

Organically Assured and Survivable Information Systems (OASIS)

Dale M. Johnson, Ph.D.

Doug Williams, Ph.D.

703-983-3668 • djohnson@mitre.org

703-983-6112 • dwill@mitre.org

DARPA/ITO



Problem

- **A survivable system is one that can continue to provide the specified services, possibly in degraded mode, to the users in the face of a cyber attack or intrusion.**

- **Tasks:**
 - **Assess current DARPA OASIS survivability technologies**

 - **Support the building of a program for developing a survivable system resistant to cyber attacks**

Background

■ *After September 11, 2001*

What was only imaginable is now a reality

What was inconceivable can now be imagined



Objective

- **Support OASIS objectives**
- **To conceive, design, develop, implement, demonstrate, and validate architectures, tools and techniques that would allow fielding of organically survivable systems**
- **To perform assessment and validation of organically survivable information systems**



Activities



- **Develop assessments of DARPA OASIS technologies for survivability and determine coverage of them over the spectrum of potential cyber threats**
- **Assist in building a program for developing a survivable system using a selection of OASIS technologies**



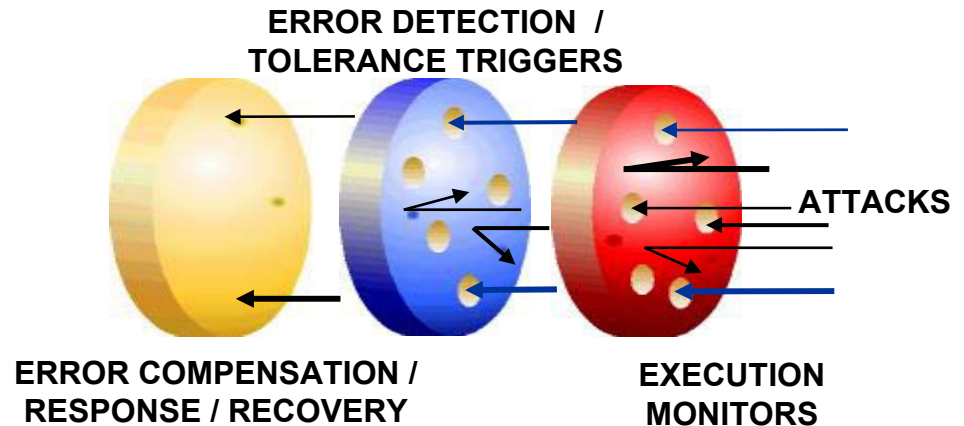
Highlight

Approach

- **Confine malicious code-- compare actual behavior with predicted**
- **Detect errors: watermark, time/value domain anomalies, rear guards**
- **Error compensation and recovery: distributed computation, design diversity & deception**

Top Technical Challenges

- Real-time trade of security, performance & functionality
- Cost-effective solutions
- Validation and verification

