NETwork Application ID (NETAID)

George Jones

(703) 983-2032 • gmjones@mitre.org

Dr. Neal J. Rothleder

(703) 983-2113• neal@mitre.org

DISA / MOIE

Problem

- **Internet tunnels, encryption, modern web applications (e.g., "AJAX"/Web 2.0) and sophisticated adversaries/attacks (e.g., Botnets, data exfiltration) are putting our networked resources and information at risk.**
- **The threat has evolved and analysis methods have not kept pace – the game has changed**
  - **Adversary use of encryption**
  - **Reduced trust in Doman Name Server (DNS) reliability**
  - **Reliance on use of traditional protocols and port numbers**
  - **Assumption that proxies will not mask one end of a network exchange.**

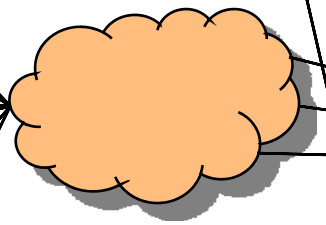
We are losing situational awareness

Background

Current detection methods are broken.

BitTorrent (rotating ports)

Port 80 → http?
App from Google cloud, Akamai...



Who is → unavailable
Packets → encrypted

HELP !!!

Objective: Explore This Hypothesis

MITRE Innovation Program

Network applications and attacks can be identified using Netflow behaviour alone

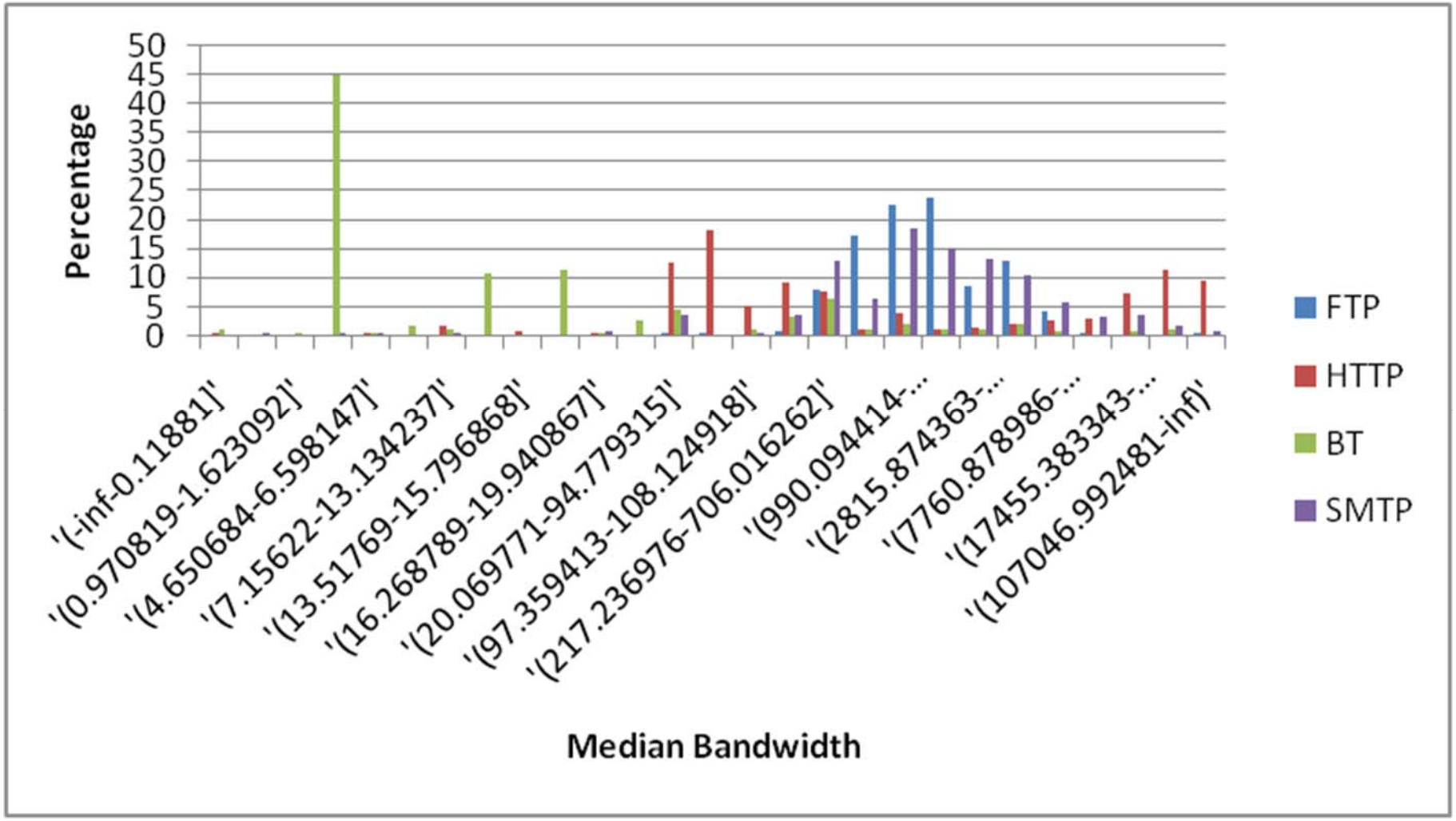
1990	Today	Future
• No encryption • Full packet capture • Destination data reliable • No Server farms/Load Balancers • Users not hiding • Few servers/services	• Some encryption • Some packet capture • Destination data less reliable/available • Server farms/Load Balancers common • Some Users hiding	• Everything Encrypted • Packet capture harder (more bandwidth) • Legal/Social barriers to destination data • Server Farms ubiquitous • More users hiding • Everyone's a server • More P2P

