

# GMNI: Graph Methods for Network Investigation

Thomas E. Daniels, Iowa State University

<http://home.eng.iastate.edu/~daniels>

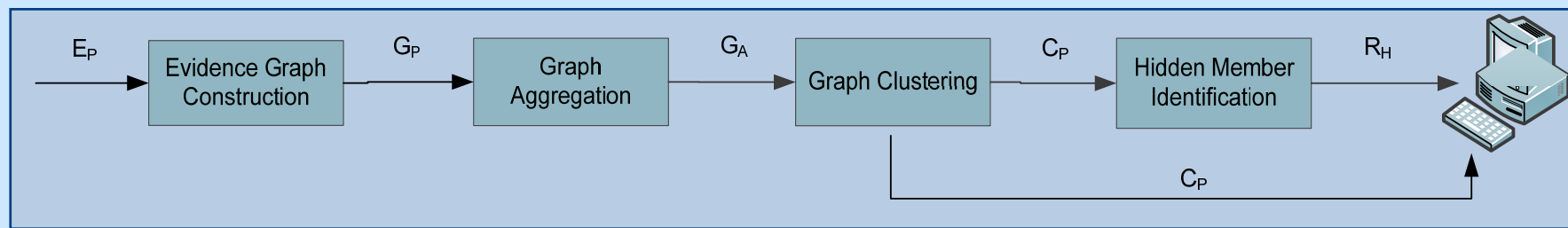


## Network Investigation

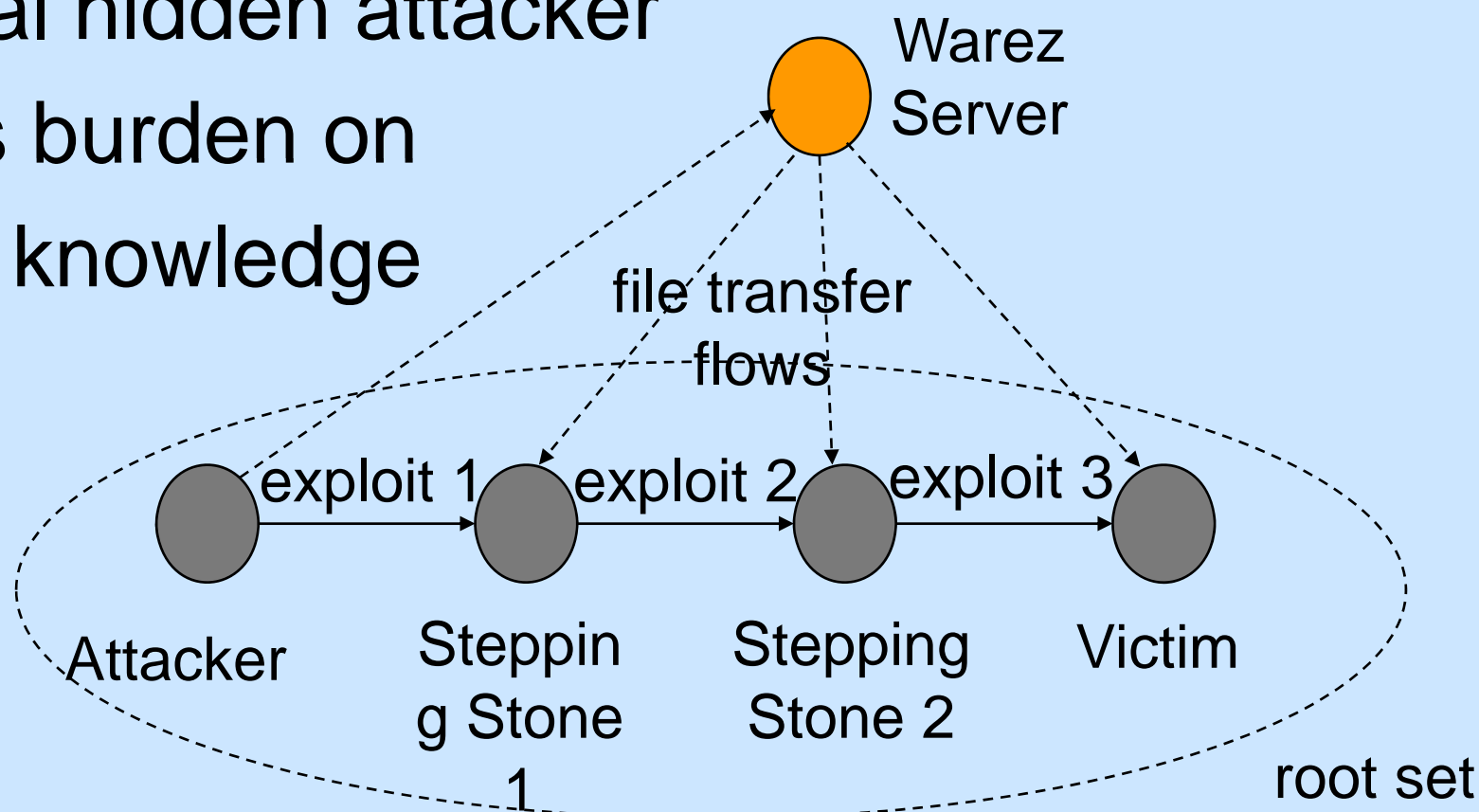
The significant limitations on most existing graph approaches for alert correlation:

- Heavily rely on prior knowledge of network vulnerabilities
- Provide no means to deal with stealth activities

## Our Solution



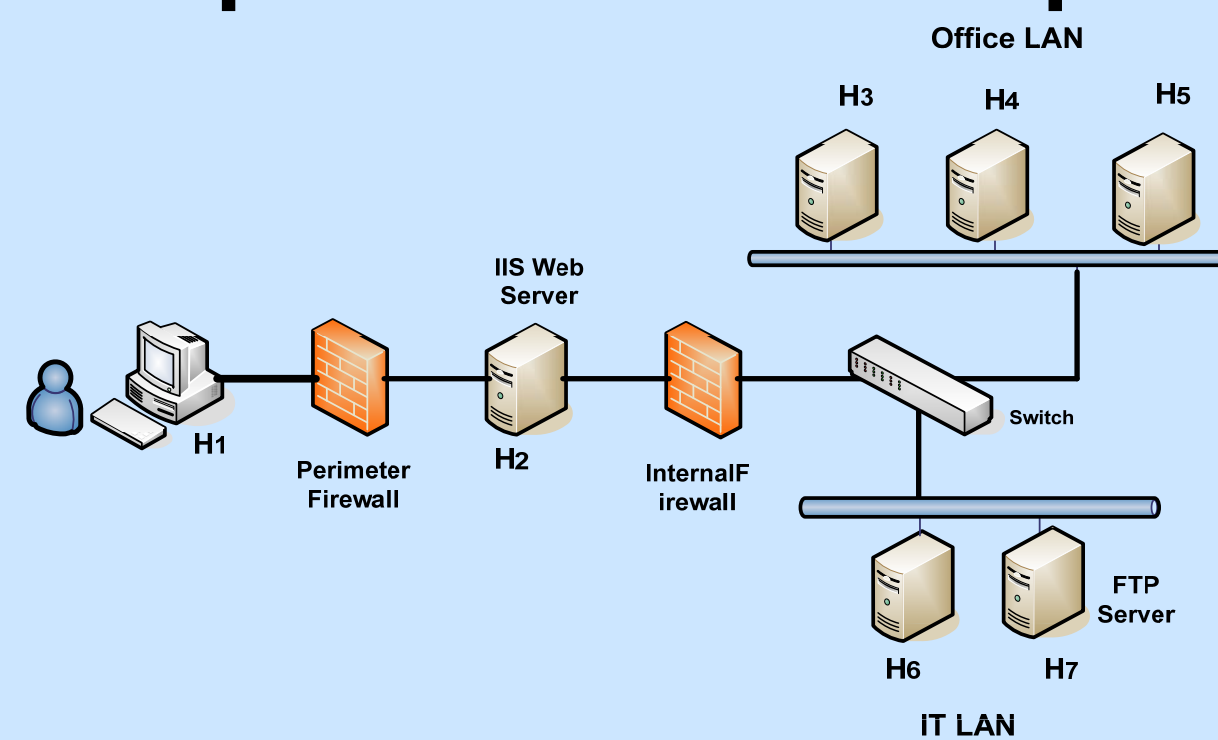
- ✓ Integrate primary and secondary evidence
- ✓ Apply the personalized Pagerank to rank potential hidden attacker
- ✓ Less burden on expert knowledge



