Intrusion Detection System

Yuan Xue

Background

- What is Intrusion
  - An intrusion can be defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. [Heady R. 1990]
- Three classes of intruder
  - Masquerader – illegitimate user penetrates the system using a legitimate user's account
  - Misfeasor – legitimate user misuses his/her privileges, accessing resources that is not authorized
  - Clandestine user -- privileged user uses supervisory control to suppress audit control

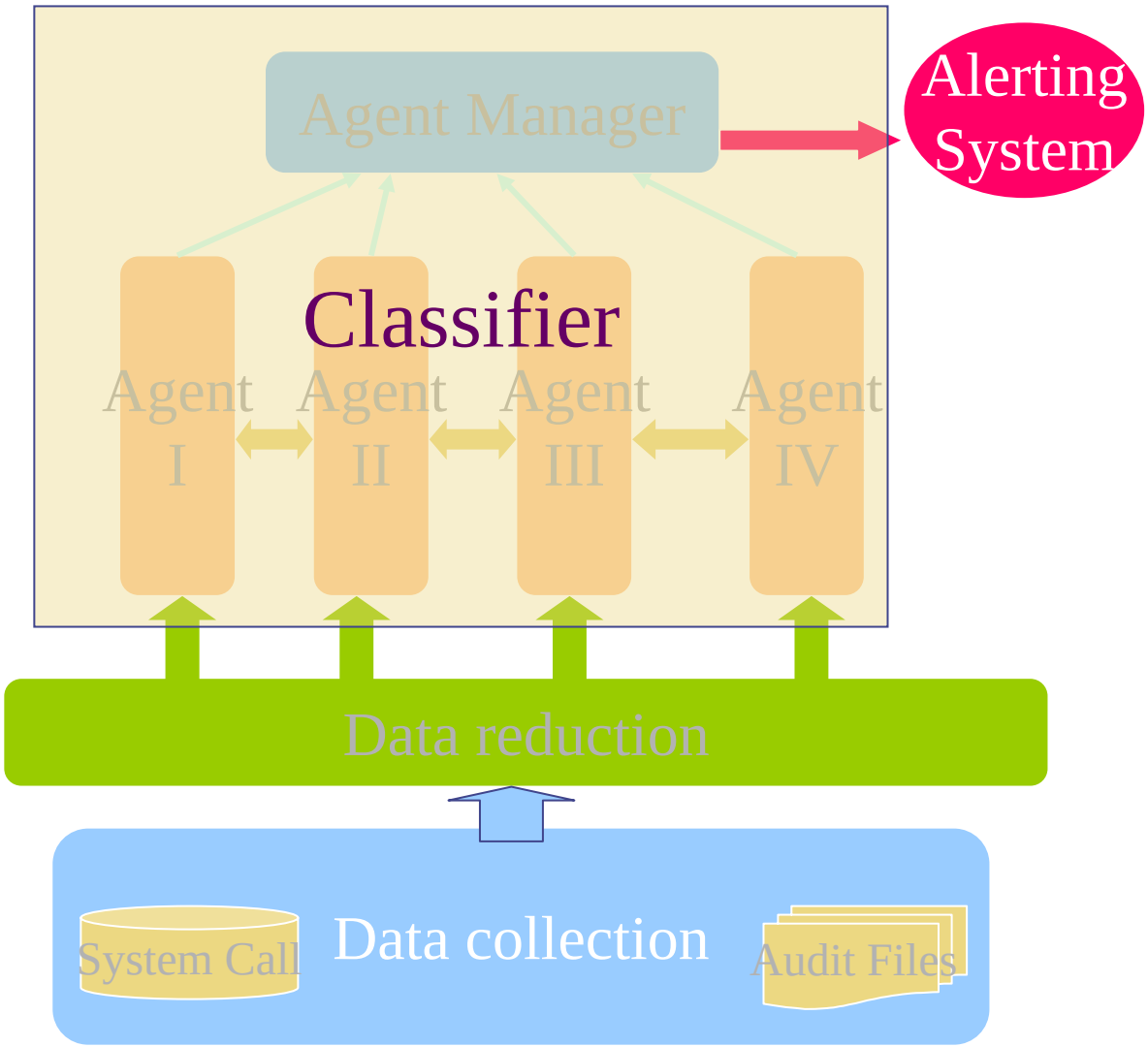
Background

- What is Intrusion Detection System
  - An Intrusion Detection System (IDS) must identify, preferably in real time, unauthorized use, misuse and abuse of computer systems
  - It is a reactive, rather than proactive, form of system defense.
- Classification
  - Misuse intrusion detection vs. Anomaly intrusion detection
    - Misuse intrusion detection -- detect attacks on known weak points of a system.
    - Anomaly intrusion detection -- detect by building up a profile of the system being monitored and detecting significant deviations from this profile.
  - Host-based detection vs. Network-based detection

History

- Conventional approach to system security: Authentication, Access control and Authorization.
- In 1980, James Anderson first proposed that audit trails should be used to monitor threats.
- In 1987, Dorothy Denning presented an abstract model of an Intrusion Detection System.
- In 1988, IDES (Intrusion Detection Expert System) – host-based IDS is developed.
- In 1990, Network Security Monitor is developed – network-based IDS is developed.
- In 1994, Mark Crosbie and Gene Spafford suggested the use of autonomous agents in order to improve the scalability, maintainability, efficiency and fault tolerance of an IDS.

