

Compound Exposure Analysis

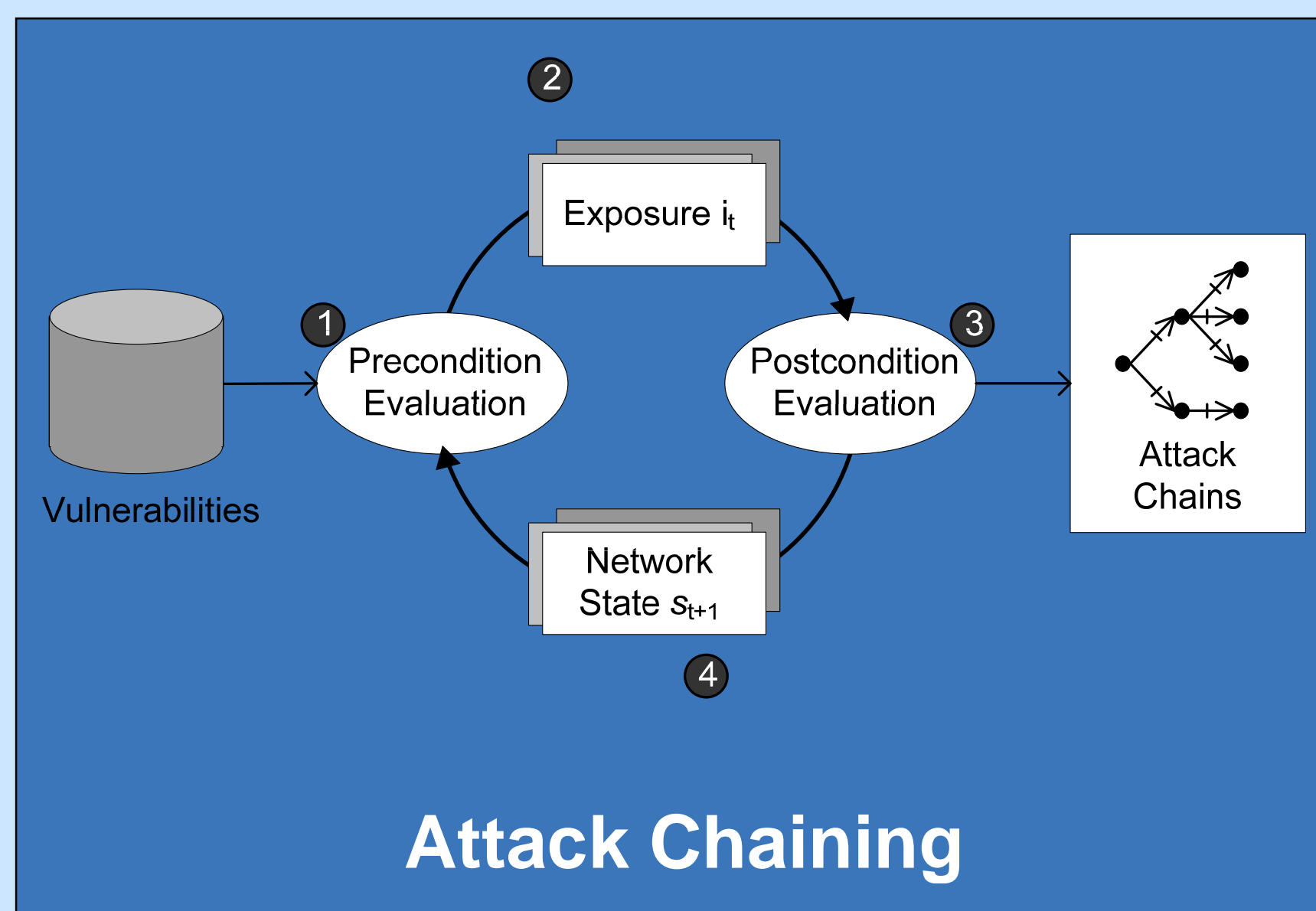
John Hale, Institute for Information Security, The University of Tulsa

