SAND2007-3011P

Assured Security by Design: A Systems Approach for a More Dangerous World

Security Systems and Technology Center

Sandia National Laboratories

May, 2007

Sandia National Laboratories

Why?

- Increasing Threat
  - Numbers
  - Resources
  - Knowledge
  - Consequences
- Increasing Cost of Traditional Security
  - Modifications
  - Response Force
  - Effect on Operations

Future State of Security

- Principles of Cost Effective Risk Management for Increasing and Evolving Threats
  - Intrinsic Physical Security
    - Built into overall system design (early and ongoing)
  - Integrated Physical Security
    - Optimized with other system functions (Operations, Safety, Cyber)
  - Dynamic Physical Security
    - System can adapt based on State Before, During, After Attack
  - Integrated Risk Management
    - Includes Threat and Consequence as Well as Vulnerability
      - Detect Adversary Gathering Resources
      - Mitigate Consequences
    - Uncertainty Risk Analysis (URA) for Risk Evaluation
      - New Tools
        - Adversary has a choice
        - State of Knowledge for Defender regarding Scenarios Adversary will Select

Intrinsic Physical Security

- Mission Critical Systems must be designed to operate in an Adversarial environment
  - During all design phases for facilities, infrastructures, and missions
  - Security is a high level requirement of the total system
- Built into the System (physical, information, operations) Design
  - Operations designed to reduce Insider Threat
- Continued throughout the ongoing operational and sustainment phases
- Complements extrinsic physical security, i.e. protection systems
  - Detection
    - Includes Extended Detection beyond Protected Area
  - Delay
    - Sufficient Delay at Correct Layer
      - Delay Deep Inside Facility can be used by Adversary
    - Active Denial Systems
  - Response
    - Minimize Number of Responders Onsite

Sandia National Laboratories

Integrated Physical Security

- **Comprehensive Risk management through integrated design and analysis requirements across domains**
- **Integrated physical security optimized with other system functions:**
  - **Safety**
    - **Resolve conflicting requirements**
    - **Seek synergy, e.g., Common means for Mitigating Consequences**
  - **Operations**
    - **Resolve conflicting requirements**
    - **Address the Insider Threat**
      - **Seek synergy: If security requirements are onerous, people will bypass those requirements to get their jobs done, thus creating opportunities for insiders.**
  - **Cyber Security**
    - **Physical Security aspects of Cyber Security**
    - **Cyber Security aspects of Physical Security**
  - **Material Control and Accounting (if required)**
    - **Ensure material to be counted *is* counted**
  - **International Safeguards (if required)**
    - **Optimize Containment and Surveillance for IAEA Safeguards**

Dynamic Physical Security

- System can adapt based on state:
  - Before the Attack
    - Proactive Readiness
      - Configure Facility and Security based on Current Threat Information
      - Interface with Intelligence Sources
        - National Regional, Local
  - During the Attack
    - Active Denial
    - Last Resort Options
      - Based on Weapons Strong Link-Weak Link Concept
      - Render Target “Inert” If Adversary Success Imminent
        - Security provides “Strong Links”
        - Last Resort options are “Weak Links”
  - After the Attack - Reduce Consequences
    - Contingency Plans to Mitigate Consequences
      - Integrated with Safety Mitigation Measures

Expand Solution Space from Vulnerability to Risk

- Risk a function of:
  - Threat
  - Vulnerability
  - Consequence
- Current practice:
  - Evaluate Vulnerability to Design Basis Threat
  - Focus on Physical Security from the Protected Area inwards
    - Fort Mentality
- Expand to Address Threat
  - Detect Gathering of Resources
    - Adversary gathering of Attributes: numbers, equipment, weapons
    - Adversary gathering of Information: reconnaissance, internet, insider
- Expand to Address Consequence
  - Multiple Consequences
    - Adversary Desired Consequences may differ from Defender Consequences of Concern
  - Mitigation of Consequences

Use of Defender Resources

Design Basis Threat

Defenders Allocate Resources on Physical Security to Defeat Attack by Adversary Using Resources at the DBT Level

Defenders Allocate Resources on Intelligence to Detect Adversary Gathering Resources above the DBT Level

Increasing Adversary Resources

Design and Evaluation for Security and Safety

- Design Criteria
  - Design Basis Accidents (DBA) for Safety
  - Design Basis Threats (DBT) for Security
- Risk Evaluation
  - Probabilistic Risk Analysis (PRA) for Safety: Existing Tools
    - Initiating events beyond the DBA
    - Subtle events within the DBA but missed
    - Uncertainty is Aleatory (random)
      - Probability for Measure of Uncertainty
  - Uncertainty Risk Analysis (URA) for Security: New Tools
    - Threat scenarios beyond the DBT
    - Subtle scenarios within the DBT but missed
    - Uncertainty is highly Epistemic (state of knowledge)
      - Belief/Plausibility for measure of Uncertainty
        - Includes Probability as a special case

