



NDIA
MDA SBIR Industry Day
26 July 2007

Information Assurance Research Area

Ms. Susan Todd
MDA/DOS



Agenda



- Research Area Objectives
- List of Topics
- Topic Overview
- Questions



Research Area Scope and Objectives



- The Ballistic Missile Defense System (BMDS) contains a diverse set of components requiring protection from a wide array of threats.
- The purpose of the Information Assurance (IA) Research Area is to research and development technologies and tools that are designed to enhance the security posture of the BMDS.



Topics



-
- Distributed Real-time IA Management Technologies
 - Configuration Validation Technologies
 - Security Policy Reconciliation
 - Voice over IP Security
 - Ballistic Missile Defense Anti-Tamper Volume Protection



Distributed Real-time IA Management Technologies



- **OBJECTIVE:** Develop and demonstrate innovative solutions to the problem of distributed security management and assessment in the context of the Ballistic Missile Defense System (BMDS).
- **KEY FOCUS:**
 - Assessment of the overall security state based on the state of the components individually and collectively across the BMDS.
 - Distributed, near real time, secure, adaptable
 - Management, analysis, correlation, assessment, and reporting of information assurance situational data throughout the BMDS.
 - Alternative approaches that do not rely on centralized storage of IA data and incidents.
 - Identifying activities that could be characterized as precursors to a malicious attack and/or correlating separate events across a wide area network.
 - No impact to the operational network.
- **PHASE I:** Analyze, design and conduct proof-of-principle demonstrations of methods for distributed, near-real-time, security management systems that provide comprehensive situational awareness of the Information Assurance state of the BMDS and its components.
- **PHASE II:** Develop and demonstrate prototype platform/software/hardware that demonstrates advancement of distributed near-real-time, security management systems that provide comprehensive situational awareness of the Information Assurance state of the BMDS and its components by illustrating functional effectiveness for a subset of BMDS components.



Configuration Validation Technologies



- **OBJECTIVE:** Develop and demonstrate innovative solutions to the problem of validating secure state and validated hardware/software baselines for computer systems that are returned to an operational status after having been in a test or development status.
- **KEY FOCUS:**
 - Verification when an asset transitions from a non-operational state to operational that it is in a known and secure state.
 - Transition to an operational status is be ready for defensive operations on short notice.
 - Validation includes:
 - the existence of only approved hardware and software, to include verification that nothing extraneous was introduced;
 - no required hardware or software has been removed;
 - system settings and parameters are as defined for the secure state;
 - hostile attempts alter the asset in a way that would harm or degrade the BMDS mission did not occur.
- **PHASE I:** Analyze, design, and conduct proof-of-principle demonstrations of techniques and mechanisms for validating the state and configuration of operational BMDS assets.
- **PHASE II:** Develop and demonstrate prototype platform/software/hardware that demonstrates the ability to discover variances from the required operational configuration and state.



Security Policy Reconciliation



- **OBJECTIVE:** The computing networks of Ballistics Missile Defense Systems (BMDS) are an important target for the enemy. One key area of critical importance to the BMDS is the ability to integrate computer systems, components and applications to perform an integrated mission implementing cooperative security policies.
- **KEY FOCUS:**
 - Preservation of the security policy within a system, subsystem and application layers in complex systems.
 - Automated policy reconciliation and composition across a distributed enterprise level system of systems to detect vulnerabilities.
 - The discovery of semantic interoperability issues that could lead to weak or limited policy enforcement.
 - Formal and semi-formal modeling techniques for validation of the divergence of the policies among integrated components, supporting the composition of security policies.
 - Solution should :
 - Apply to large-scale, dynamic, enterprise level systems in a system of systems context
 - Accommodate multiple, evolving, and flexible device management protocols.
 - Be system-independent
 - build upon on-going research including the Department of Defense (DoD) Goal Security Architecture (DGSA).
- **PHASE I:** Develop methods and tools that support security policy interoperation and application level certification and accreditation in a system of system context.
- **PHASE II:** Continue development of technology based upon based on Phase I results and demonstrate technology in a realistic environment. Identify opportunities for transition of this technology into BMDS programs.



Voice over IP Security



- **OBJECTIVE:** Develop and demonstrate innovative solutions to the problem of enforcing and implementing security solutions for Voice over IP (VoIP) that can be controlled outside of private network boundaries.
- **KEY FOCUS:**
 - VoIP security solutions that enforce and maintain security policies and mechanisms implemented within private network boundaries outside of those boundaries.
 - Privacy, confidentiality, authentication, integrity of communications
 - Consideration of existing firewall and network address translation policies and implementations.
 - Protection from denial of service, replay, or spoofing
- **PHASE I:** Analyze, design, and conduct proof-of-principle demonstrations of techniques and mechanisms for establishing secure VoIP within the BMDS.
- **PHASE II:** Develop and demonstrate prototype platform/software/hardware that demonstrates the ability to enforce the security policies necessary for communication within the BMDS.



Ballistic Missile Defense Anti-Tamper Volume Protection



- **OBJECTIVE:** Develop and implement new innovative anti-tamper (AT) volume protection technology for the protection of critical technology against exploitation.
- **KEY FOCUS:**
 - Development of innovative AT techniques and technologies that provide protection from reverse engineering and compromise of both hardware and software.
 - Integration into weapons platforms and their associated hardware and software
 - Portable and re-usable.
 - Applicable to and compatible with various commercial-off-the-shelf (COTS) and military hardware.
- **PHASE I:** The contractor shall develop the conceptual framework for new and innovative AT volume protection technology or technique that is integrated with, or tailorable to, the volume being protected. The contractor will also perform an analysis and limited bench level testing for an understanding of the new and innovative volume protection technology.
- **PHASE II:** Demonstrate and validate the use of AT volume protection technologies into one or more prototype efforts and estimate the effectiveness of the techniques. A partnership with a current or potential supplier of MDA systems, subsystems or components is highly desirable. Identify any commercial benefit or application opportunities of the innovation.