

Automated Worm Detection and Response

Dan Ellis

703-983-5807 • ellisd@mitre.org

MITRE Sponsored Research



MITRE
Technology
Program

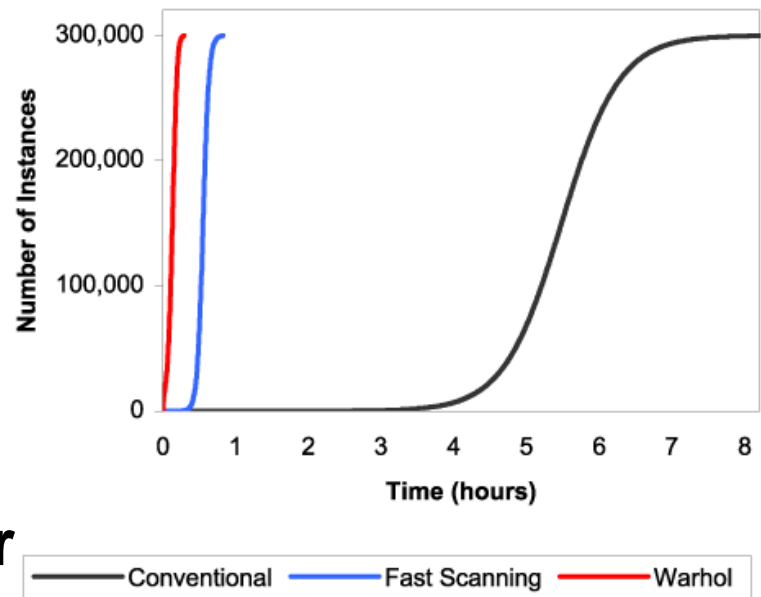
Problem

- **Worms can infect enterprises in seconds**
- **Current intrusion detection and response technologies are not sensitive, accurate, or fast enough**
- **Can worms be detected quickly enough to respond in real time?**
- **Can effective countermeasures be deployed automatically to minimize spread?**

Background

- Worms are *weaponizable*
 - Fast spread!
 - Arbitrary payloads
- Current intrusion detection & response are measured in hours
- Contemporary research focuses on Internet-scale response or perimeter defenses

$$a = \frac{e^{K(t-T)}}{1 + e^{K(t-T)'}}$$



Objective

- **Develop real-time worm detection and response capabilities for enterprise networks**
 - **Develop sensitive and accurate detection capability**
 - **Develop ability to execute realistic, repeatable tests on a *production network***
 - **Evaluate different response strategies**
 - **Transfer technology to vendors**

Activities

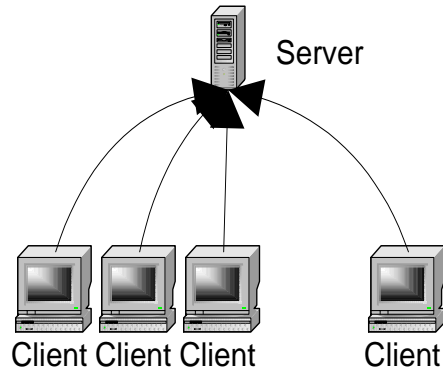
Done

- Evaluated detection accuracy and sensitivity on real-world network in off-line mode
- Developed benign test capability (Message Relay System)

Current

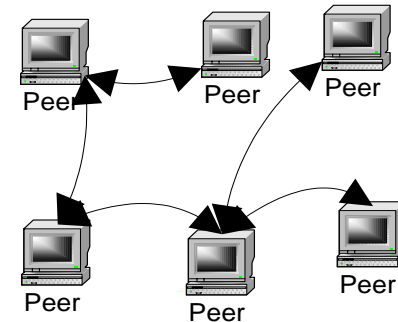
- Evaluating real-time performance
- Developing response strategies
- Transferring technology