Structure of IDS



- Data collection system
- Data reduction system
- Classifier
- Alerting system

Data Collection and Reduction

- Data source
  - Audit files
    - system audit files: messages,xferlog,syslog,sulog, .bash_ history…
    - application audit files: Web server log files,….
  - System Call
- Audit record [Denning 87]
  - Subject, Action, Object, Exception, Resource usage, Time stamp
  - User operation → elementary actions

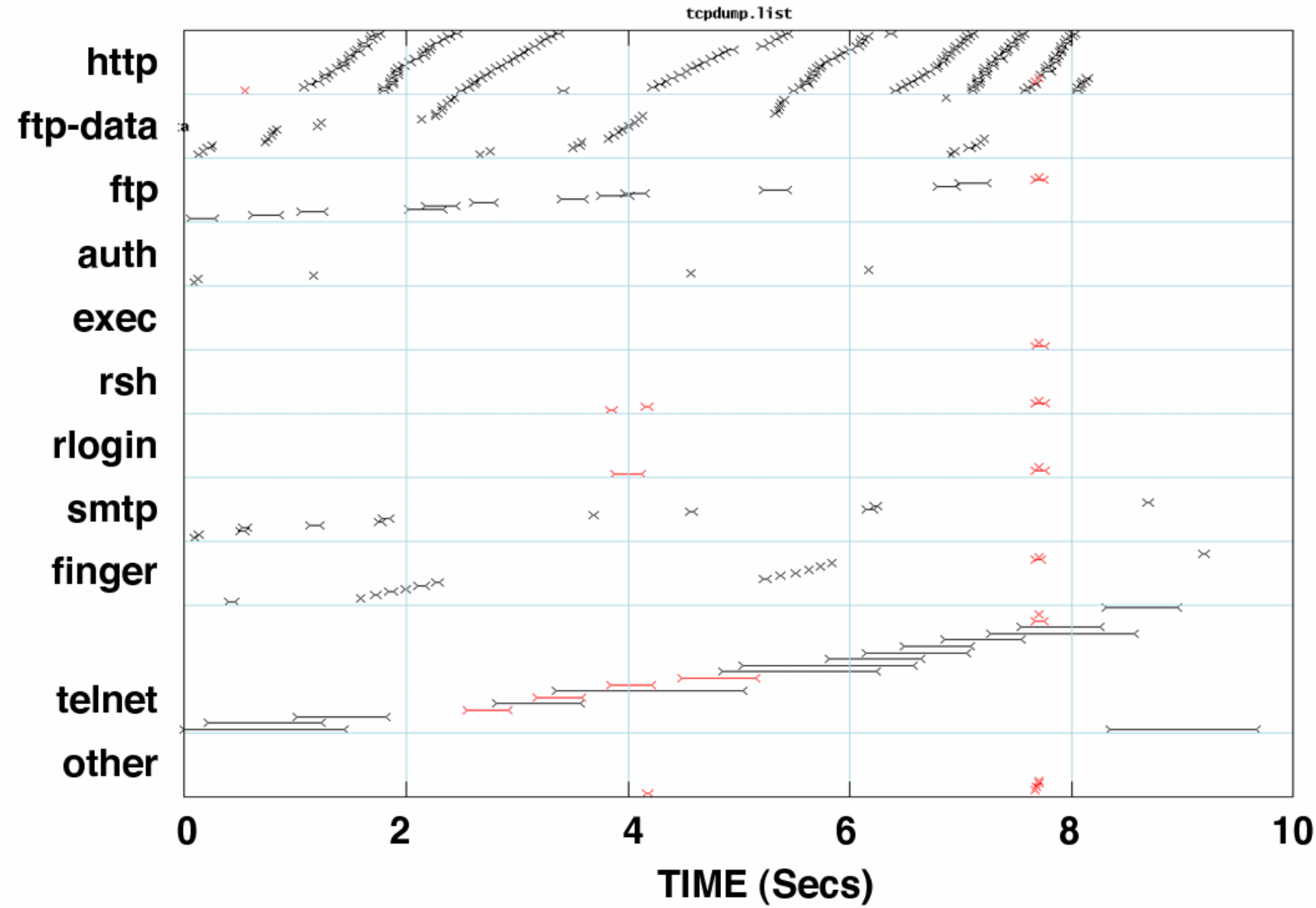
- COPY GAME.EXE to /usr/GAME.EXE

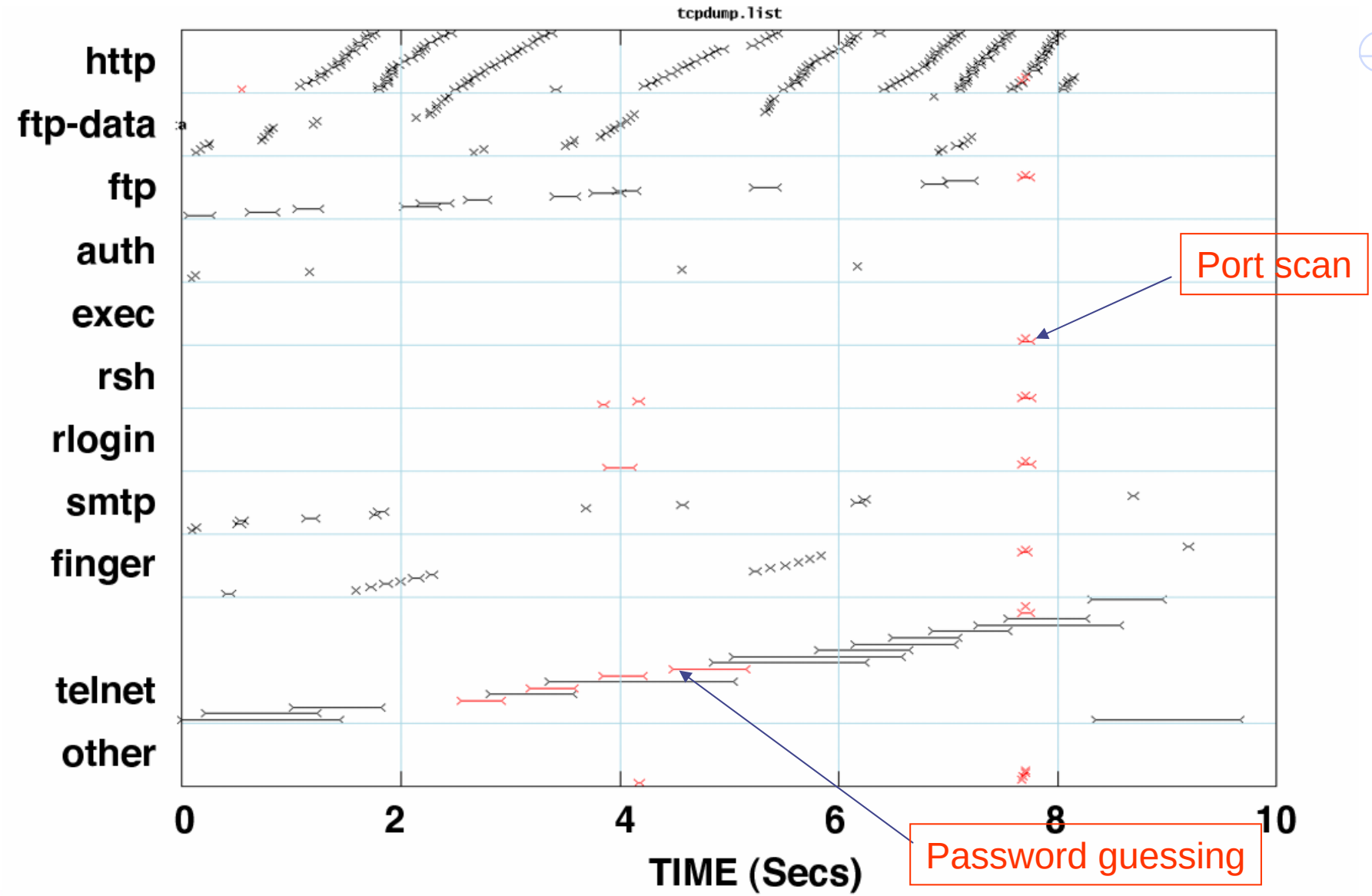
Smith	exec	COPY.EXE	0	CPU = 00002	1058721678
