CS261 – Firewalls

7 October 2009

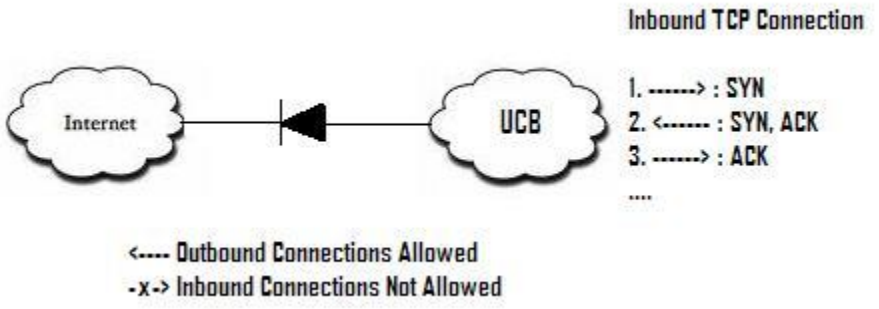
Scribe Notes by Chia Yuan Cho

1. Motivation – Why Firewalls were Invented

- There is no time to patch your systems against an ongoing attack. So the quick fix is to restrict in-bound connections from the internet.
- Considerations:
  - For simplicity, want to enforce this at the network chokepoint(s) where all traffic pass through - on a border router.
  - Routers are already designed to inspect packet headers. So, it's easy to extend this to filter packets.
  - For scalability and efficiency, packet inspection is stateless.

2. Stateless Firewalls

- How might one implement a stateless firewall to restrict in-bound connections?
  - Problem: Cannot simply drop all incoming packets since TCP is bi-directional.
  - One way is to use the ACK-bit trick. This is how it works:

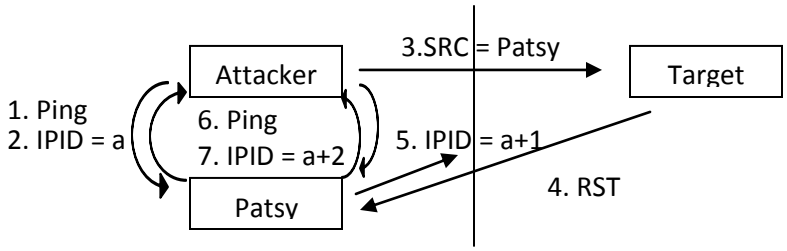


  - Referring to the above figure, a stateless firewall can be implemented by simply dropping all inbound packets with SYN but no ACK (step one of TCP handshake).
  - This mechanism relies on the TCP/IP stack of internal hosts for correctness – when an internal host abruptly receives an ACK or SYN,ACK, it sends out a RST to terminate the connection.
  - What about non-TCP packets?
    - The most useful non-TCP traffic is DNS, which uses port 53. Thus, one might allow only port 53 on UDP, and drop all other inbound non-TCP traffic.
  - Weakness of this implementation – non-SYN incoming packets can reach internal hosts. The attacker can do the following:

- *Ping of death*
  The 2-byte IP Packet length allows the packet to be up to 65,535 bytes. A packet of 65,535 bytes is broken down into fragments and sent. When it is re-assembled at the target host, an integer overflow may occur.

- *Port Scanning*
  The attacker can send a (NULL) packet to a target port on the target host. If there's no reply, the attacker knows the target port is open. If the host sends back a RST, the target port is closed.

- *Stealthy Port Scanning (Nmap "Idle Scan")*
  The underlying basis is the IPID is incremented every packet for most operating systems. The sequence of steps are shown in the figure below. In steps 1 and 2, the attacker first pings Patsy to learn that Patsy's IPID = a. In step 7, if IPID = a + 2, the Target port is closed; if IPID = a + 1, the target port is open.



- *TCP Traceroute*
  The Attacker can do TCP Traceroute through the firewall to map the internal network route to the Target. This is achieved by limiting the TTL and incrementing it in successive hops.

3. Stateful Firewalls

- Problems:
  - Scalability
  - Reliability
  - Still coarse-grained
  - Susceptibility to Denial of Service (state-holding) attacks

4. Firewall Weaknesses – What firewalls cannot prevent

- Trojans
  - Trojans can still initiate outbound connections (data leaks) or do harm inside the network.
  - Typically transmitted through email attachments and externally infected laptops.
- Application Layer attacks

    - Attacks semantic layer, bypassing firewalls
    - Eg: phishing, web browsing, email …
- Consequence of the above
    - Because firewalls are not able to prevent the above attacks, they are now regarded only as basic defense mechanisms. Deployment of firewalls has been stabilizing.
    - Need application-layer firewalls

5. Considerations to Deployment of Firewalls

- If you have a firewall between your network and the internet, where might you place your servers (e.g. email server, web server, etc) ?
    - Place servers internally (behind firewall):
        - Fragility problem: Compromised servers may harm entire internal network.
    - Place servers externally (outside firewall):
        - Servers are not protected from the internet.
    - Create a DMZ, place servers inside DMZ
        - Downside: If a single server is compromised, the attacker obtains access to all inbound / outbound traffic. This allows sniffing, MITM attacks, …
    - Create a DMZ with separate channels for internal network & network services. Each channel is segregated through its firewall.
        - Internal network is protected from compromise of servers

6. Content-based Filtering

- Example: filter HTTP mime types and filenames. Filename = foo.jpg is allowed; filename = foo.exe is denied.
    - Problems:
        - Need to reassemble data from packets
        - Attack against content-based filtering
            - Attacker can send 2 packets with same sequence number, one with foo.jpg and another with foo.exe. Then control which packet makes it to the target host using TTL.
            - Due to lack of semantics, it is difficult for content filter to determine how this is handled by the end host.
            - Downside is to be conservative and drop traffic at expense of legitimate traffic.
- Key insight: Any discrepancy between the filter and the end host allows the attacker to craft a message to exploit that discrepancy. This is the same as the shadow state problem faced in sandboxing.