Highlight

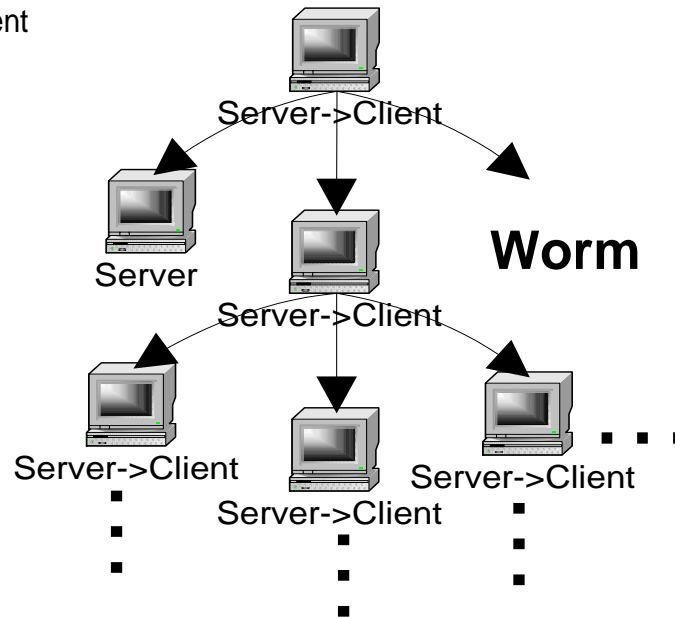


**Normal
Client-Server**

Worm traffic looks
different from other
types of network
traffic

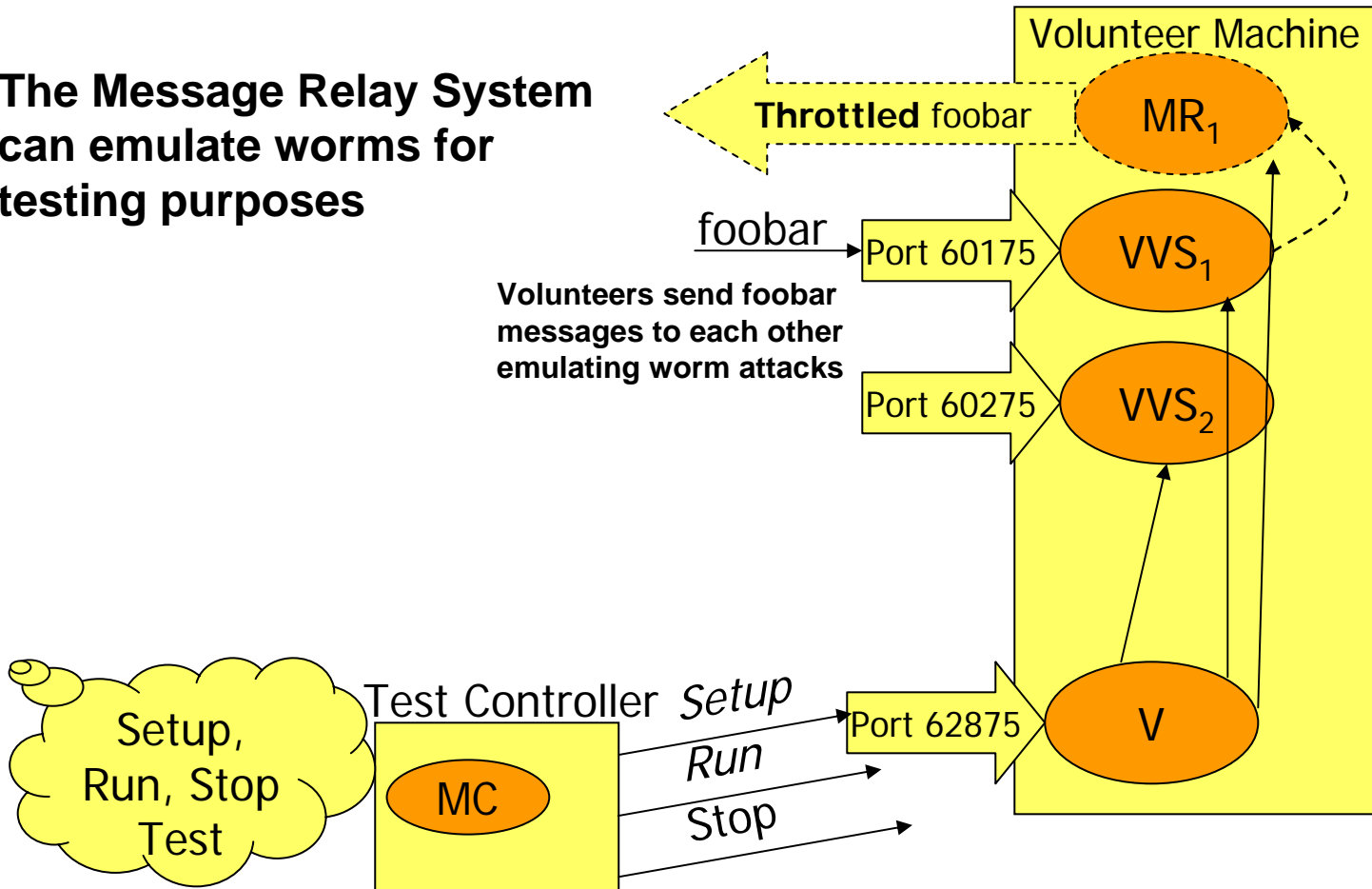


Normal P2P



Highlight

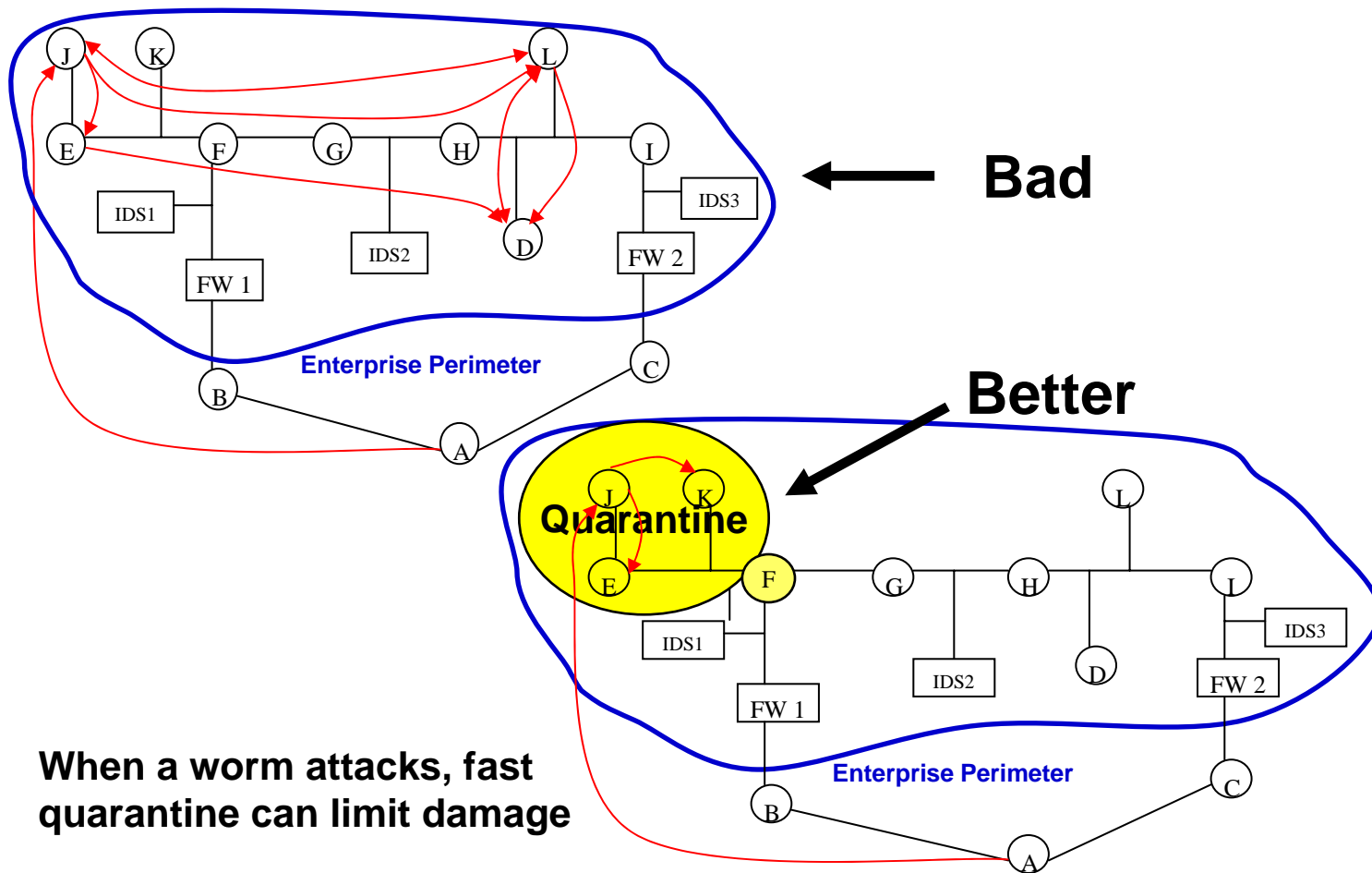
The Message Relay System can emulate worms for testing purposes



Impacts

- **Improve state of the art of enterprise security management**
 - **Push industry to develop adaptive defense support capabilities**
- **Technology transfer to:**
 - **Vendors**
 - **MITRE operations**

Future Plans



When a worm attacks, fast quarantine can limit damage