

Decision Trees for Server Flow Authentication

James P. Early and Carla E. Brodley
Purdue University

West Lafayette, IN 47907

earlyjp@cerias.purdue.edu, brodley@ecn.purdue.edu

September 24, 2003

Motivation

- Port numbers can be unreliable for determining traffic type
 - Proxies
 - Port Remappers (e.g., AntiFirewall)
 - “Backdoored” services
 - User-installed services

Motivation

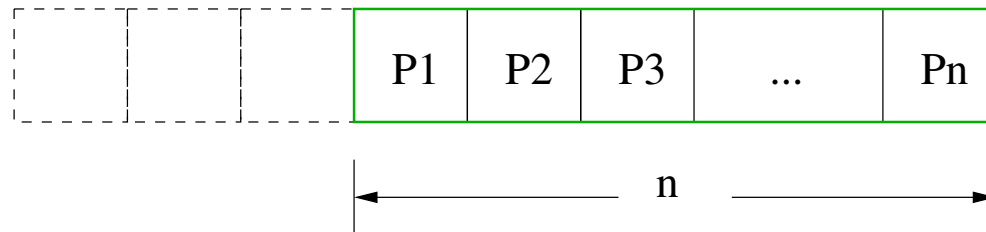
- Strong reliance on port number
 - Firewall filtering rules
 - IDS signatures
- Given a flow of packets from a server, can we identify the application?

Modeling Flow Behavior

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

Feature Construction

- Individual packet features
 - TCP state flags
 - Packet length
 - Inter-arrival time
- Use an overlapping packet window



Supervised Learning

- Train learner to classify unseen flows as one of k classes
- Assumption:
 - Policy specifies services for a host
- Does flow match expected service?

Aggregate Flow Experiments

- FTP, SSH, Telnet, SMTP, HTTP
- Data sets (1999 Lincoln Labs)
 - Training : Week 1
 - Test: Week 3
- Fifty flows / protocol
- Packet window sizes: 10 to 1000
- Use C5.0 to build decision tree

Aggregate Flow Results

Window Size	FTP	SSH	Telnet	SMTP	HTTP
1000	100%	88%	94%	82%	100%
500	100%	96%	94%	86%	100%
200	98%	96%	96%	84%	98%
100	100%	96%	96%	86%	100%
50	98%	96%	96%	82%	100%
20	100%	98%	98%	82%	98%
10	100%	100%	100%	82%	98%

Per-Host Flow Experiments

- Operational characteristics of a host
 - Server implementation
 - OS platform
- Five hosts with three or more services
- Build decision trees (window size 100)
- Classify unseen flows for same host

Per-Host Flow Results

Host	FTP	SSH	Telnet	SMTP	WWW
172.016.112.100	95%	-	100%	90%	100%
172.016.112.050	92%	100%	84%	100%	-
172.016.113.050	100%	-	100%	100%	-
172.016.114.050	100%	95%	100%	95%	95%
197.218.177.069	100%	-	100%	100%	-

Water Cooler Effect

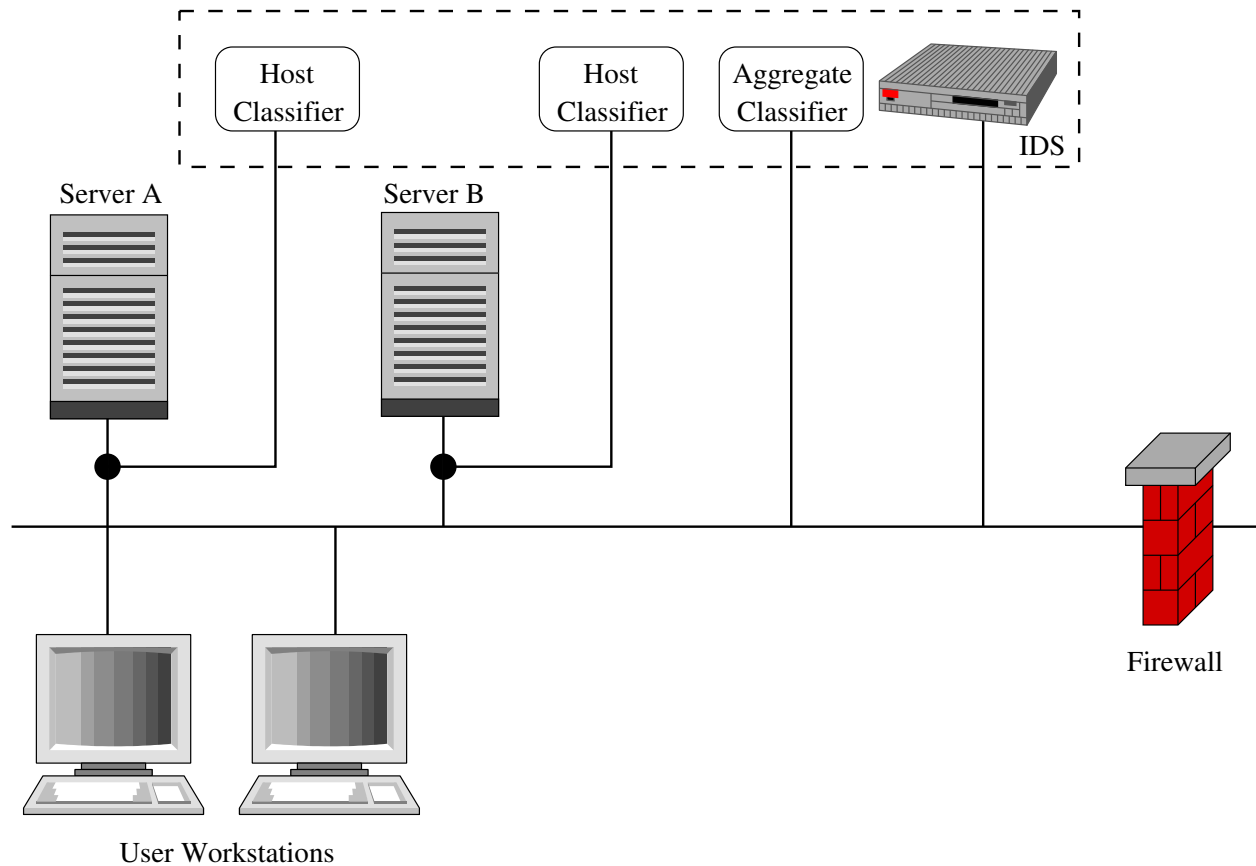


- Cause: long lapses in user activity
- Result: large increase in mean IAT
- Future work
 - Analysis of sub-flows

Experiments Using Live Traffic

- Data collected from our test network
- Augmented with file-sharing data (Kazaa)
- Accuracy 85-100%
 Comparable to synthetic data

Utilizing Flow Classifiers



Subverting Classification



- Water Cooler Effect
- Extraneous TCP Flags (e.g., URG)
- Duplication of particular behavior unlikely

Related Work

- “Flow Classification for Intrusion Detection”
Tom Dunigan and George Ostrouchov, ORNL/TM-2001/115 (2000)
- “Detection and Classification of TCP/IP Network Services”
Tan, K.M.C. and Collie, B.S., Proceedings of the 13th Annual Computer Security Applications Conference (1997)
- Signature Based
 - Connection
 - Payload

Conclusions

- Designed features that model application behavior
- Achieved high classification accuracy in real time
- Future work
 - IDS integration
 - Mitigation of Water Cooler Effect
 - Attempts to subvert classification