An Assessment Methodology, Models For National Security Systems

Jennifer Guild, University of Idaho

The Model Methodology

- Provides an objective characterization of the system, not a checklist or grade
- Complementary to existing methodologies
- Provides mechanisms to map system evidence to mathematical models to represent assessment findings
- The models, and the results they yield, must be simple enough for non-computer scientists, non-mathematicians to understand because they provide a level playing field of understanding for those that implement them, as well as those that interpret their results
- Each stage correlates to the progression of the assessor's exposure to the system
  - Initial Exposure
  - System familiarization
  - Continuous Review
  - Assessment
  - Data correlation (Evidence to models)
- Each assessment is individualistic, so the number of stages will vary
- Content of the models will evolve from generalized to specific as the assessment progresses

Models

- $(V_{T1})_n$ and $(V_{O1})_n$ represent the set of technical and operational environment vulnerabilities for system s1 in state *n,* then:

$$(V_{S1})_n = (V_{T1})_n \cup (V_{O1})_n$$

- Threat (TR) is some combination of threat source (TS), it's capabilities (TC) with it's motivation(s) (TSM)

$$(TR_{S1})_n = TS_{OrgCrime} \times TSM_{Financial} \times (TC_{LevelOfExpertise})_{Sophisticated}$$

- Probability (P) that an attack will occur with some level of success and certainty

$$(P_{S1})_n = PA_{AlmostCertain} \times PS_{HighlyLikely} \times PC_{HighlyCertain}$$

- An attack vector (AV) is a physical mechanism or vector through which a threat source may exploit a vulnerability

$$(AV_{S1})_n = (AV_{O1})_n \cup (AV_{T1})_n$$

- An impact (I) is the variable result of a threat exercising an exploit against a vulnerability via an attack vector

$$(I_{S1})_r = TR_{AdversaryState} \cup V_{SomeVulnerability} \cup AV_{Internet} \cup (PA_{HighlyLikely} \times PS_{HighlyLikely} \times PC_{HighlyCertain})$$

- Risk (R) is the probability of threat source(s) with the capability of exercising an attack vector to exploit a vulnerability for a specific motivation, the probability of success of that attack, the certainty of the knowledge

$$R = (TS \times TC \times TSM \times PA \times PS \times PC \times AV \times V)^{+} \cup I^{+}$$

Additionally

- An operational environment is a situational instance or state, which reflects a physical characterization of the operational environments
- The use of the models increases objectiveness/explicitness, repeatability, and knowledge of system robustness from assessor to risk acceptor, as well as assessor to assessor
- Threats and probabilities are modeled together to represent their direct relationship
- The probability of attack models describe a threat source's desire to attack
- An asset's value is variable and based on perception:
  - Perceived importance to the mission
  - Perceived importance to the adversary
  - Our ability to replace asset
  - Time