SAND2010-1646C

Integrated Protection System to Mitigate the Insider Threat

Betty Biringer
Manager, Security Risk Assessment Department
Sandia National Laboratories
(505) 844-3985
bebirin@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Mitigating the Insider Threat – Formidable Task

- Greatest challenge to any security system is protecting against the insider threat
  - Maintain respect and confidence of personnel
  - Employees must be able to do their job
  - Problems are detected only after event has occurred
  - No easy solution
    - Technology/procedures are limited or may not exist
    - Protection measures for insider threat may be limited by legal and political issues

Previously Most Common Protection Features

- Background investigations
  - Clearance process
  - Personnel reliability programs
- Peer reporting
- Two-person rule
- Tamper-indicating sensors
- Inventories/material accounting systems (may not be timely)
- Contraband detection screening on entrance
- Asset detection screening on exit

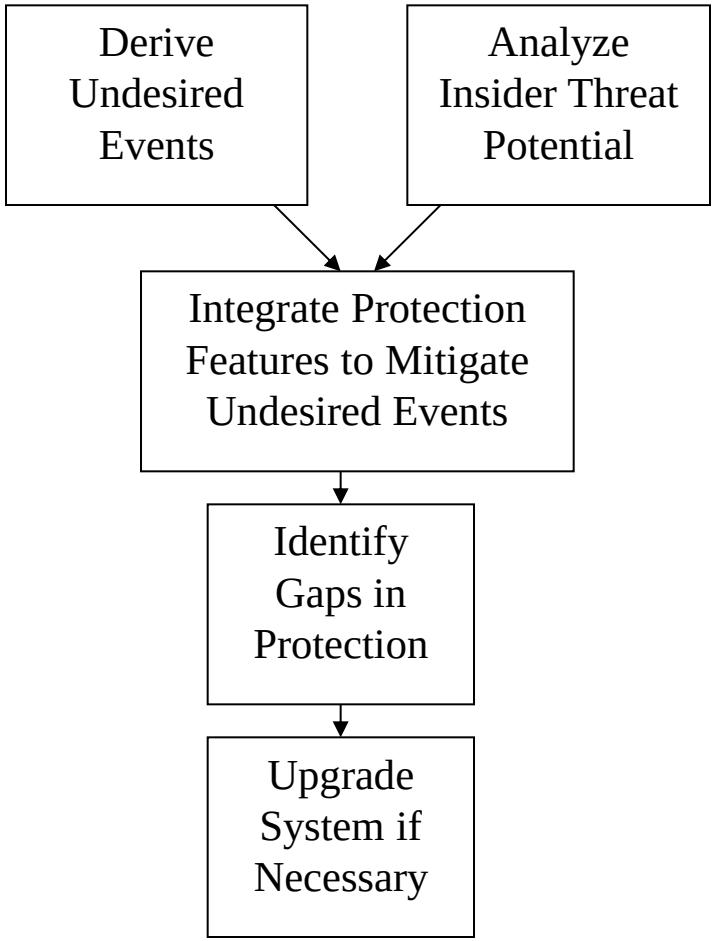
Lessons Learned

- Protection schemes for insider threat must demonstrate high regard for adhering to laws that protect personnel privacy
- Organizations must maintain trust of employees
- Valuable to know apriori what if ?… have an adversary in specific job positions
- No single protection function can solve the insider mitigation problem
- Total System Approach Needed
  - A protection system that integrates protection functions
  - Central repository of information (derogatory) can be used to mitigate the insider threat (potential for pre-event information)

Protection Objectives to Mitigate the Insider Threat

- Minimize potential for hiring an adversary
  - Pre-employment screening
  - Continuous monitoring
- Deter on-staff employee from becoming an adversary
  - Integrated protection system
    - Integrate protections functions
    - Provide protection-in-depth
      - Increase risk/uncertainty to the insider adversary
        - Add opportunities to detect unauthorized actions
        - Add obstacles/tasks for adversary
      - *Make it easy to do the right thing, very difficult to do the wrong thing*
  - Complete proper response to malevolent acts that do occur

Total System Process



Summary-
Mitigating the Insider Threat

- Minimize the risk of hiring an adversary
- Understand the potential consequences incurred of an adversary in key job categories
- Implement a protection system that makes it hard to do the wrong thing
  - Provide protection-in-depth (increased detection opportunities and obstacles)
  - Maintain active/timely central repository of (suspicious behavior) information