www.isec.utulsa.edu



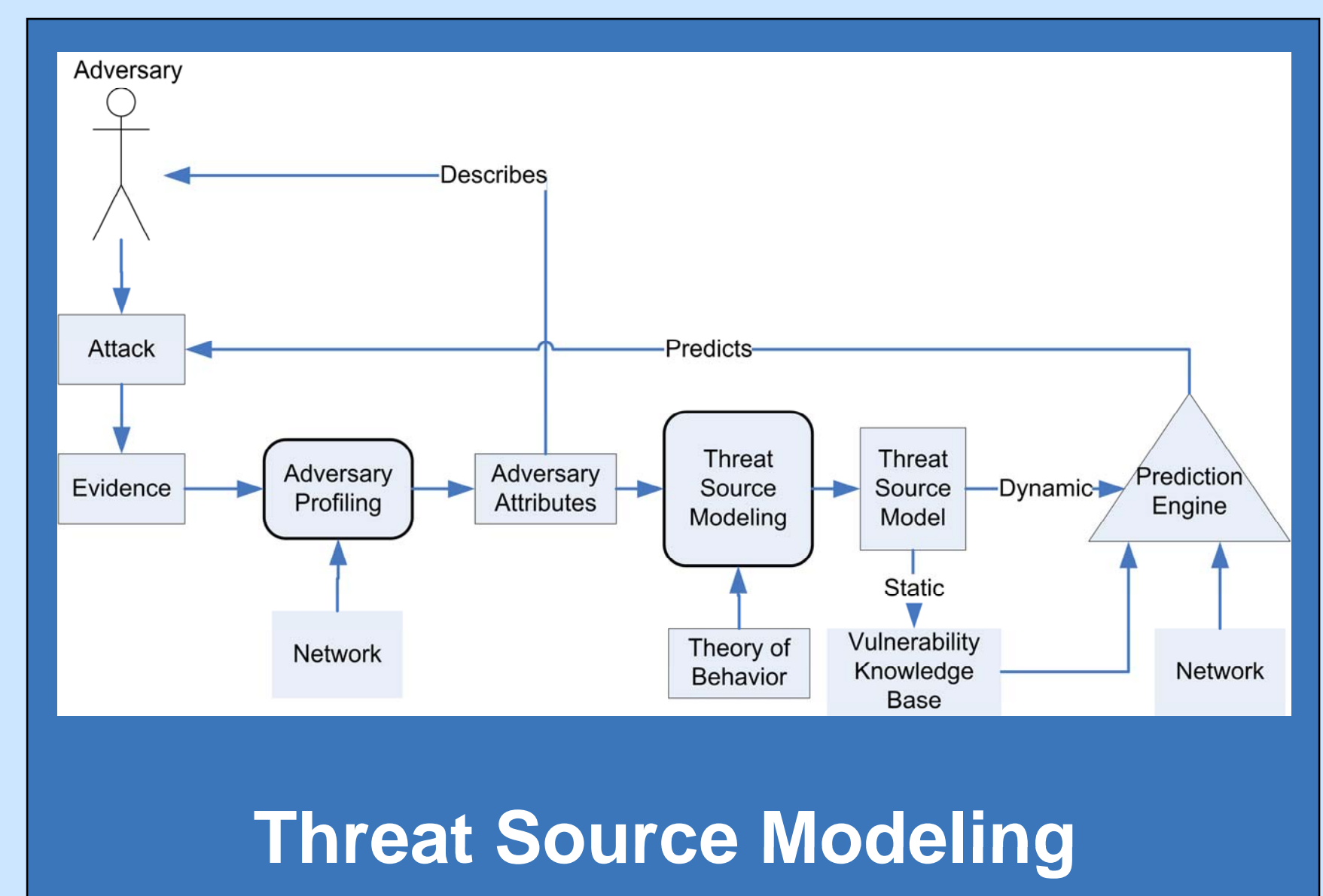
Attack Chaining

Attack chaining links functional vulnerability specifications of exposures over a network model to create a graph of multi-stage attacks. The primary challenge is *scalability* over realistic network models.



Threat Source Modeling

Threat source modeling maps adversarial profiles to heuristics for shaping and optimizing attack graphs. Profiles may relate skill, resources, risk tolerance or other characteristics.