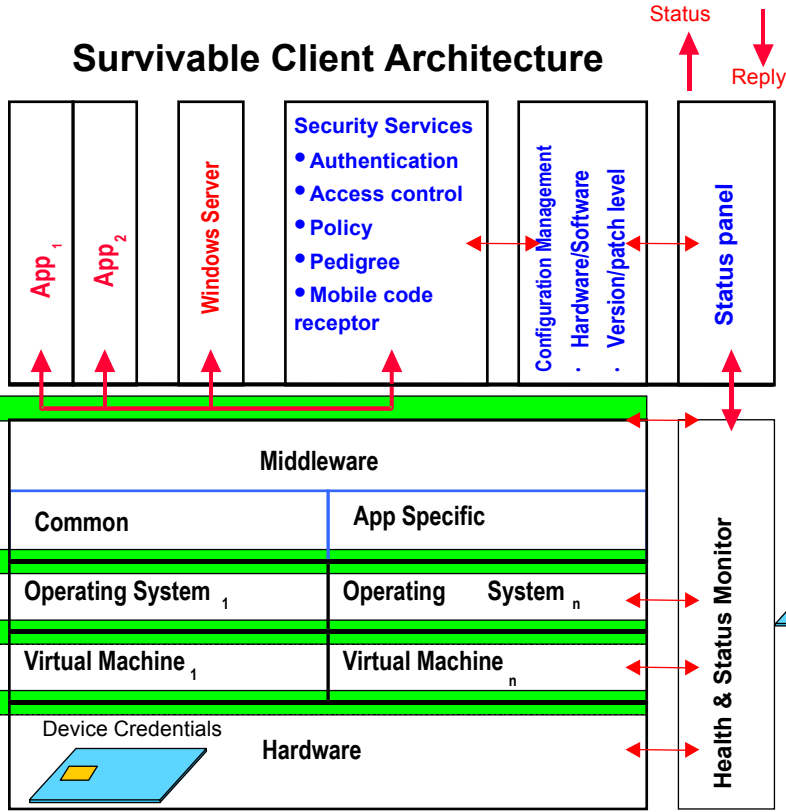


Selected Accomplishments & Transition Partners

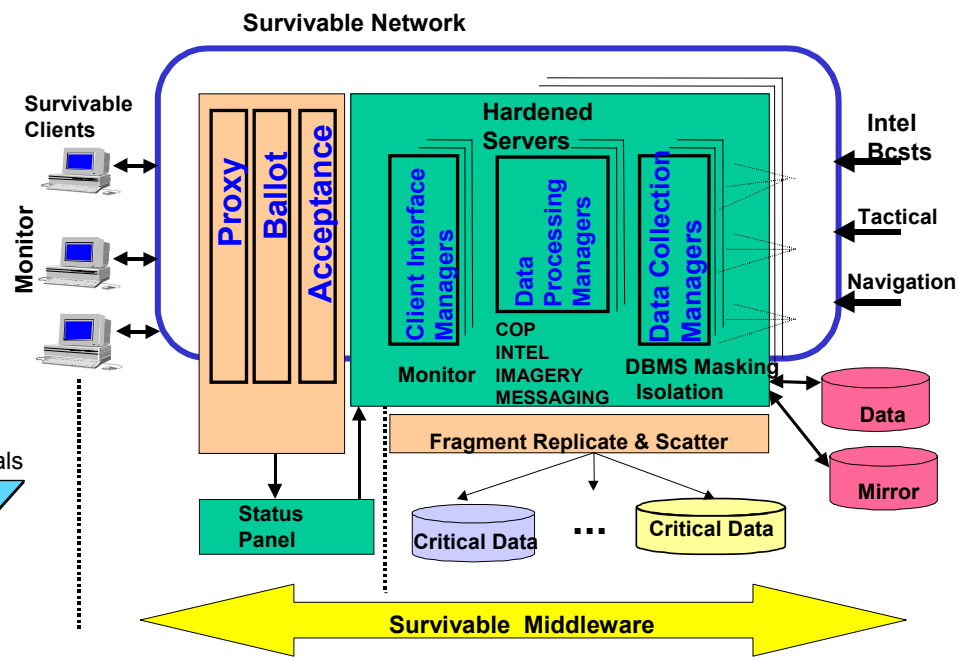
- Protection against mobile malicious code - **US Pacific Command**
- Intrusion-tolerant data storage - **USAF Joint Battlespace Infosphere**
- Watermarking of imagery - **USAF Information for Global Reach ATD**
- Insertion of code to monitor malicious action by legacy software - **Phase Forward, Inc**
- Proof-carrying code - **Intel**

Highlight/Demonstration

Survivable Client Architecture



Survivable Server Architecture



**Design, Demonstrate & Validate
Intrusion Tolerant Military Application**



Impact



- **Completed development of assessments of DARPA OASIS technologies for survivability and analysis of coverage of them over the spectrum of potential cyber threats**



Future Plans

OASIS Technologies



**ERROR
COMPENSATION/
RESPONSE/
RECOVERY**

Spatial, Temporal, Design, and Analytical Redundancies, Dynamic Reconfiguration, Quality of Service Trade-Offs, Fragmentation & Dispersal, Deception (Randomness, Uncertainty, Agility, Stealth), Graceful Degradation, Intrusion Tolerant Architectures

**ERROR
DETECTION/
TOLERANCE
TRIGGERS**

Watermarks, Mediated Interfaces, Rear Guard, Value & Time Domain Error Detectors, Comparison & Voting, Acceptance Checks, Redundancy-Based Cyber Attack Detection

**EXECUTION
MONITORS**

In-Line Reference Monitors, Sandbox Active Scripts, Code Interposition, Wrappers, Proof Carrying Code, Graph Based Program Encoding, Monitor COTS Binaries, Secure Mobile Code Format, Operate through Mobile/ Malicious Code Attack

**FAULT
AVOIDANCE**

Provably Correct Protocols, Secure-design Principles, Software Vulnerability Detection, Design Assessment and Validation