Nfsight: Netflow-based Network Awareness

Michel Cukier (with R. Berthier (UIUC), M. Hiltunen (AT&T), D. Kormann (AT&T), and G. Vesonder (AT&T))

Goals
- Gaining situational awareness on large networks:
  - What servers are deployed?
  - Are there rogue services?
- Visualizing network traffic at various granularities

Contributions
- Netflow-based client/server detection
  - Heuristics and Bayesian inference are used to generate bidirectional flows from Netflow
- Lightweight and easy to deploy
  - Back-end as plugin for Nfsen/Nfdump
  - Web-based front-end developed in PHP and Javascript
- Anomaly detection and automated alerts

Intrusion Detection
- Nfsight enables operators to write anomaly detection signatures and be alerted by email
- Signatures are based on data fields from graphlet structures stored for each IP

Architecture

Dr. Cukier’s Research
- Goal: quantification of computer security
- Empirical studies using all security related data collected on the UMD network
- Research projects examples:
  - Profiling attacker behavior following SSH compromises
  - Analyzing Intrusion Prevention System Event Data
  - Honeypot Architecture for Network Threats Quantification
- PI of NSF REU Site on computer security (collaboration with Women in Engineering)
- Funded by NSF, DARPA, AT&T, Raytheon

Visualization Front-end

Top 20 Scanned Services:

Detection of Scanning Activity: