Automating Attack Strategy Recognition to Enhance Cyber Threat Prediction – Yang @ NetIP @ RIT

Challenge:

How to recognize emerging critical cyber attack scenarios early on with incomplete, noisy, and potentially deceptive observables?

Scientific Impact:

The predicted emerging attacks can enhance cyber SA, alleviate unknowns, and lead to more timely and effective cyber defense.

Observables of malicious activities

Salient Features

ASSERT

Critical Scenarios

CASCADES
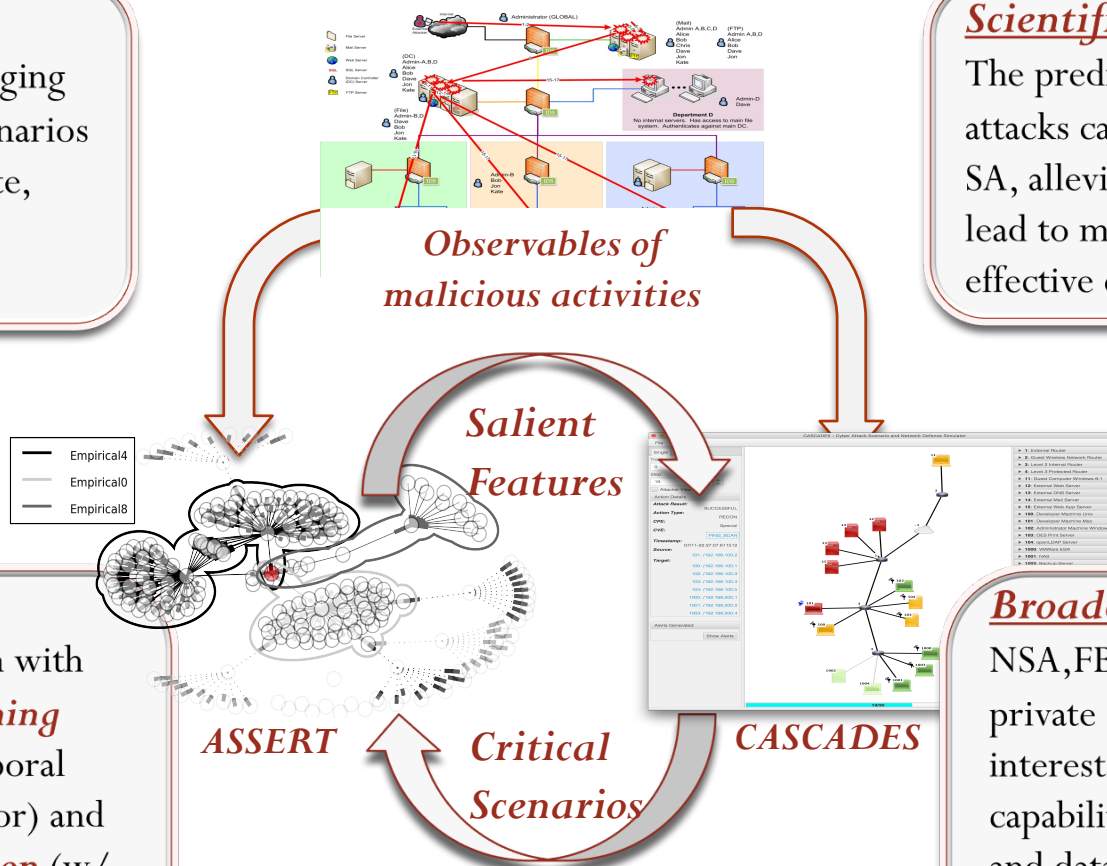
Solution:

An integrated approach with *semi-supervised learning* (w/ novel spatial/temporal features & dynamic prior) and *Monte-Carlo simulation* (w/ important sampling) of attack behaviors* to reveal critical emerging scenarios.

*Interdisciplinary study of hacker behaviors.

Broader Impact:

NSA, FBI, DHS, AFRL & private sectors have shown interests in such predictive capabilities. Prototyping and data collection are underway. The project has involved 13 students, including 4 women and 2 hard-of-hearing students.