

# Network Benchmarks for Security Analyzers

Ethan Singleton, Stephen Tyree, John Hale  
University of Tulsa, Institute for Information Security

# Performance Analysis of Security Analyzers

- **Attack graphs**
  - Identifying compound exposures in networks and systems
  - Generation and analysis is inherently complex
- **Performance: Not all about  $O()$** 
  - Scalability is important, but theoretical results do not guarantee good performance
- **Current tools/techniques are measured inconsistently**
  - Each evaluated under its own network model
  - Comparative performance analysis is therefore difficult
- **Goal: Comparing apples to apples**
  - Standard measures
  - Reproducible results

# Security Analysis Benchmark Design

- Canonical network architectures
  - Flat network
  - Simple enterprise network
  - Expanded enterprise network
- Host architecture
  - Core attributes and services
  - Customizable application base

## Future Work

- **Extensions**
  - Addition of permissions into host models
  - Trust and logical relationships
- **Tools**
  - Network model construction toolkit (benchmark compliant)
  - Online repository of attack graph tools, models and results
- **Adoption**
  - Integration into NOVA
  - BOF on Benchmarks @ Attack Graph Summit