Risk Analysis

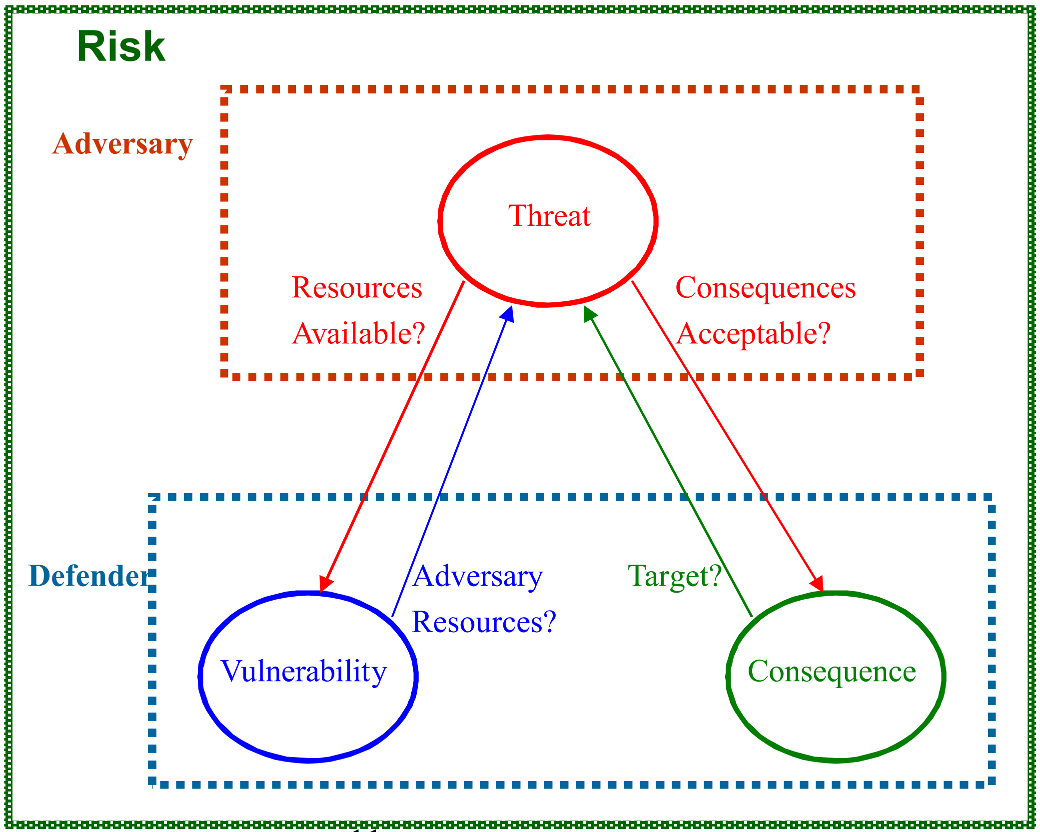
- For Both Safety and Security
  - Risk = Initiating Event x System Response x Consequence
- Initiating Event
  - "Dumb", Random event for Safety
  - Malevolent, Intentional event for Security
    - Adversary has a Choice, Not Random
    - Defender does not know Adversary Choice: Epistemic Uncertainty
- Uncertainty Risk Analysis (URA) for Security
  - New Tools
    - Adversary/Defender Model and Grammar
    - Plausible Threat Envelope
    - Linguistic Evaluation with Belief/Plausibility

Sandia National Laboratories

Uncertainty Risk Analysis for Security: New Tools

The Concept:

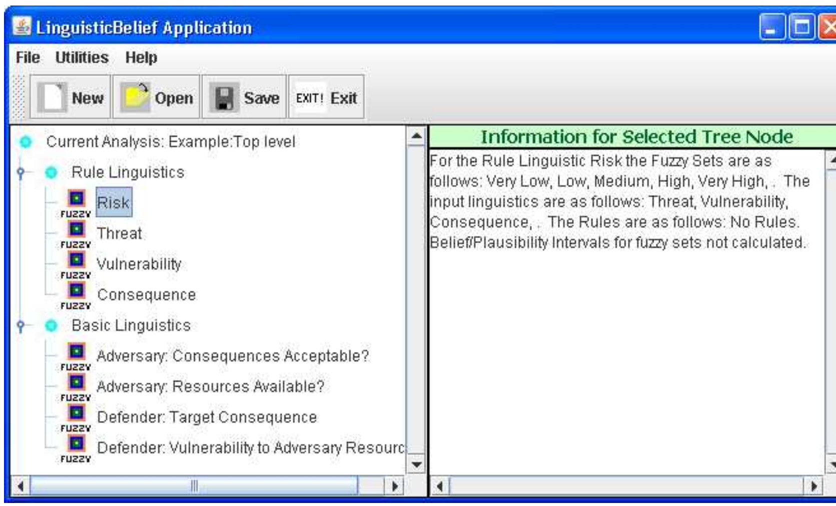
Adversary Defender Interaction Model



The Software Tool:

Linguistic Reasoning with Uncertainty

- Fuzzy Sets
- Approximate Reasoning
- Belief/Plausibility



Sandia National Laboratories