Smith	read	GAME.EXE	0	RECORDS = 1	1058721679
Smith	exec	COPY.EXE	Write-viol	RECORDS = 0	1058721680

Misuse intrusion detection

- Misuse intrusion detection
  - Use patterns of well-known attacks or weak spots of the system to match and identify intrusions
  - Perform pattern matching
  - Used in the environment where a rule can be recognized.

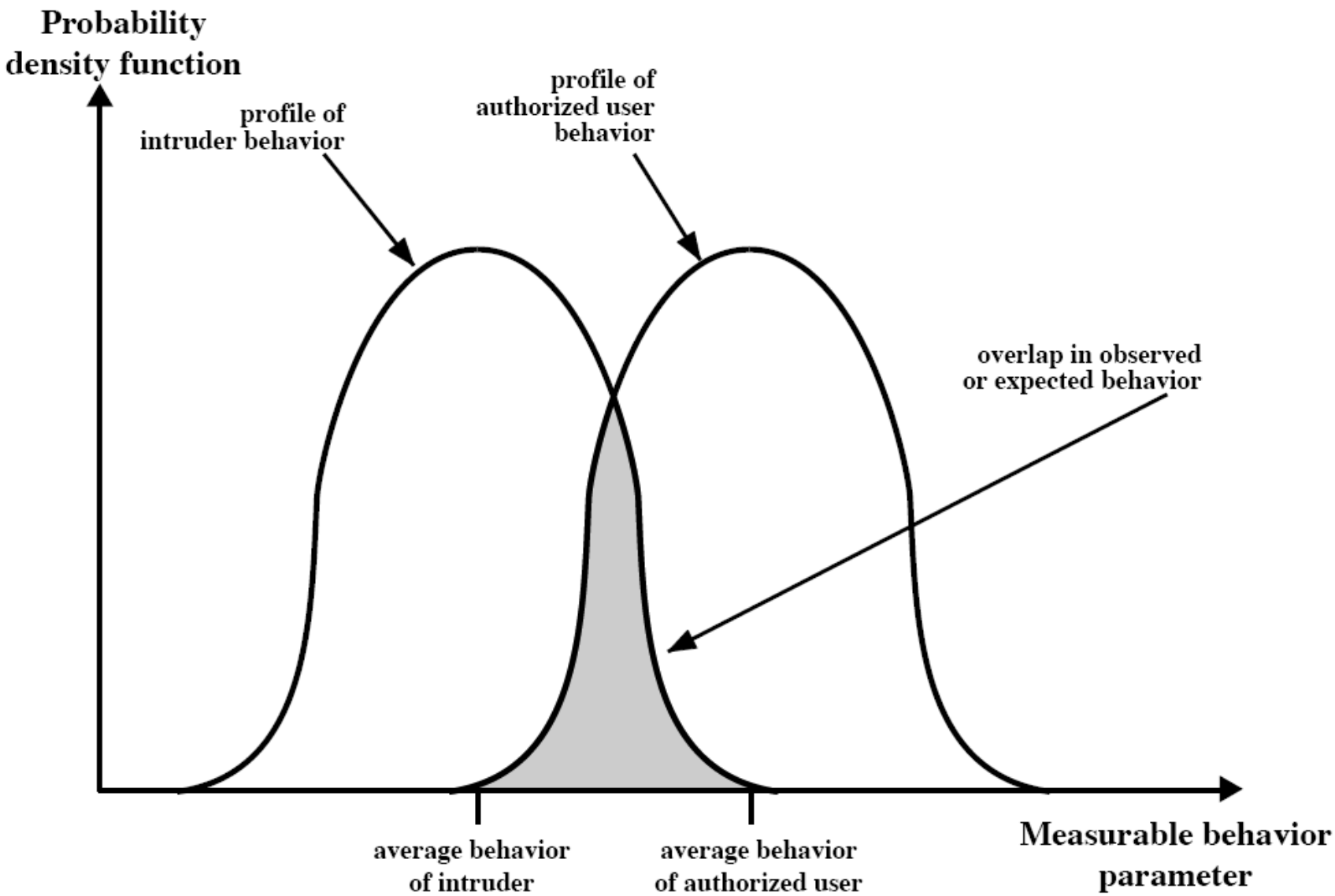
- Example
  - Misuse Intrusion Detection (Purdue) using Patten Matching
  - USTAT, a real-time IDS (UCSB) using State Transition Analysis
  - IDES using rule - based expert system


