Housekeeping

Final exam: Monday, Dec. 17, 8:45 AM – Sloan 9

Makeup final exam: Tuesday, Dec. 18, 5 PM – my office

Record check: in class, Friday

Class evaluation: today

Denial of service attacks

- With a small expenditure of resources attacker causes victim to make a large expenditure of resources
- Many DOS attacks are based on flaws in the victim software
  - For example, victim software crashes when it receives an ill-formed packet
- Others are based on capturing non-owned resources to mount the attack
  - Viruses that spread trojan horse software are one way to enable such an attack

The SYN Flood Attack

- Send (lots of) SYN packets to the victim with a bogus source IP address
  - Victim creates a *half-open* TCP data structure for each packet and keeps it for several minutes
  - Victim failure occurs when it runs out of memory for new connections
  - Notice that the attacker spends only the resources to send the packets while the victim ties up memory for long periods

Defending against SYN Flood (Defense against the Dark Arts)

- SYN Cookies
  - Idea: instead of keeping state for half-open connection in memory, securely encode it in the initial sequence number the victim includes in its SYN/ACK packets
    - Legitimate clients of the victim will return the ISN in their own ACK of the SYN/ACK packet, and the victim will establish a fully open TCP connection for them
    - Attacker won't be able to return the cookie. The victim's resource expenditure now match the attackers – and all the *fun* is gone for the attacker

SYN Cookies (continued)

- What is a SYN cookie?
  - Must obey rules for TCP ISN's
  - Must be unpredictable from src and dst ip/port info
  - Must be possible for victim to establish that the seqno in client ack corresponds to a recent SYN cookie it has sent
  - Must be possible for victim to establish client's MSS (included in the first SYN received) when it receives the cookie

SYN Cookies (continued)

- Example:
  - Determine an array of 8 common MSS's
  - Establish a slowly changing counter (once a minute is fine)
  - Let x = client ISN, z = MD5(sec, saddr, sport, daddr, dport) + x + counter<<24 +MD5(sec, counter, saddr, sport, daddr, dport) % (1<<24), i = index of the greatest MSS smaller than the client's MSS
  - Victim ISN = (i << 29) + z % (1 << 29)

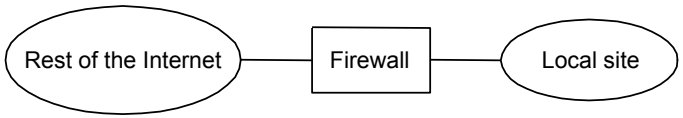
SYN Cookies (continued)

- Limitations:
  - Can't handle TCP extension options (such as big window extension)
  - Limited number of MSS's
- Implemented in Linux kernel but not enabled by default
  - Even when enabled, used only when an attack is happening – as determined by running out of resources for TCP control blocks

Naptha: A harder but even more insidious attack

- Another attack based on TCP's fundamentals (not a bug in the OS)
- If you can send arbitrary packets and hear the replies you can create TCP connections in the victim and leave them in any chosen state for arbitrary periods
  - There has to be a return path to the source network address the attacker uses
  - But if the attacker controls any machine on that network there does not have to be a machine at that address
    - Another machine on the network with its interface in promiscuous mode can handle the traffic

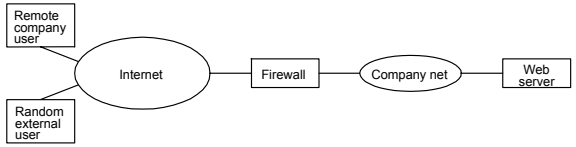
Firewalls



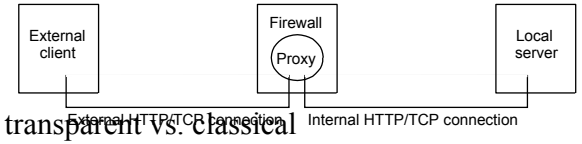
- Filter-Based Solution
  - example
    (192.12.13.14, 1234, 128.7.6.5, 80)
    (*,*, 128.7.6.5, 80)
  - default: forward or not forward?
  - how dynamic?

Proxy-Based Firewalls

- Problem: complex policy
- Example: web server



- Solution: proxy



- Design: transparent vs. classical
- Limitations: attacks from within