CERIAS

Behavior Authentication of Server Flows

Motivation

- Strong reliance on port number
  - Firewall filtering rules
  - IDS signatures
- Port numbers can be unreliable for determining traffic type
  - Proxies
  - Port Remappers (e.g., AntiFirewall)
  - “Backdoored” services
  - User-installed services

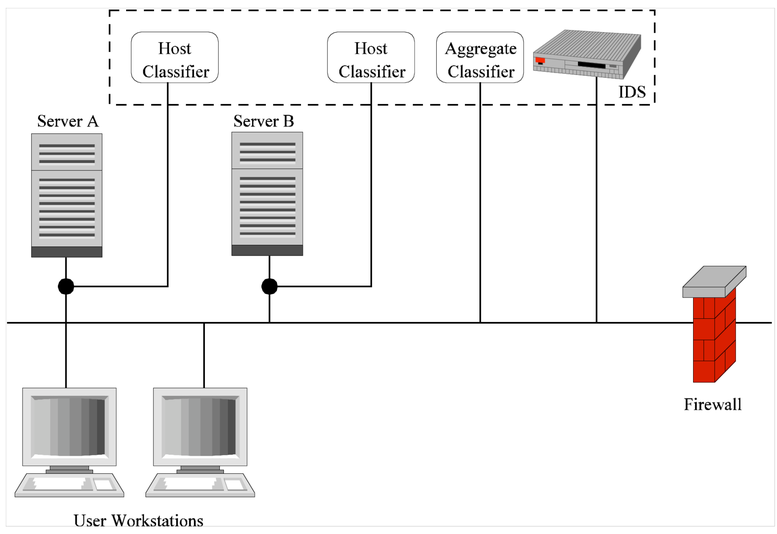
Modeling Flow Behavior

- Capture operational characteristics
- Connection initialization data not required
- Payload data not required
- *Application protocols use the underlying TCP state mechanism in different ways, thus they can be differentiated*

Building Classifiers

- Create feature set
  - TCP state flags
  - Packet length
  - Packet inter-arrival time
- Collect FTP, SSH, Telnet, SMTP, and HTTP flows
- Train a decision tree classifier
  - Service (aggregate)
  - Host

Utilizing Flow Classifiers



Results

- 86-100% classification accuracy
- Real-time classification

Paper by J. Early, C. Brodley, and C. Rosenberg presented at ACSAC 2003:
http://www.acsac.org/2003/papers/66.pdf

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center