A Quantitative Model for Security Risk Management in Information-Technology Intensive Organizations

Jeffrey Mounzer
Stanford University

Tansu Alpcan
Deutsche Telekom Laboratories

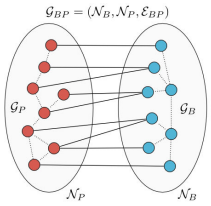
Nicholas Bambos
Stanford University

Introduction

Security risk management (SRM) is becoming increasingly important in areas related to information technology (IT), such as telecommunications, cloud computing, and banking information systems. Most approaches to SRM currently used in industry are relatively ad hoc and qualitative in nature. We present a systematic quantitative framework for SRM called Risk-Rank, which integrates risk modeling, assessment, and mitigation through the mathematical techniques of diffusion processes over graphs and Markov Decision Processes. Approaching risk management in this way can shed light on the complex interconnected nature of security risks across the components of an IT organization, providing decision-making support to the risk manager.

Dependency Model and Risk Diffusion

- The three key factors in security risk management are
  1. Business units/organizational assets
  2. Security threats/vulnerabilities
  3. People
- To model the relationships between these factors, we use regular and bipartite graphs.
  - Regular graphs model intradependencies, such as the relationships between people.
  - Bipartite graphs model interdependencies across these factors, such as relationships between business units and people.



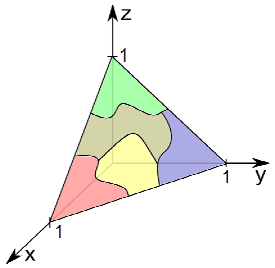
- Using the mathematics of diffusion processes, we can estimate the short and long term relative risk distributions across nodes in these graphs. This allows us to compare, for example, the amount of risk faced by a particular business unit compared to all other business units.
- For the nodes in a graph Y, the vector $\mathbf{v}^Y(t)$ gives the proportion of risk on each node at time t, and based on how risk can "diffuse" back and forth across the graphs described above, this vector evolves as

$$\mathbf{v}^Y(t+1) = \alpha \mathbf{v}^Y(t)\,\mathbf{H} + \beta \mathbf{v}^Y(0)$$

where $\mathbf{H}$ is a matrix which describes the diffusion.

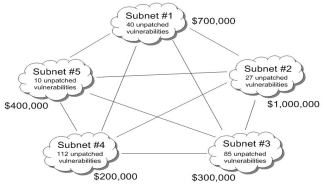
Control of Risk Dynamics

- Based on the dependency model and risk diffusion dynamics, we can proceed to design a control problem, where the goal is to improve the distribution of risk across an organization's business units/assets.
- Our assumptions are:
  - Time is discrete and indexed by t.
  - In each time period, the risk manager can take various actions to combat risk (such as assigning employees to patch computers), and the result of each of these actions is a different modification to the matrix $\mathbf{H}$ for that period.
  - An artificial node called a "risk sink" is introduced among the business units/assets, so that risk which diffuses into that node is considered to have been removed from the organization (to capture absolute reductions in risk).
  - Risk cost accumulates over time. In each time period, the risk cost is the proportion of risk on each node multiplied by that node's value, summed over all the nodes in the organization.
- Now, we can structure a Markov Decision Process (MDP) which advises the risk manager which actions to take in order to optimally reduce risk cost over time. The state can be taken to be the value of the vector $\mathbf{v}^Y(t)$, but this causes two problems:
  1. In practice, *observability* is an important issue – how is the risk vector estimated? It is more common to quantize risk into levels such as "High" or "Medium."
  2. It makes the state space continuous (the probability simplex), which is typically intractable for MDPs.
- Therefore, we partition the probability simplex into *risk regions* to discretize the state space. This is visualized in the figure below.

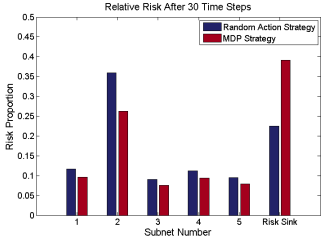


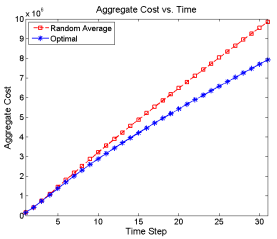
Numerical Example

- Suppose that we have subnets in an organization which require patching, and that only one of them can be worked on at a time (due to a limited number of workers). Costs are incurred if a subnet is compromised by an attack.



- The figures below depict the differences between using the MDP control strategy and choosing actions at random, for a specific set of numerical parameters.





Conclusions

- Quantitative modeling techniques such as Risk-Rank can provide significant insights for risk managers.
- By utilizing bipartite graphs and diffusion processes to model dependencies among risk factors, the risk state of an organization can be quantified.
- Risk managers can influence the risk diffusion process to minimize risk costs over time. Markov Decision Processes can be used to find optimal strategies.

Acknowledgements

We thank Deutsche Telekom AG for their continuing support of this research.