Approach and Impact

Approach

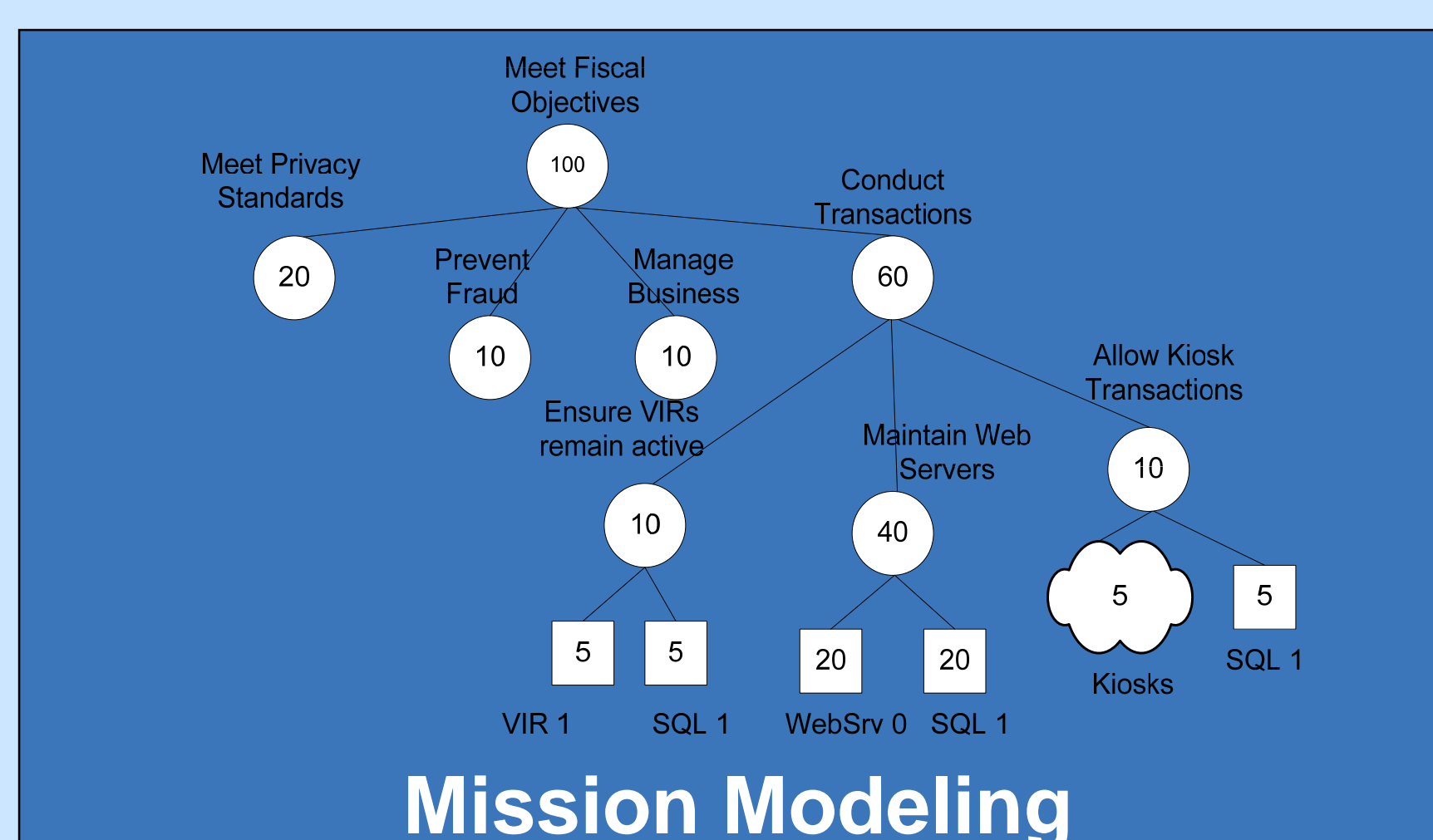
- Integrate formal enterprise models within risk management framework
- Heuristical approach to accelerating attack chaining

Research Impact

- Bridge between business and IT domains of IA
- Practical attack graph analysis
- Potential for RT attack mgmt

Mission Modeling

Mission modeling identifies the role of IT assets in organizational mission to determine asset criticality and sensitivity.



Future Work

- Acceleration techniques for scalable attack chaining
- Network model acquisition solutions
- Expansion and evaluation of threat models.
- Real time attack management prototype