tcpdump.list
http
ftp-data
ftp
auth
exec
rsh
rlogin
smtp
finger
telnet
other
0
2
4
6
8
10
TIME (Secs)

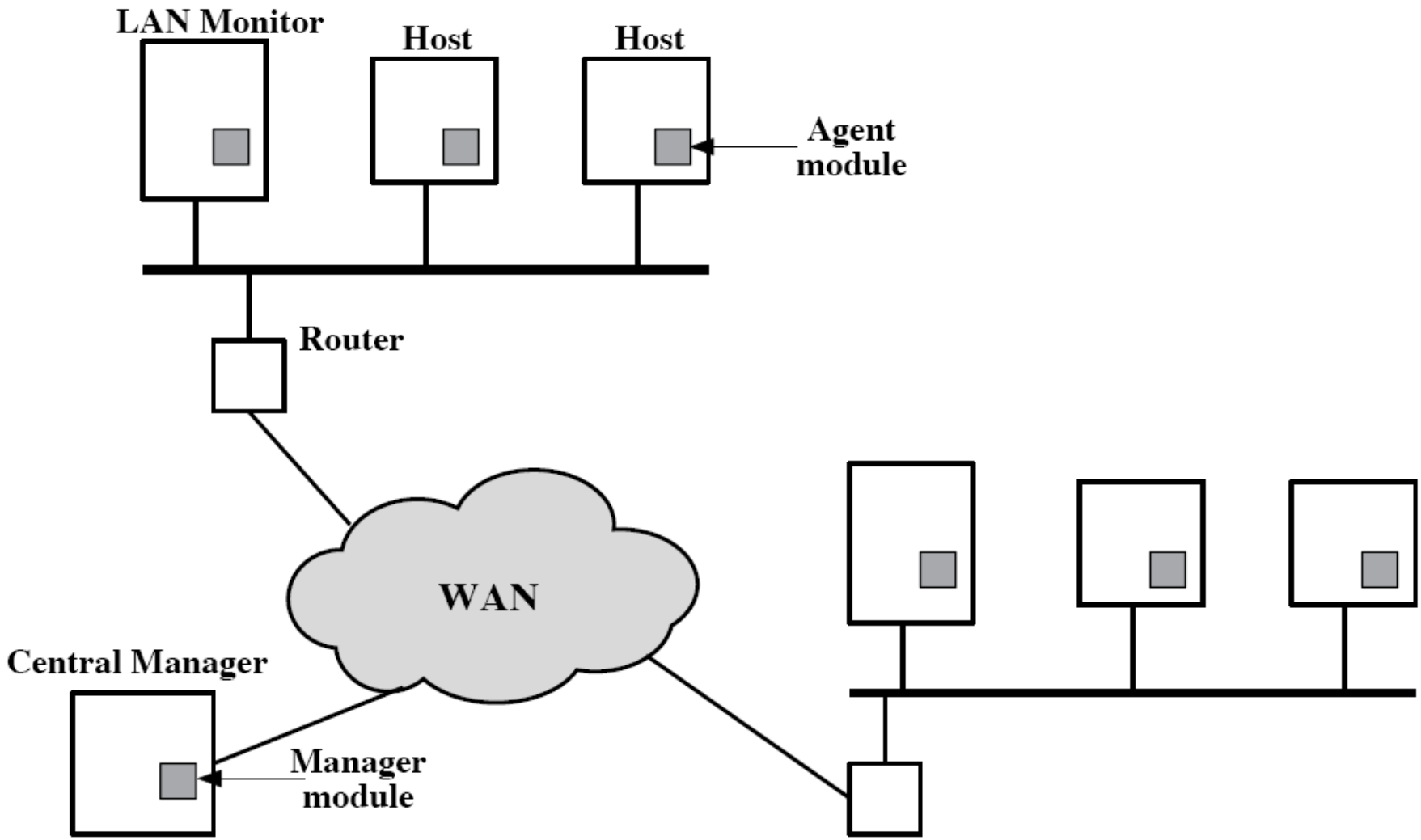

tcpdump.list
http
ftp-data
ftp
auth
exec
rsh
rlogin
smtp
finger
telnet
other
0
2
4
6
8
10
TIME (Secs)
Port scan
Password guessing

Anomaly Intrusion Detection

- Anomaly Intrusion Detection
  - Establish normal usage profiles
  - Observe deviation from the normal usage patterns
  - Example profiles: loginfrequency, locationfrequency, UseofCPU,UseofIO, ExecutionFrequencyFileReadFails、FileWriteFails
- Metrics
  - Mean and standard deviation
  - Multivariate
  - Markov process
  - Time Series
- Approaches
  - Data Mining Approaches
  - Neural Networks
  - Colored-petri-net


Probability
density function
profile of
intruder behavior
profile of
authorized user
behavior
overlap in observed
or expected behavior
average behavior
of intruder
average behavior
of authorized user
Measurable behavior
parameter

Distributed IDS



Honey Pot

- **Honeypots** are closely monitored network decoys
  - Distract adversaries from more valuable machines on a network
  - Provide early warning about new attack and exploitation trends
- Example
  - Honeypot can simulate one or more network services that you designate on your computer's ports.

