6.857 Computer and Network Security	**Fall Term, 1997**
Lecture 19 : November 4, 1997	
Lecturer: Ron Rivest	*Scribe: Thor Sewell*

1 Topics Covered

- Java Security (continued)
- TCP/IP
- Syn Flooding
- Firewalls - Packet Level

2 Review: Java Security

Malicious Applets:

a) Barking Dog Applet - sets up thread which is immortal; redefines its own "step" method to do nothing

b) Business assassin applet - kills competitors

c) D.O.S. - soaks up all CPU cycles

d) Continious Window Opening

e) Forging e-mail - telnet to port 25

Digitally Signed Applets Browser has approved list of applets signed by Y; Y is approved by X

3 TCP-IP

Internet sessions are TCP-IP session. In a TCP conversation packets flow in both directions. Acknowledgment packets and control packets flow to both directions regardless if data is flowing one way. The following illustrates a TCP-IP conversation:

Client————————————Server

————————Syn(1000)————————>

<————Syn(2000), Ack (1001)——

————————Ack(2001)————————>

<————————Data, Acks————————>

————-Ack(2300), Fin(1500)——>

<————Ack(1501), Fin(2400)——

————————Ack(2401)————————>

4 Syn Flooding

- send many Syn's to server, but never follow up
- source address can be bogus
- approaches:
  1. trace source of packets
  2. short time-out
  3. sign cookies - offload memory requirement to client
  4. table capable of holding large number of entries

Internet<——Side B——->Firewall<——Side A——->Corporate Network

Firewall should be secure, meaning that all packets going from the corporate network to the outside must go through the firewall. The firewall should allow communication according to policy.

5 Firewalls - Packet Level

Packet Filters are an inexpensive and feasible level of gateway security because primarily they are imbedded in the router software. Packet filters will descriminate between packets based on the source, destination, and port. Packet filters are configured by (1) determining a security policy, (2) specifying the allowable packets formally, and (3) expressions rewritten to a vendor supported syntax. Therefore, the firewall looks at each packet and decides, based only on that packet, what to do. As illustrated in the following table, what is not expressly permitted is prohibited.

FROM....ACTION..SOURCE..PORT...DESTINATION...PORT.....FLAGS

A.....allow.....Inside.....*.....*.....25

B.....allow.....*.....25.....*.....*.....Ack

A.....allow.....Inside.....*.....*.....25.....Ack

* - matches anything

FTP difficult

Client.....Server

<———Establish connection———->

————–User name————->

<————Password?————

————-Password————>

————-Port X (1906)————->

Server opens a connection to port

————Get foo————>

<———Connection established———

<————File foo————–

<————Transfer done————

Tunneling The goal of firewalls is to control and watch what is happening. However, tunneling is a method to by-pass firewalls by encapsulating a message from one protocol in another protocol. After reaching the destination point the second protocol is removed and the original message is available in the network.