

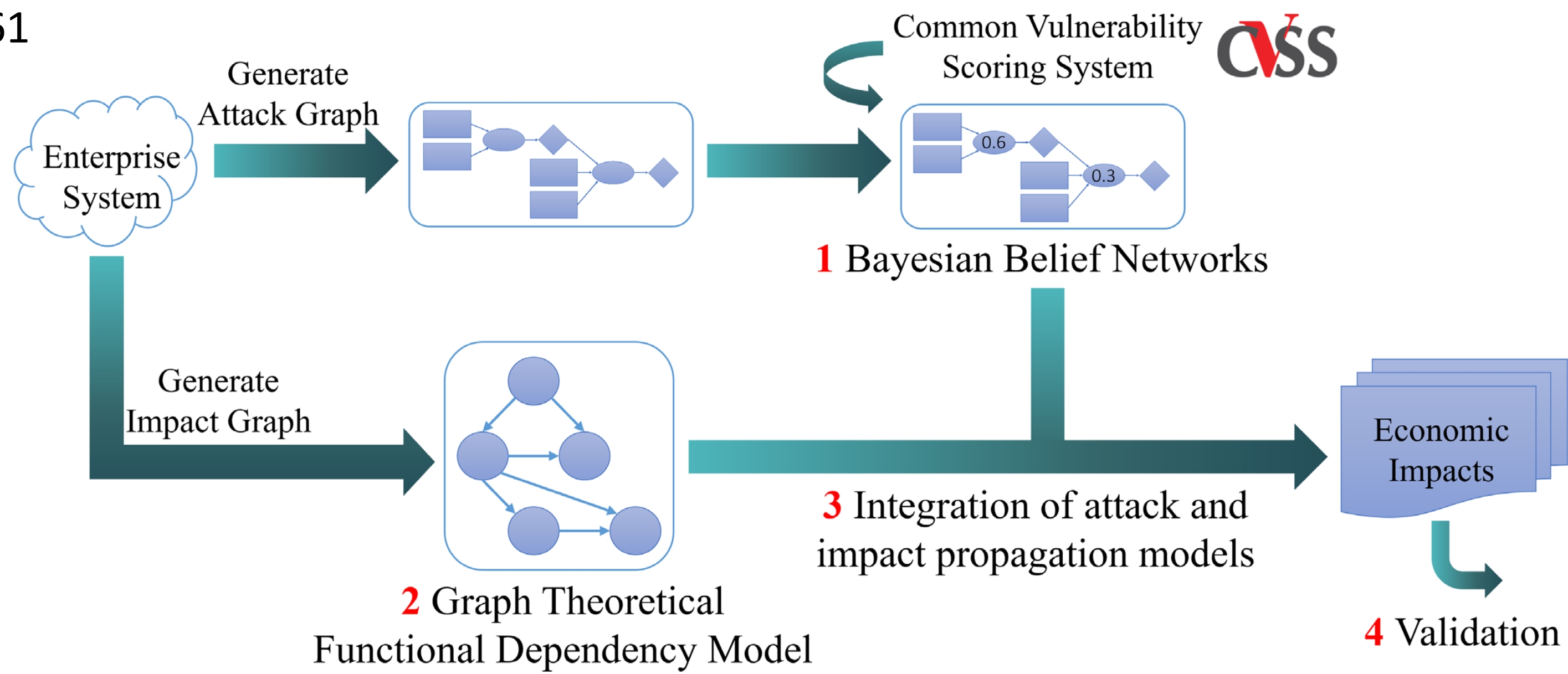
CRII: SaTC: Graph-based Probabilistic Cyber Risk Modeling



Unal Tatar, University at Albany – State University of New York

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1948261

Award ID#: 1948261



The **goal of this research** is to build a probabilistic quantitative cybersecurity risk analysis model to relate asset-level risk to organizational-level risk and supply chain level risk. In this risk analysis method, we will consider the cascading impacts through internal (i.e., within and among asset, service, and business process layers) and external (supply chains) dependencies of an organization.

This project utilizes probabilistic attack graphs, which are based on known vulnerabilities in computer software and network topologies, assessed using the Common Vulnerability Scoring System (CVSS).

The dynamic risk assessment capabilities are augmented in the attack graph using Bayesian Belief Networks.

Broader Impacts are intrinsic to the decision making, as well as the risk management and resilient system design in cybersecurity. This model will also result in the creation of a common language between senior level decision makers and technical experts, and eventually a more effectual risk communication.

Broader Impact on Education
Collaboration with the Girls Inc. – recruited high school interns for summer, and PI participated in Girls Inc. meetings to talk about the research in cybersecurity.



Scientific contribution of the project to the field is to improve the existing attack graph methodology and impact propagation methodology and integrating these two approaches to provide a holistic method for risk management. In the developed model, we calculate the risk by considering the likelihood using the vulnerability scoring and probabilistic attack graph methodology and the impact on the business processes by computing the level of dependency among the assets, services, and business processes.

A graph-theoretical functional dependency model is also developed to analyze the ripple effects of cyber-attacks from missions to failures in supply-chains. Simulations and sensitivity analysis are conducted on a smart grid testbed to validate the developed risk analysis model as smart grids and conventional computer networks exhibit several similarities.

Students employed:

- 3 graduate students
- 2 REU students
- 4 undergraduate students
- 6 high school students

13 products include:

- 4 journal articles
- 3 juried conference papers
- 5 other presentations
- 1 dissertation