Insider Threat Mitigation Framework

Student: Simon Slobodnik
Advisors: Victor Raskin, Melissa J. Dark

Background
In military cyber operations, Mission Oriented Risk Design Analysis (MORDA) [Buckshaw et al 2005] is used to carry out risk assessment of adversary action. MORDA has been used in operations since 1999 in various missions. It is a systemic and comprehensive model for risk, vulnerability and cost assessment.

Methodology of such scope is lacking in the world of insider threat mitigation. Mechanisms exist to detect and sometimes predict insider threat. However models and the scope of MORDA are not used with insider threat in mind. Events that lead to an insider becoming malicious are rarely viewed as deterministic because full information is not available for computation. Therefore identifying an individual as “high risk” in terms malicious activity has historically fallen to humans rather than any automated system.

Proposed Approach
MORDA in conjunction with a Reasoner that is based on a Dynamic Bayesian Network (DBN) as used by Greitzer et al (2009), and Bishop et al (2010) is an approach to evaluate malicious insider threat comprehensively.

Advantages
This approach assures a systemic approach to evaluating impact of adversary action. Specifically that of a malicious insider. A systemic approach to evaluating impact of adversary action. MORDA has been used in operations since 1999 in various missions.

Factors and Methodology
In the heart of the MORDA system is the Socrates model:
An aggregate set of behaviors known as adversary data, when viewed as nodes in DBN allows to determine the likelihood of an insider becoming malicious. Reasoner model is proven by correlation with human experts.

Bishop’s Unifying Policy Hierarchy (UPH) allows to determine how much access the insider is granted under the security policy. Sensitivity analysis refers to degree of access granted as defined by Bishop’s Unifying Policy Hierarchy. Weights refer to gravity of resources or capability that may be compromised by that individual. Assumptions will draw on results of the Dynamic Bayesian Reasoner for security policy. Sensitivity analysis refers to degree of access granted as defined by Bishop’s Unifying Policy Hierarchy.

Cost-Benefit analysis and budget feed into overall mission impact along with above mentioned factors to ascertain overall mission impact.

References