Product

- **http://www.snort.org/**
  - **Snort® is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods.**
- **http://www.dshield.org/**
  - **A distributed intrusion detection system, or a distributed firewall system. ☺ an attempt to collect data about cracker activity from all over the internet. This data will be cataloged and summarized. It can be used to discover trends in activity and prepare better firewall rules.**
  - **Right now, the system is tailored to simple packet filters. As firewall systems that produce easy to parse packet filter logs are now available for most operating systems, this data can be submitted and used without much effort.**
- **NFR Security Inc.**
  - NFR Security provides a comprehensive, integrated intrusion detection system that protects networks and hosts from known/unknown attacks, misuse, abuse and anomalies. *http://www.nfr.com*
- **Real Secure by ISS**
  http://www.iss.net/products_services/enterprise_protection/

Reference

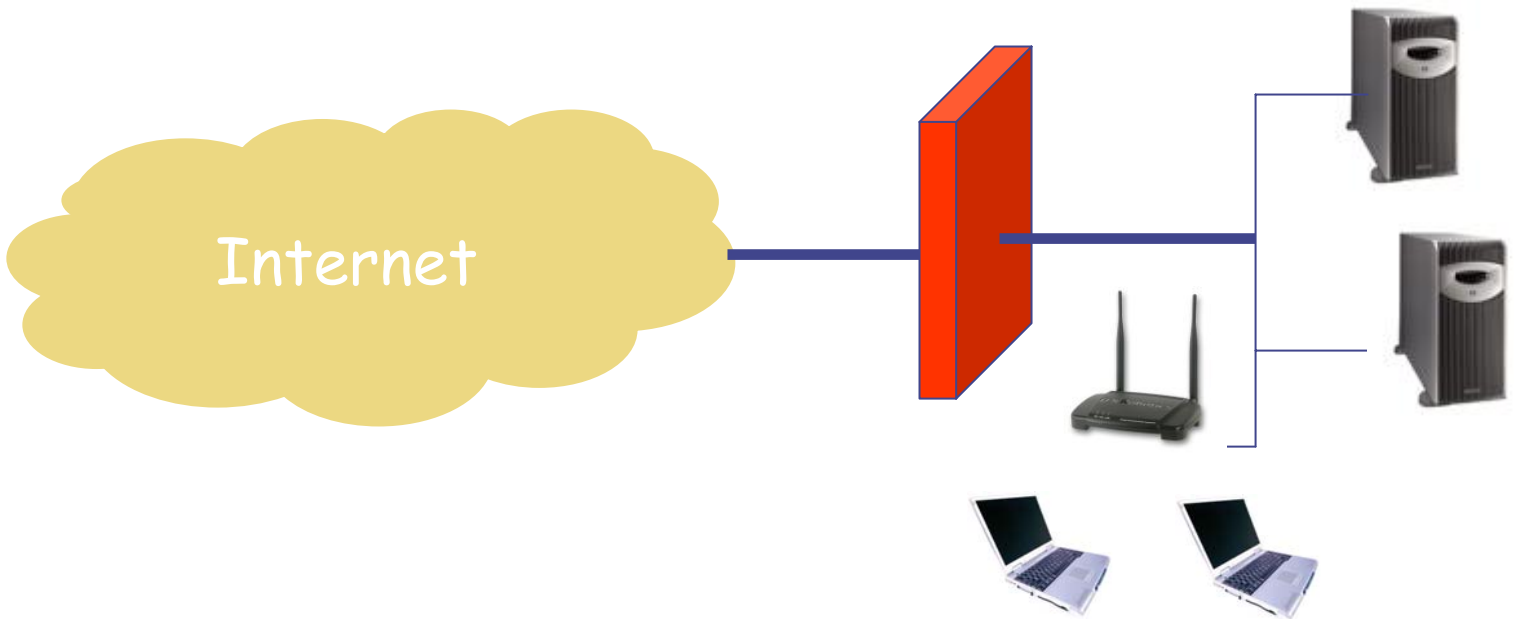
- Intrusion detection FAQ
  - http://www.sans.org/resources/idfaq/
- Purdue Information Security Center
  - http://www.cerias.purdue.edu/
- http://www.cert.org/
- http://www.first.org/

Firewall

Yuan Xue

What is Firewall?

- Design goals
  - All traffic from inside to outside and vice versa must pass through the firewall
  - A single checking point that keeps unauthorized traffic out of the protected network