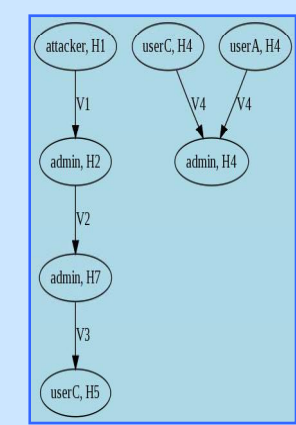
## Issue with Attack Graphs

Attack graphs have been widely proposed for network security analysis. However we discover that many wide-spread inherent vulnerabilities have been left out for analysis. The attack graph for any realistic environment are by necessity so dense and the utility is quite limited.

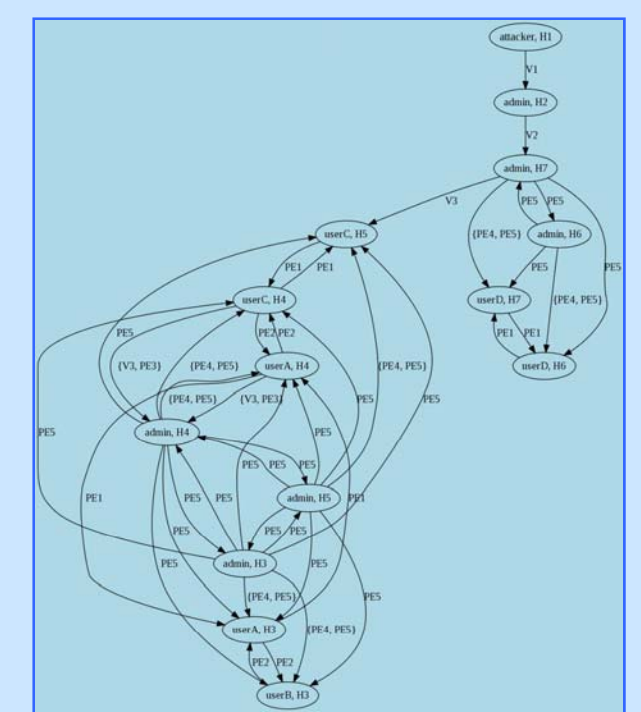
## Simple Network Example



initial:



closure:



Step	Initial	Closure
# Max States	3	13
# Edges	4	41
Density	0.026	0.263

## Approach and Impact

### New approach

- Pagerank and spectral analysis of intrusions
- Formalizing inherent vulnerabilities to determine of the density effects on attack graph

### Research Impact

- Well founded methods for network investigation
- Reconsidering the results and utility of attack graphs

### Network Investigation

We propose a novel graph based approach for network intrusion. We apply the spectral clustering methods to extract natural clusters from primary evidence graph as candidates of coordinated attack scenarios. Clusters are further used in identifying hidden members from the secondary evidence. We use the personalized Pagerank algorithm to rank the potential hidden members with respect to their relative importance in the secondary evidence graph.

### Issues with Attack Graphs

We present our initial study of inherent vulnerability on attack graph. We formally define a set of privilege expansion vulnerabilities and associated rules for adding edges to attack graphs. We show that the resulting graphs are very dense for many network configuration. We then show that dense attack graphs reduce the utility of many analysis methods presented to date.