CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Insider Threat Mitigation Framework

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

Background

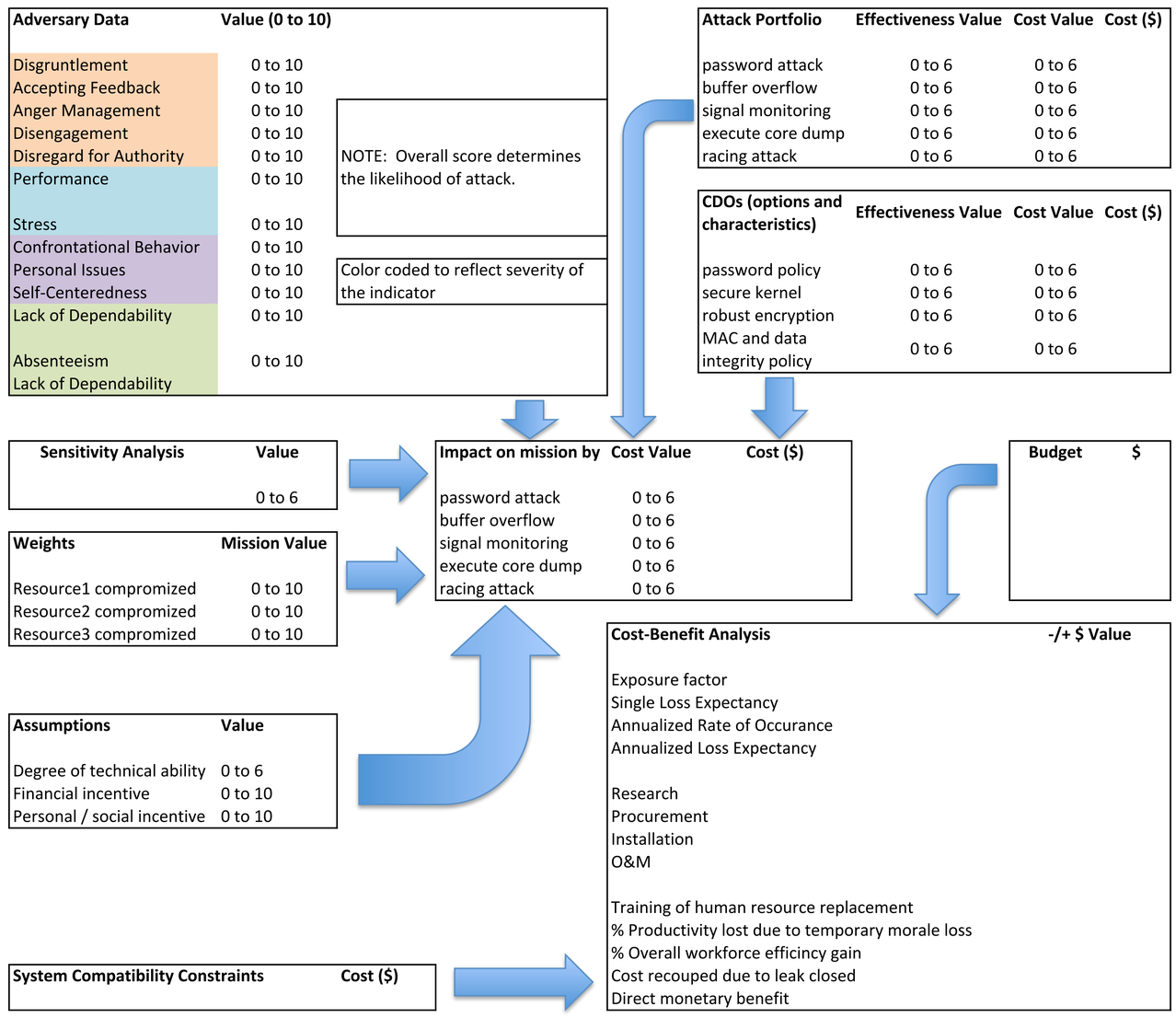
In military cyber operations, Mission Oriented Risk Design Analysis (MORDA) (Buckshaw *et al* 2005) is used to carry out risk assessment of adversary action. MORDA has been used in operations since 1999 in various missions. It is a systemic and comprehensive model for risk, vulnerability and cost assessment.
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's et al (2010) Unifying Policy Hierarchy to be used to evaluate malicious insider threat comprehensively.

Advantages

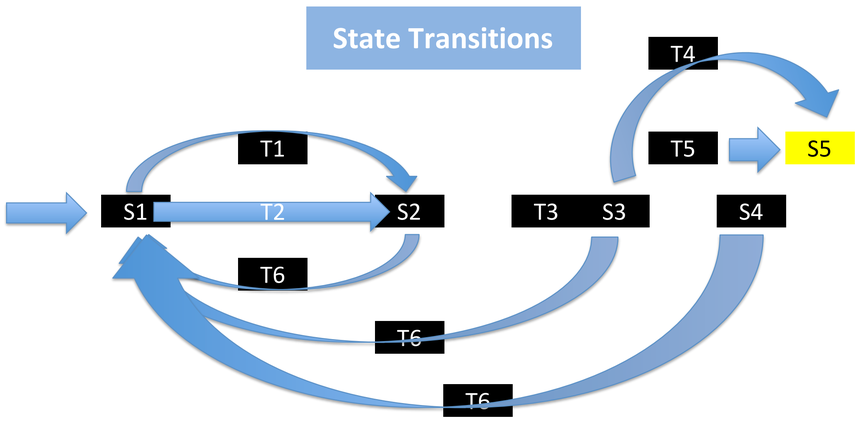
This approach assures a systemic approach to evaluating impact of adversary action, specifically that of a malicious insider. A systemic, approach with costs attached will allow to address the issue of a malicious insider from a business as well as security viewpoint. This will contribute to insider threat detection and prevention mechanisms rather than "after-the-fact" response.



