SAND2009-4304C

A Systems-based Approach to Insider Security

Felicia A. Durán
Sandia National Laboratories - Security Systems Analysis

David P. Duggan
Sandia National Laboratories - Threat Analysis Technologies

Patrick T. Hester
Old Dominion University – Department of Engineering Management and Systems Engineering

July 15, 2009

Project Team
Betty Biringer, Gregory N. Conrad, Stephen H. Conrad, Bruce Held, Kim Mitchiner, Roger Suppona, Carla Ulibarrí, Gregory D. Wyss,

LDRD
LABORATORY DIRECTED RESEARCH & DEVELOPMENT

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
This work is funded by Sandia's Laboratory Directed Research and Development Program

Sandia National Laboratories

Introduction

- **Describe work we are doing to support the development of a systems-based approach for insider security**
  - **Investigate, develop, and demonstrate formal systems engineering methods**
  - **Modeling and simulation**
  - **Create a process and architecture with principles, methods, and practices for designing, evaluating, and operating systems that are resistant to insider threats**

Overview of Problem

- **Malicious insiders**
  - Among the most ubiquitous and capable security threats
  - Affect every organization in forms that range from petty theft and fraud to espionage and terrorism
- **Focus of previous efforts**
  - Characterize the insider threat
  - Review reported insider incidents
  - Advanced detection strategies
- **Current protections against malicious insider activity**
  - Expensive, intrusive, implemented piecemeal, and operate independently
  - Demonstrate varying levels of effectiveness
  - Little understanding of integrated protections and overall effective insider security
- **High asset facilities need to demonstrate effective insider security while also improving operational efficiency**
- **A significant need exists for improved insider security methods**

Systems-based Approach

- View the problem as more than detection – instead consider all operational activities
- Consider the entire organization as a system that includes elements that not only provide protection against the insider threat, but also influence the insider's characteristics, motives, and capabilities

Systems View of Insider Security

- **Organizational systems and operations that contribute to insider security – existing and others**
  - **Mission and organizational requirements**
  - **Human resources (hiring practices, background checks, medical, benefits, employee assistance, vacation, sick leave)**
  - **Personnel security (clearances, visitor requests, travel)**
  - **Physical security**
  - **Cyber security**
  - **Counterintelligence**
  - **Information security**
  - **Intelligence community**
  - **Management**
  - **Waste, fraud, and abuse**
  - **Security incident management**
  - **Others…**

Systems View of Insider Security

- **Key system element is the Employee Population – all "employees" are insiders**
  - **Have some level of access, knowledge, and opportunity**
  - **Includes contractors, consultants, and service providers that are not direct employees of an organization**
  - **Of concern is the malicious insider**

Systems-based Approach to Insider Security

- Consider how the insider threat would evolve throughout an employee's career (employee life cycle)
  - Motive, opportunity, and means
- Integrate information and practices from different security disciplines and operational processes
  - Important interactions and interdependencies
- Determine interactions of employee population with insider protection methods
- Explore system changes
  - Effectiveness and costs of different sets of protection measures
  - Changes in policies and practices
  - Impacts of new security technologies, policies, access controls

Results To Date

- **Insider detection and protection mechanisms**
  - Secondary component of other systems
  - Many are ad hoc
  - Operate independently of each other
  - Not well funded
  - Therefore, are results of individual efforts
- **Employee Life Cycle**
  - Modeled using system dynamics
  - Resonates with those working insider problem
  - Identifies transition points of employees
- **Glossary of insider terminology**

Path Forward

- **Modeling and simulation**
  - **Employee Life Cycle**
    - **Map sensing, deterrence, and protections to transition points**
    - **Exercise using case studies**
    - **Determine shortfalls**
    - **Understand important interfaces**
  - **Information Protection and Control**
- **Insider security system**
  - **Determine or develop metrics**
    - **Security culture, deterrence, others**
  - **Develop notional system architecture**
  - **Develop or describe additional sensors or actions necessary to cover shortfalls**
- **Process development**
  - **Demonstrate application for design and evaluation**
  - **Apply to a range of organizations**