Summary

This project is exploring ways to use assistance and information from end systems to improve network performance and security.

Approach

**Collect** information at end systems about network performance, security-related events, etc.

**Report** information to network devices that can take action.

Network operators: Have view of network and direct control over network elements.

Users and end systems: Have direct control over host software and wider view of network traffic.

Real-World Applications

- Defense against unwanted traffic (e.g., spam, phishing, denial of service)
- Network performance diagnosis
- Scalable network monitoring

Application: Spam Filtering with Behavioral Blacklisting

For each sender, SpamTracker:

1. Constructs a behavioral fingerprint of the sender;
2. Clusters senders with similar fingerprints;
3. Filters senders that map to existing clusters of known spammers.

Application: Packet Provenance

Pedigree instruments hosts with a trusted tagger that marks packets with information about:

1. The authority of the process that generated the traffic (ContainerID and optional crypto token)
2. The other processes from which that host has taken input (taint set)

- Tag enables flexible policies (e.g., secure network regions)
- Taint set enables outbreak tracking and possible mitigation
- Prototype: POSIX message queue w/library interposition
- 1.5-4.5x latency overhead. (in-kernel implementation planned)

Feature: distribution of sending volumes across recipient domains
- Spamming IP addresses form distinct clusters
- Each cluster has an average vector that represents that cluster’s “fingerprint”
- At least 15% of spam missed by current techniques receives high score: possible early detection scheme
- Current work: Trial deployment and additional feature analysis