The Center for Cyber Defenders
Expanding Computer Security Knowledge

SAND2015-5713C

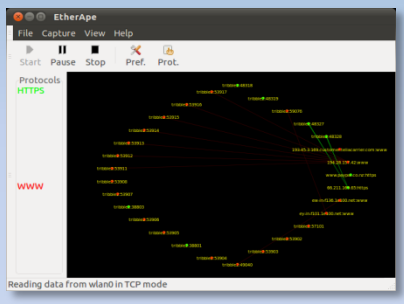
THEARTICLES: TrafficSoup

Lance Chao, Virginia Polytechnic Institute; Khiem Tang, The University of Texas at Austin;
Marcus Dominguez-Kuhne, Albuquerque Academy

Project Mentors: Nick Pattengale, Jon Bradley, Craig Buchanan, Eric Gottlieb, and John Montoya, 5624

Problem Statement:

- Network security research typically involves a Red team, a Blue team, and a test network. However, for cost-efficiency purposes, these test networks often are virtual network simulations rather than physical ones, making it trivial for the Blue team to notice activities and take countermeasures.



Graphic display of network activity using EtherApe.

Objective and Approach:

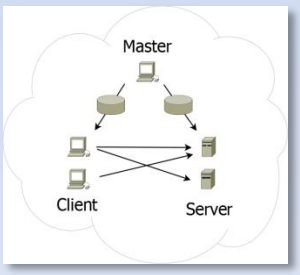
- TrafficSoup is designed to effectively clone the environment of an operational network in order to conduct experiments without causing disruptions on the real network.
- To generate arbitrary traffic,
  - Packet captures (Pcap) of traffic are played over real networks and replayed in the virtual network.
  - Pcaps are dissected and traffic is stored into databases that contain the request/response pair data.
- Virtual hosts are each assigned a role as a client sending requests to virtual servers, or a server sending responses based on what the client sent it.

Results:

- TrafficSoup accurately replays a majority of the traffic seen on a typical network. TrafficSoup has been successfully run on a 66 node virtual network, showing that the system is not only practical but scalable as well.
- Future objectives for TrafficSoup include:
  - The ability to respond to requests not recorded into the database by generating dynamic content.
  - The ability to increase cross-platform compatibility.

Impact and Benefits:

- TrafficSoup is an excellent training aid for both sides of the Cybersecurity team because it provides:
  - The Blue team with realistic background traffic that is typical of real networks.
  - Cover for the Red team to infiltrate the network undetected.
- TrafficSoup helps provide security teams with a realistic, cheap environment to run: simulations, experiments, and Capture-the-Flag events .



TrafficSoup System Communication