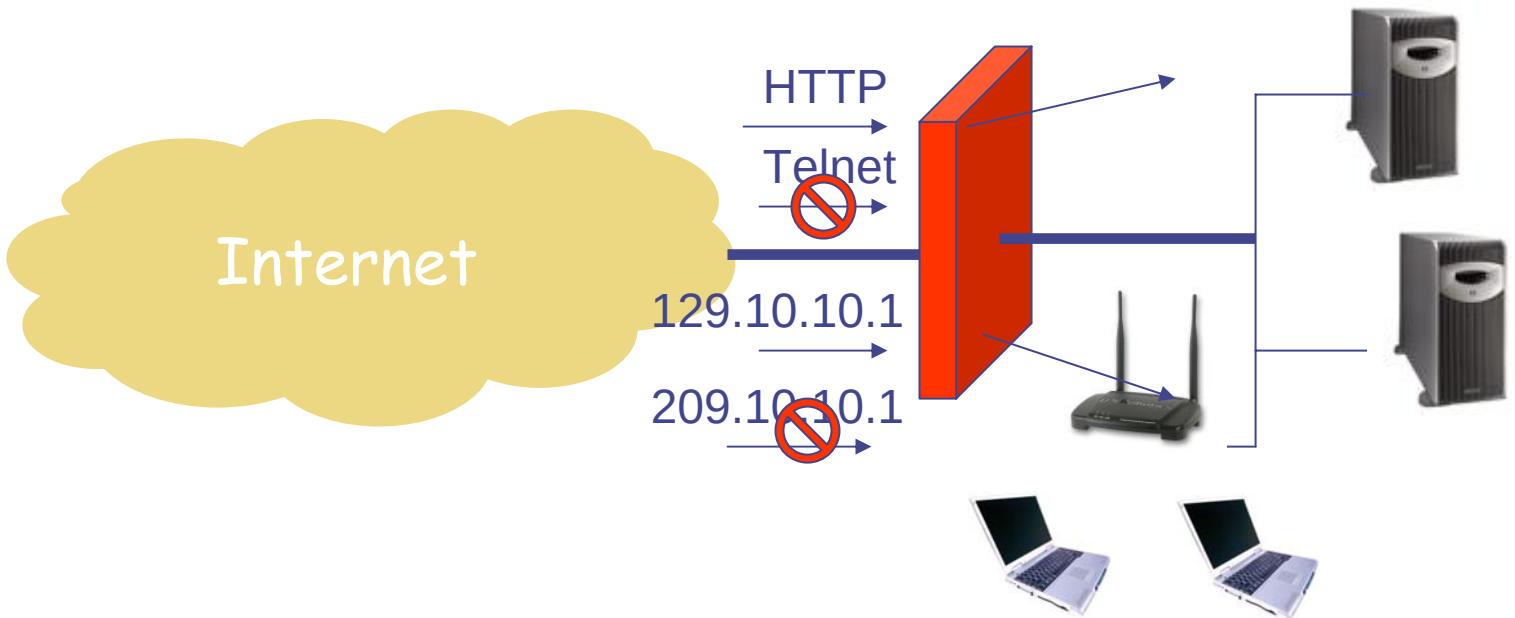


How it functions?

- Technique
  - Control access via security policy
- Types
  - Packet filter router
  - Application-level gateway
  - Stateful filter vs. stateless filter
  - Personal firewall

Packet-Filtering Router

- Packet-Filtering Router
  - Applies a set of rules to each incoming IP packet
  - Decides forwarding or discarding the packet
  - Only examine the header, do not “see inside” a packet
- Pros & Cons
  - Simple
  - No application-specific protection



Packet-Filtering Router

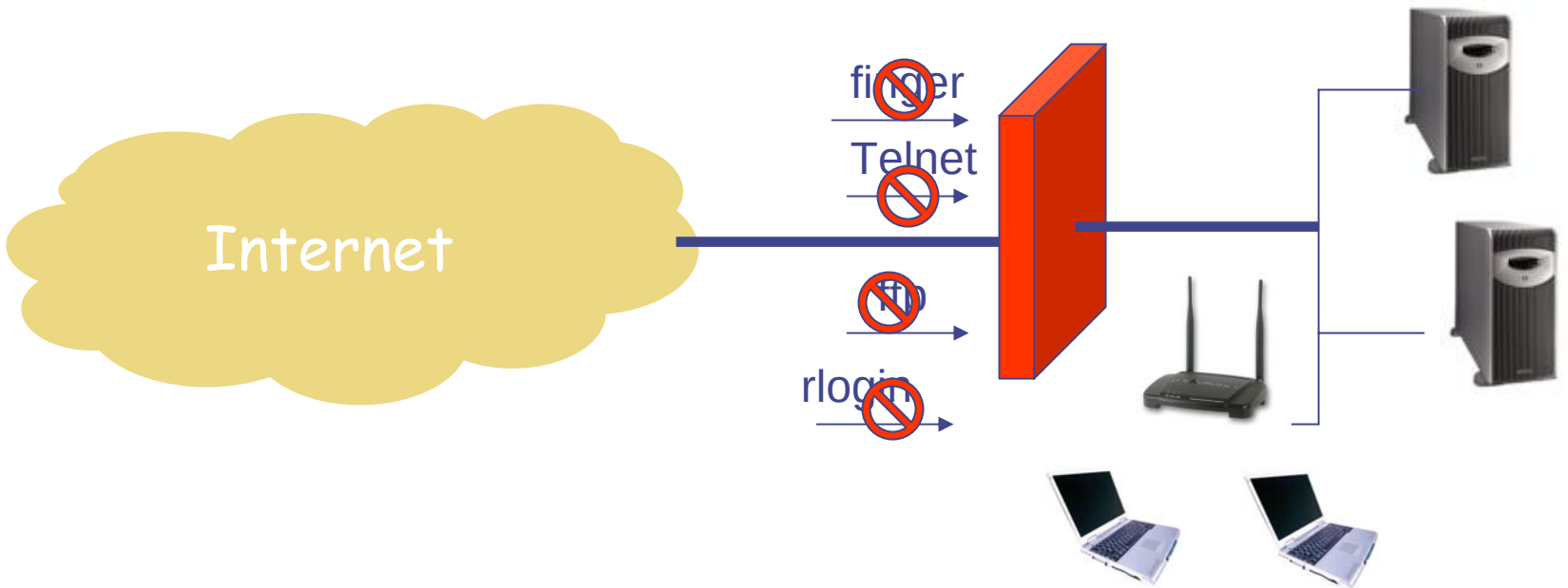
- Filtering rules
  - Src/dest IP address; src/dest port; protocol field; etc.
  - Default
    - Discard vs. forward

