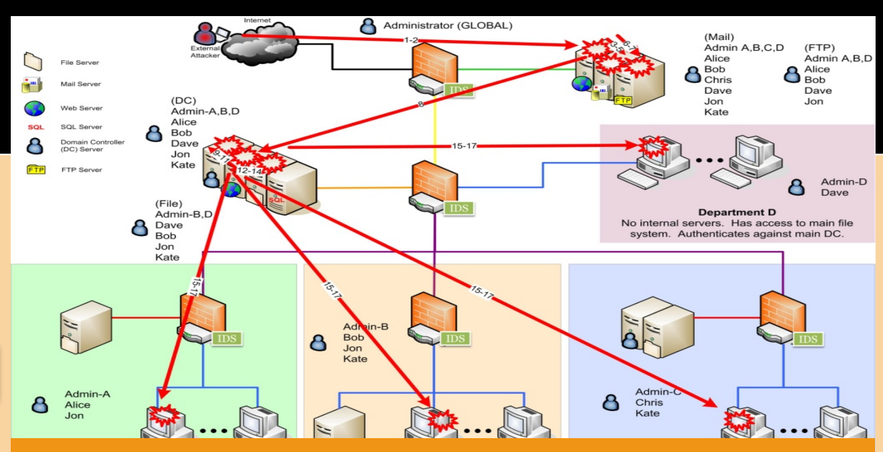
Automating Attack Strategy Recognition to Enhance Cyber Threat Prediction

S. Jay Yang, M. Kuhl, B. Stackpole, D. Johnson, & E. Rantanen

Rochester Institute of Technology

<u>Research Goal</u>: Recognizing emerging cyber attack scenarios with incomplete, noisy, and potentially deceptive data in early attack stages can help provide predictive capability for cyber situation awareness and threat assessment. The goal of this research is to develop a system that can synthesize critical and likely cyber attack models and scenarios in a timely manner as observables emerge.



