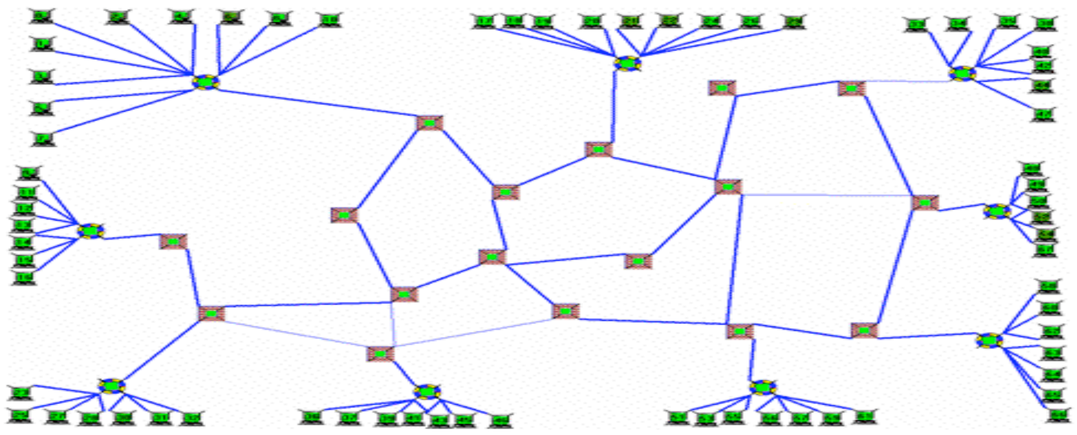
CERIAS

(EMIST)

Evaluation Methods for Internet Security Technology

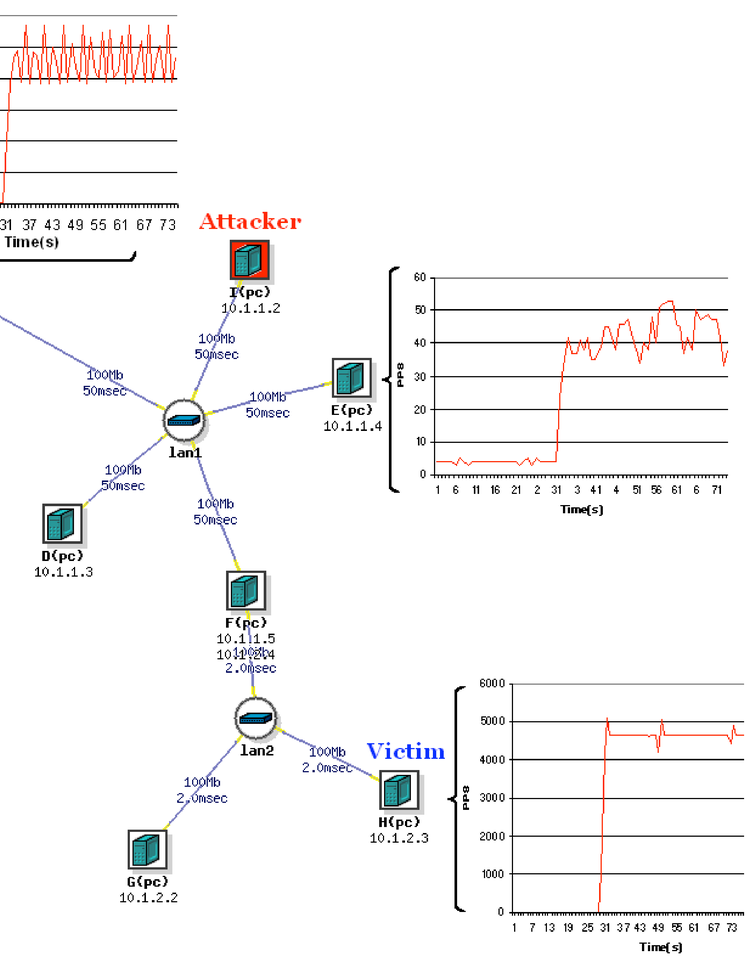
PI: Catherine Rosenberg, Co-PI: Carla Brodley, Sonia Fahmy



What is EMIST?

- A National Science Foundation and a Department of Homeland Security funded project to develop scientifically rigorous testing frameworks and methodologies for representative classes of network attacks and defense mechanisms.
- In conjunction with DETER (Cyber DEfense Technology Experimental Research), build an enduring realistic testbed for security research to support national-scale experiments on emerging security research and advanced development technologies.

EMIST@ Purdue



Students:

Roman Chertov
Bryon Gloden
Chris Kanich
Jacky Lee
Yu-chun Mao
Kevin Robbins
Rupak Sanjel

Objectives

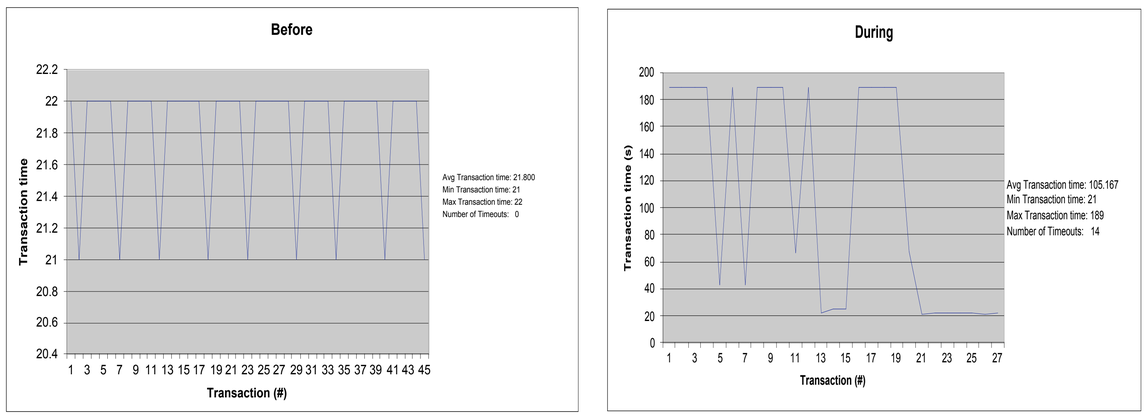
- Provide an experimental infrastructure and rigorous scientific methodologies for developing and testing next generation cyber security technology.
- Conduct research and experiments in three areas: worm propagation, denial-of-service attacks, and routing infrastructure attacks.
- Create, operate, and support a researcher-and vendor-neutral experimental infrastructure open to a wide community of users.
- Yield deeper understanding of how different attacks have, and will, affect the Internet and its users.
- Impact research directions in security, testing, data acquisition, data processing and visualization.

Partner Organizations

USC Information Sciences Institute · Berkeley University of California · PennState · McAfee · Sparta · ISI · SRI International

Preliminary Experiments

- Proposed techniques for scale-down and automatic generation of cyber security experiments.
- Determined limitations of existing simulation and emulation platforms (NS and Emulab) in handling such experiments.
- Investigating the modeling/characterization and the simulation/emulation of distributed denial of service attacks.
- Currently focusing on different research and commercial intrusion detection mechanisms.
- Designing attack, automation and measurement tools.



Transaction time in the client before and during an attack burst on the server (based on the scenario above)

PURDUE UNIVERSITY · CERIAS · Discovery Park e-Enterprise Center