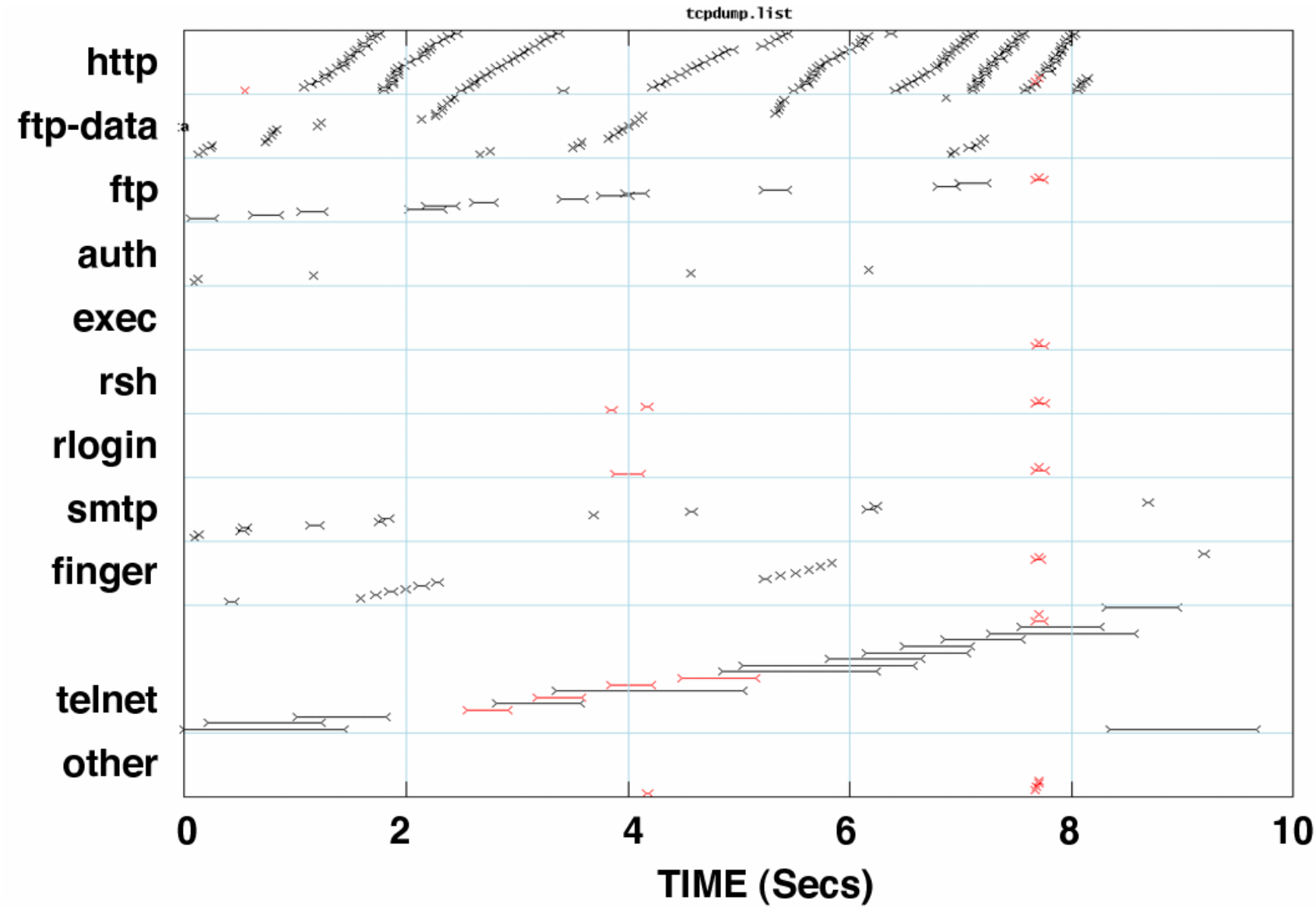
action	Internal host address	Internal port	External host address	External port	function
block	*	*	192.10.*.*	*	Block all packets from 192.10.*.*

action	Internal host address	Internal port	External host address	External port	function
allow	129.10.10.3	25	*	*	Allow inbound mail to 129.10.10.3

Packet-Filtering Router

- The dangerous services
  - finger (port 79)
  - telnet (port 23)
  - ftp (port 21)
  - rlogin (port 513)
  - ICMP




tcpdump.list
http
ftp-data
ftp
auth
exec
rsh
rlogin
smtp
finger
telnet
other
0
2
4
6
8
10
TIME (Secs)