Observables of malicious activities

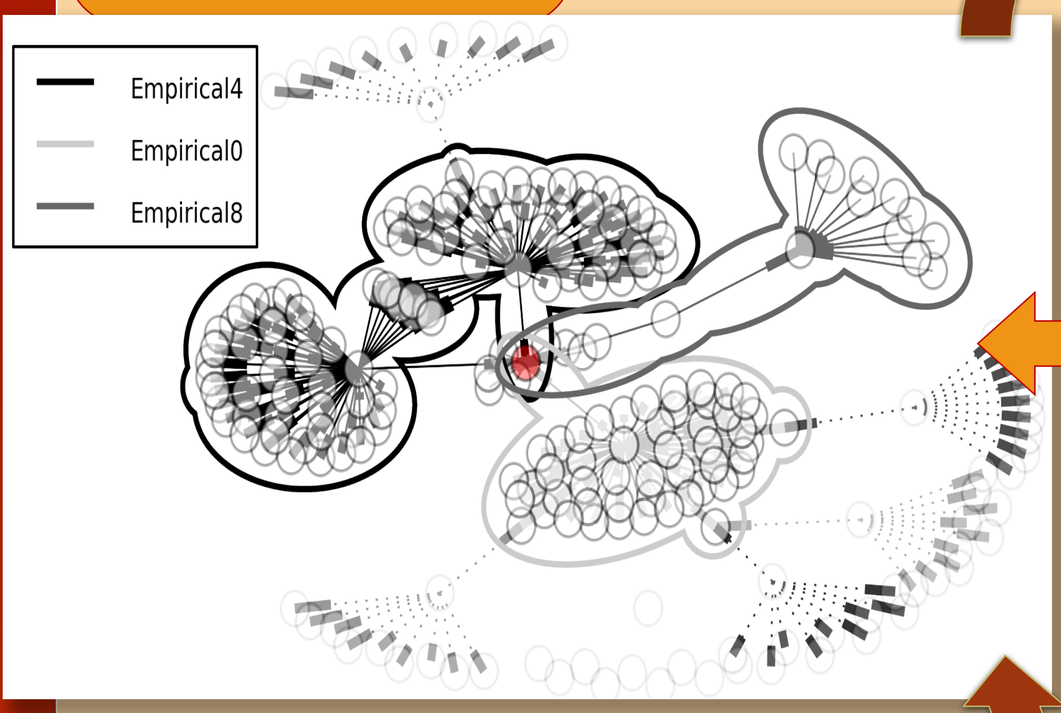
ASSERT

Attack Strategy Synthesis & Ensemble Prediction

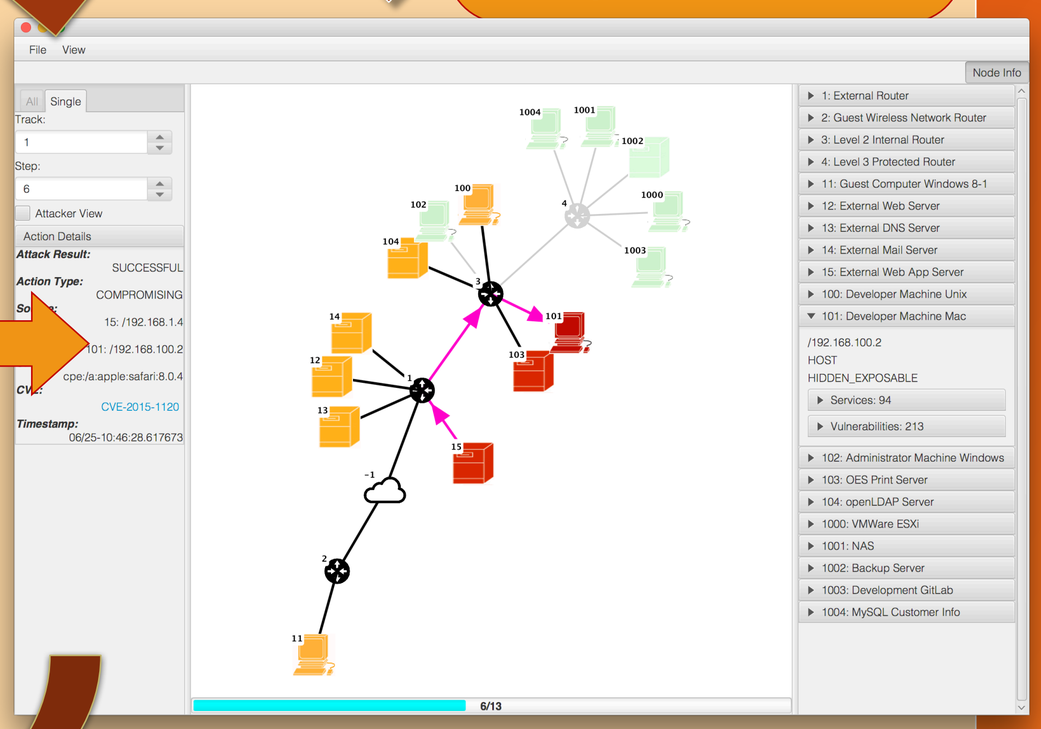
CASCADES

Cyber Attack Scenario & Network Defense Simulator

Salient Features & Early Indicators



Interdisciplinary study of hacker behaviors



Critical & Likely Scenarios

ASSERT:

- Semi-supervised learning to iteratively classify collections of observables, as defined in Attack Social Graph (ASG), to attack models.
- Bayesian classifier with empirical models generated based on optimal clustering index and dynamic prior.
- Features include:
  - Histogram of malicious action types, as exhibited by, e.g., CVE/CWE/CPEs.
  - Transition patterns of malicious actions.
  - Spatial relations as exhibited in the ASG.
  - Attack intensities.

CASCADES:

- Monte-Carlo simulation (w/ important sampling) to generate attack scenarios subject to attacker behaviors & network defense configurations.
- Attacker Behavior: Intent + Opportunity + Capability + Preference
  - Attacker accumulates knowledge and moves in cyber kill chain stage over time.
  - COI derives plausible actions, while Preference choose each executed action.
- Scenarios reflect emerging attack patterns/goals, effective of cyber defense, and impact on network mission.

Interested in meeting the PIs? Attach post-it notes below!

The 3rd NSF Secure and Trustworthy Cyberspace Principle Investigator Meeting
January 9-11, 2017
Arlington, Virginia