Network Monitoring Challenges

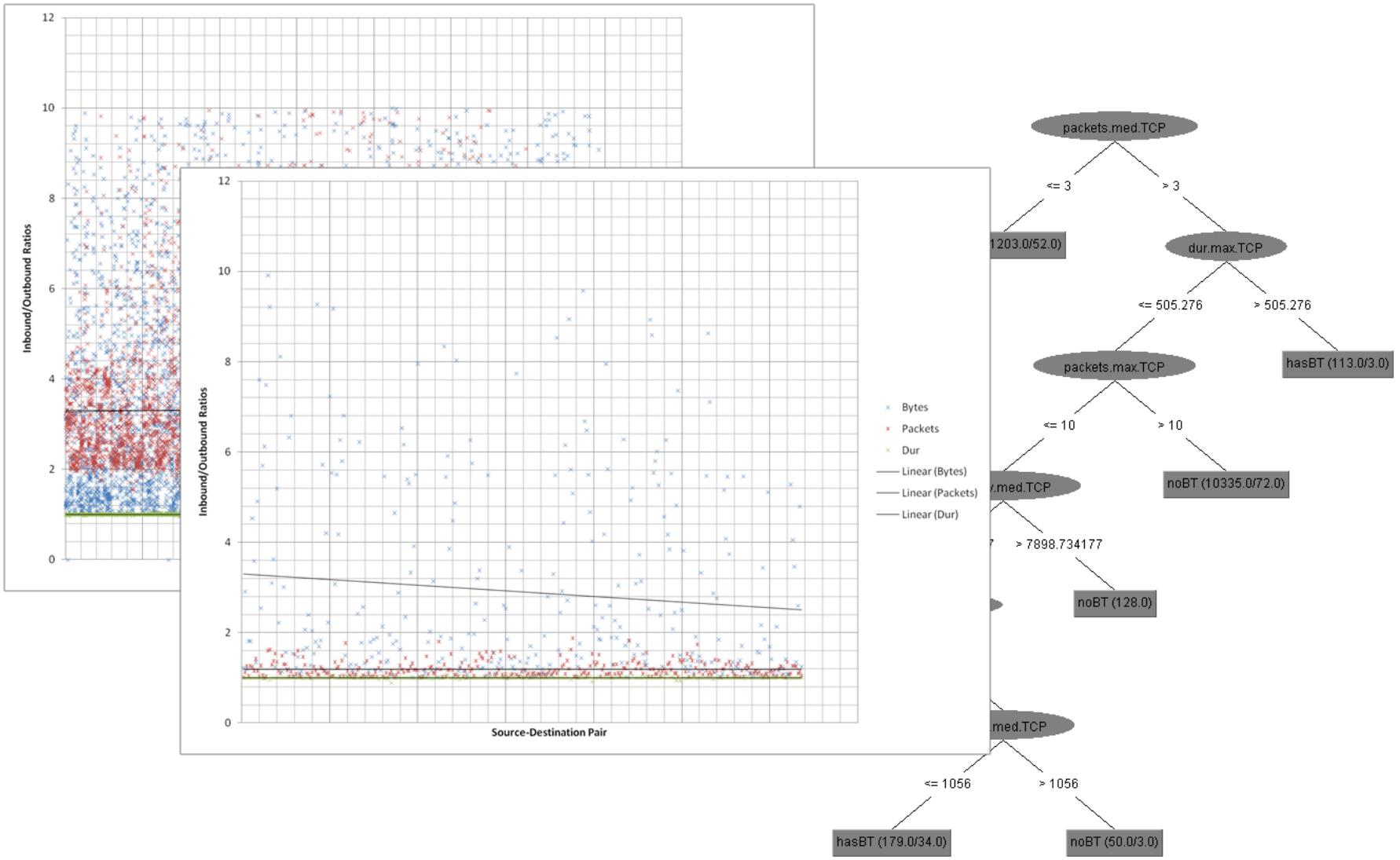
Activities

- Build on work by Collins (2007) in using simple heuristics to identify BitTorrent.
- Exploit a range of data
  - Controlled data on a single host
  - MITRE proxy data
  - CENTAUR/SILK.
- Build data pipeline process to build key attribute descriptions of network flows.
- Apply range of data mining classification techniques to train a model of malicious behavior.
- With infrastructure in place, explore identification of Remote Access Tools (RAT) and Exfiltration.
- Engage with sponsor security analysts as results are available. Use feedback to revisit.

Highlight: Feature Identification



Demonstration



Impacts

- Better Situational Awareness to reduce mission-impacting noise on tactical links
  - Detecting BitTorrent in the presence of proxies
  - Improvements on state of the art
  - Feature identification in progress
    - Tie together with a classifier
    - Test within community.
- Detection of exfiltration and C2 of compromised host by RAT
  - Remote Administration Tool Detection
  - Initial heuristics developed and testing now
  - Positive results with few false positives
  - Potential improvements
    - Coupling with NetSA capabilities (beaconing)
    - Data mining techniques.

Future Plans