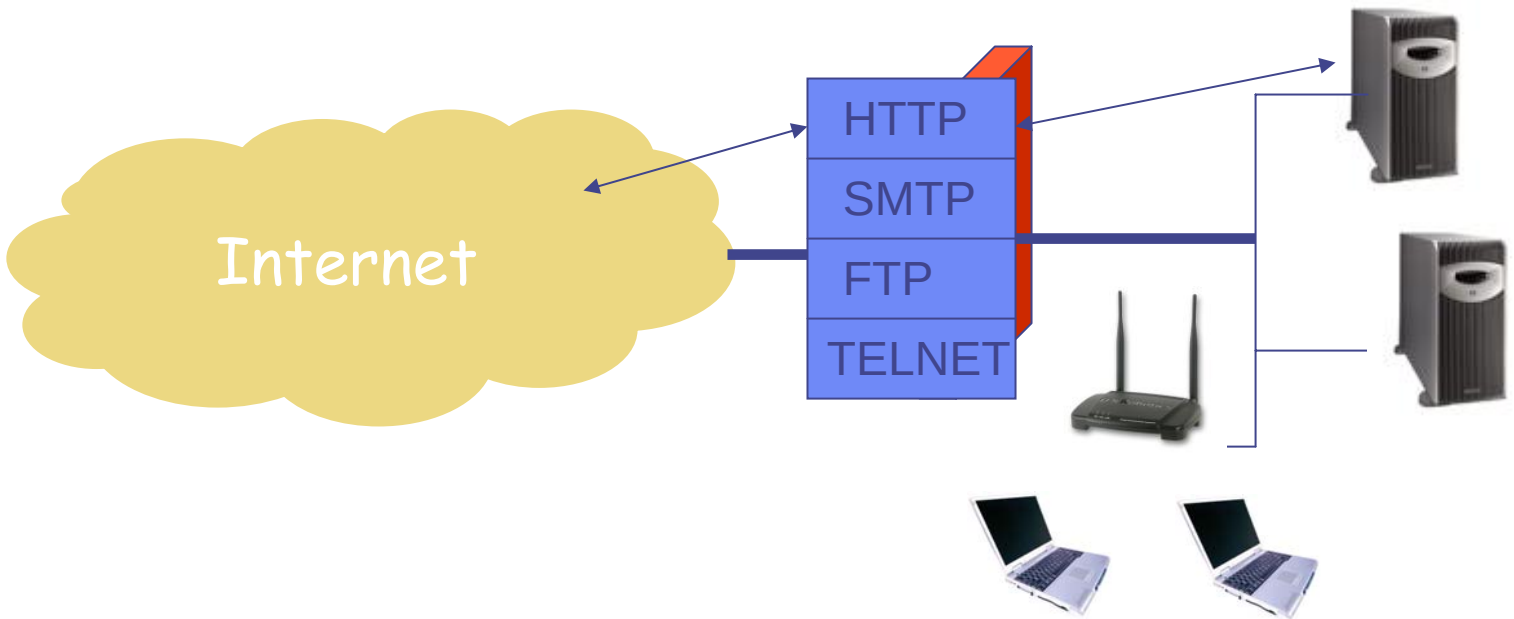
Stateful Inspection Firewall

- Stateful Inspection Firewall
  - Maintains state information from one packet to another in the input stream
  - Tightens up the rules for TCP traffic

Source address	Source port	Destination address	Destination port	State
192.10.10.16	3321	216.10.18.123	80	established

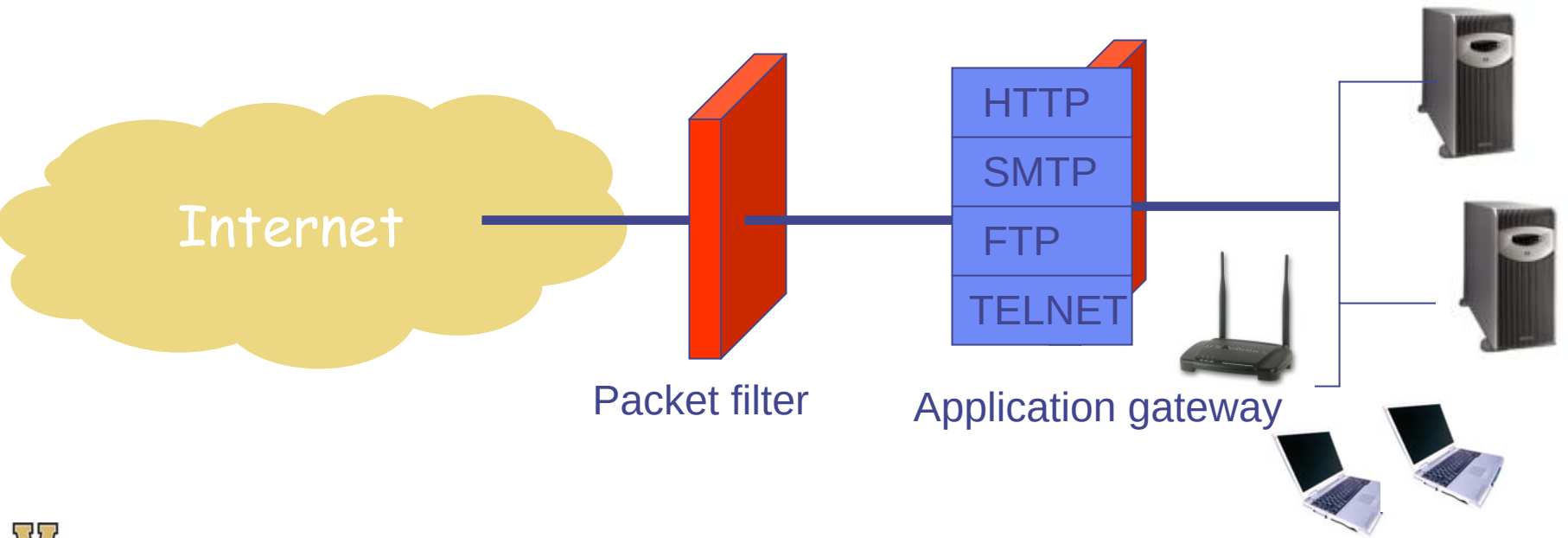
Application-level gateway

- Application level proxy/gateway
  - Relay of application traffic
  - Run pseudoapplications
  - Looks to the inside as if it is the outside connection
  - Looks to the outside as if it is the inside
- Pros & Cons
  - Processing overhead
  - Diverse functionality



Deployment

- Considerations
  - Performance
  - Security of firewall itself
  - Runs on minimized OS
    - non-firewall functions should not be done on the same machine
- Network Topology



Personal Firewall

- Personal Firewall
  - An application that runs on a personal computer to block unwanted traffic
- Product
  - ZoneAlarm
    - www.zonelabs.com
  - BlackICE Defender
    - blackice.iss.net
  - Tiny Personal Firewall
    - www.tinysoftware.com
  - Norton Personal Firewall
    - www.symantec.com
  - Windows XP

Benefit & Limitation

- Benefit
  - Provides a location for monitoring security-related events
  - Provides a platform for security-related functions: NAT, IPSec
- Limitations
  - Attacks that bypass firewall
  - Internal threats
  - Performance
  - Usability vs. security