Selected Products & Tools
- Event Monitoring, Logging & Analyses

- Acquired Testing Evidence
- Technical Assessments
- Plan Product Trade Offs
- Create Roadmap

Customize Processes & Assess Vulnerabilities

Command and Control of System Defenses essential during O&M phases to assure effective responses to evolving threats.
Evolving “On Demand” Architectures Will Depend on Linked Sequences of Services to Provide Required “End-to-End” Quality of Service (QoS) Capabilities

- For example, boundaries of computing Enclaves

- Personnel supporting a given Enclave are part of its assessment, but may also support other Enclaves and/or move physically between Enclaves
- Personnel within Enclaves may also be sources of Cyber attacks

- Boundaries of Enclave to Enclave Communications

Vulnerability assessments and certifications need to also address security, safety and dependability issues associated with Mobile Support Personnel and their interactions with wireless networks
Need to Contend With Multiple Applications With Varying Security Requirements and Current System Benefit/Value, Competing for System Hardware, Software and Human Resources

Increasing Levels of QoS Management Automation Will Enable Initial Reductions in People Support, But System Designs Must Assure Human Understanding of Current System Status and Provide Means for Effective Human Participation in Detecting, Interpreting and Recovering From Continuously Evolving Levels of System Stresses
Broad Spectrum of Adaptive Resource Management Advances Under DARPA’s “Quorum” Program Established Foundation for Current Industry-Wide Commitment to Providing End-to-End, QoS Controlled, “On Demand” Services

**Monitor**
- **MONITORING**
  - Instrumentation
  - Performance and health monitoring
  - QoS Monitoring
  - Resource Discovery
  - Resource Availability Monitoring
  - Fault Detection and Prediction

- **ADAPTIVE RESOURCE MGMT**
  - QoS Negotiation
  - Fault Mgmt/Recovery
  - Resource Allocation/Reallocation
  - Stability Analysis

- **PROGRAM CONTROL**
  - Application Control
  - System Initialization and Cleanup
  - Dependency-based Control

- **Service Level Agreement (SLA)**
  - QoS Negotiation
  - Fault Mgmt/Recovery
  - Resource Allocation/Reallocation

- **Visualisation**
  - System/Resource Configuration and Statuses
  - Performance Statistics
  - System Specifications

**Decide**
- **Information Assurance Services**
  - Authentication & Policy Based Authorization
  - Secure, Safe and Dependable Measurement, Interpretation & Management of System Wide Resources

- **Control**
  - Performance & Status Fault/Failure/Overload Detection & Prediction
  - Fault Analysis

- **QoS Specifications**
  - App Profiles
  - Fault Mgmt Specs
  - Config Specs

- **Control Orders**

- **Results**

- **Config Changes**

- **Application Performance**

- **Config Specs**

- **Application Orders**
- Accepts directives from higher levels
- Provides status to higher levels
- Manages lower levels
- Higher levels receive information about performance of lower levels
SCALABLE PERFORMANCE

"When you need the system the most, that's when it performs the worst..." -- CDR D. Stevenson

- Today's systems often exhibit degraded performance as tactical load increases
- Systems may be over-designed for worst case; this increases complexity & cost
- Scalability provides constant performance despite load & allows sharing of resources

Scalable Computing Architecture
- Networked computers
- Distributed system middleware
- Scalable computer programs
- Load sharing management
QoS Resource Manager

Network Resource Monitor

Mission Critical Application

“On Demand” Quality of Service (QoS) Management using QoS Metric Services (QMS)

QoS Self Adaptation

Monitoring of System Resource Allocation Reasoning Processes

Competing Application

Sample QMS Application
Resilient System Fall Back Modes Will Require Both Automated and Human Based Monitoring, Detection, Interpretation and Recovery Control Capabilities
A coherent approach towards assuring their defense requires:
- Ability to provide visibility into the extent of the security attacks
- Ability to counter the attacks through coordinated control of distributed system resources

Security is another dimension of the end-to-end service guarantee.

Assured communications of measurement and control information between distributed system resources and their system security management facilities.

Assured communications to distributed system resources of attack countermeasure control commands generated by the system security management facilities.

Capabilities must be survivable despite failures of individual Node, Group or Enclave defenses.

"Dependable and Secure System Spinal Cords"
Cyber Command and Control

Human-Computer Interaction for Strategic Decision Making

O. Sami Saydjari, CDA

6 July 2004
Problem and Premises

• Attackers are creative
• Missions and values are dynamic
• Defenders are creative
• Human brain recognizes patterns well
• Policies are limited to known
Command Cycle Feedback Loop

**Decide**
- Rapid Response
- Tactical Decisions
- Strategic Decisions

**Orient**
- Visualization
- Cognitive Science
- Correlation and Fusion

**Act**
- Change Firewall Rules
- Disable Accounts
- Retask Sensors

**Observe**
- Vulnerability Assessment
- Intrusion Detection
- HUMINT

- Game Theory
- Adversary Models
- Complexity Theory
- Assurance Methods
- Red Teaming
- Forensics

Strategic Decisions
Tactical Decisions
Rapid Response
Command and Control

- **Command**
  - Decision-making process among possible actions given one’s understanding of the situation.

- **Control**
  - Process of ensuring a command choice is correctly executed and has desired effect.
Cyberspace Character

- Butterfly effects
- Super-human tempo
- Poorly understood interdependencies
- Attack-Defense asymmetry
Basic Operation

Situation

- Attacks

Decision

- Defenses
Situation

- Model defense readiness
- Model attack status – multi-threads
  - Best guess on possible attacker plan
  - What is he doing, and where is he going
- Alert humans when decision is needed
- Status of defensive actions
- Delta to goal state (control)
Models Models Everywhere
Decision

- What are action options given the situation
  - Remind user in stressful situation of choices
  - Give less experienced users benefit
- Which have been most successful
  - In real situations
  - In simulations
- How long do decisions take to execute
- What are the consequences
  - On my mission
  - On attacker’s goal
- What further information do I need
- Where is attacker headed?
Sample Cyber Command and Control Interface

**Enclave Monitors**
- **Enclave Function Status**
  - Edit View Plans
  - Distribute Plans
  - Distribute/Receive Reports
  - Send/Receive Email
  - Browse Internet
- **Service Status**
  - Heartbeat
- **Daily Scan Results**
  - Virus
  - Vulnerable

**Situation Monitor**
- **Indications and Warnings**
  - 0801 Stealthy scan on VPN from WOC
  - 0802 Anomalous email from WOC to BR
  - 0804 Stealthy IP address scan
  - 0805 Anomalous connection from WS1 to DB
  - 0805 Anomalous Filename scan & DB access
- **Possible Causes**
  - Plan Corruption Attack
  - Plan Compromise Attack
  - Adversary Reconnaissance
- **Impact**
  - Plan corruption or compromise risks mission

**Response Planning and Execution**
- **Recommended Actions**
  - Review audit logs on anomalous host
  - Automated internal consistency check of plan
  - Increase sensor sensitivities
- **Executing Actions**
  - Vulnerability Scan
  - Virus Scan

**Enclave Function Status**
- Edit View Plans
- Distribute Plans
- Distribute/Receive Reports
- Send/Receive Email
- Browse Internet

**Service Status**
- Heartbeat

**Daily Scan Results**
- Virus
- Vulnerable

**Alerts Per Minute**
- 200
- 160
- 120
- 80
- 40