SOCRATES Model (MORDA)

Factors and Methodology

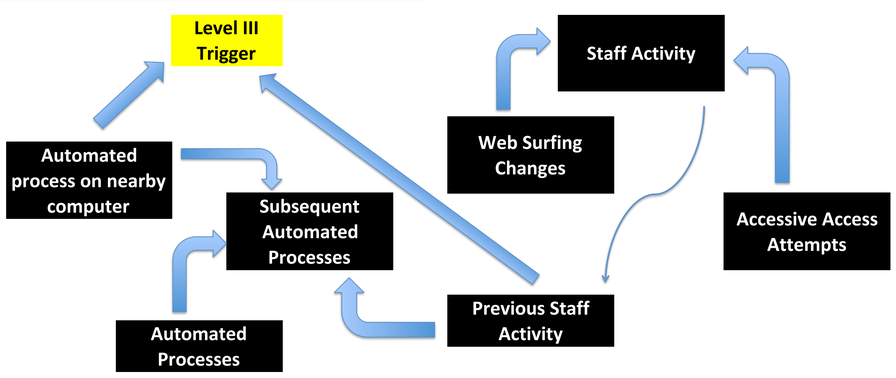
In the heart of the MORDA system is the Socrates model:
An aggregate set of behaviors known as *adversary* data, when viewed as nodes in DBN allows to determine the likelihood of an insider becoming malicious. Reasoner model is proven by correlation with human experts.
Bishop's *Unifying Policy Hierarchy* (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 *personal/social incentive*.
Financial incentive may be calculated by running a financial background check combined with knowledge of the individual such as if he/she has expensive taste or not.
Degree of technical ability is rather straightforward and can be at *least* as high as required by the job function and at most reasonably higher. Depending on personality indicators such as superiority complex.
Attack portfolio is the potential insider's technical arsenal with which he/she can do harm.
CDOs are countermeasures that a specific organization may have in place to thwart a would be attacker.
Cost-Benefit analysis and budget feed into overall mission impact along with above mentioned factors to ascertain overall mission impact.
Weights assigned to each contributing factor are assumed to be unique to particular mission and must be determined by experts.



Employee	Status Indicator	Monitoring Level
Employee111		Nominal
Employee222		Level II
Employee333		Nominal
Employee444		Level III

State	Description
S5	Level II Trigger
S4	Subsequent Automated Processes
S3	Previous Staff Activity
S2	Staff Activity
S1	Start state

State	Description
T5	Nearby Computer enters S2
T4	Automated Processes
T3	Time passes…
T2	Web surfing changes
T1	Excessive access attempts
T6	Lots of time passess…



Dynamic Bayesian Network (DBN), Greitzer et al 2009

Level of Policy	*Domain*	*Description*
Oracle Policy	*S x O x A x E*	What should be authorized, including intentions.
Feasible Policy	*S x O x A* containing system-definable entities	What can be authorized in practice, considering system constraints.
Configured Policy	*S x O x A* containing system-defined entities	What is allowed by the system configuration
Run-Time Instantiation	*S x O x A* containing system-defined entities	What is possible on the system, factoring in any flaws or vulnerabilities.

Table 1 The Unifying Policy Hierarchy. The entities are subjects s ∈ S, objects o ∈ O, and actions a ∈ A. The condition e ∈ E describes additional constraints on the ability of s to execute a on o due to external factors such as intent. The "Run-Time Instantiation" is, strictly speaking, not a policy, but instead a description of what a user can do, whether those actions are authorized or unauthorized; that is, it encompassed unauthorized actions possible due to security flaws.

Unifying Policy Hierarchy - Bishop *et al* 2010

References

Bishop, M., Engle, S., Frinkle, D.A., Gates, C., Greitzer, F.L., Peisert, S., Whalen, S. (2010). A Risk Management Approach to the "Insider Threat".

Buckshaw, D.L., Parnell, G.S., Unkehholz, W.L., Parks, D.L., Wallner, J.M., Saydjari, O.S., (2005). Mission Oriented Risk and Design Analysis of Critical Information Systems. *Military Operations Research, V10 N2 2005*

Greitzer, F.L., Paulson, P.R., Kangas, L.J., Franklin, L.R., Edgar, T.W., Frincke, D.A. (2009). Predictive Modeling for Insider Threat Mitigation. *Pacific Northwest National Laboratory.*

CERIAS®

Discovery Park e-Enterprise Center