Network Security

Friday, February 23, 2018 12:56 PM

Network Layers

- Layered model, every layer built on top of a virtual connection layer
  - Every layer = header + payload
- Peer entities in same layer N communicate via protocol defined at that layer
- Attack at any layer can modify data, including header
  - E.g. spoofing "source" ip-address

Name Resolution

Some domain names have multiple IP addresses (especially large sites)

- Need to find the name of the layer below (resolution protocol)
  - Resolver wants to resolve domain name by finding address
  - e.g. DNS (at the application layer), Address Resolution Protocol (ARP)
- Attacks
  - DNS attack: domain name <-> ip-addr (nslookup)
    - Can be the single point of failure for the network
  - ARP attacks: ip-addr <-> mac-addr (media access control)

DNS query

- queryID (QID) must match in query and response
  - Original intention meant for matching, no mac/ encryption
- Attacker can sniff/ spoof, but cannot modify/ remove
  - Note: DNS = application layer, attack = physical layer
- Can be the single point of failure for network
- Cannot attack via https (authentication and private key required)

DoS attack

- Affects availability (prevention/ delay)
- Large numbers of attackers required (each attacker can only send requests at a low rate)
  - Distributed DoS (DDoS)

Reflection and Amplification Attacks

- Reflection: intermediate nodes involved, harder to trace
  - Reflected traffic may be amplified (a request triggers multiple responses)
  - E.g. ICMP/ Smurf flood, ICMP PING: victim network overwhelmed with echo replies
    - Most routers now configured not to broadcast
- Amplification factors
  - Memcache (50000), NTP (556.9), CharGen (358.8)

Botnet

- Bot = zombie, botnet = zombie army (communicating via covert channels)

Useful Tools

- Wireshark (link layer for packet analysis)
- Nmap (port scanner)
  - Transmission Control Protocol (TCP): IP + port (http, 81)
  - Listening: ready to process packets from port
    - Open port: processes running in server which are listening

- Port scanning: see which ports are open in network
- Network administrator can scan for vulnerabilities (and attacker can attack)

Protection

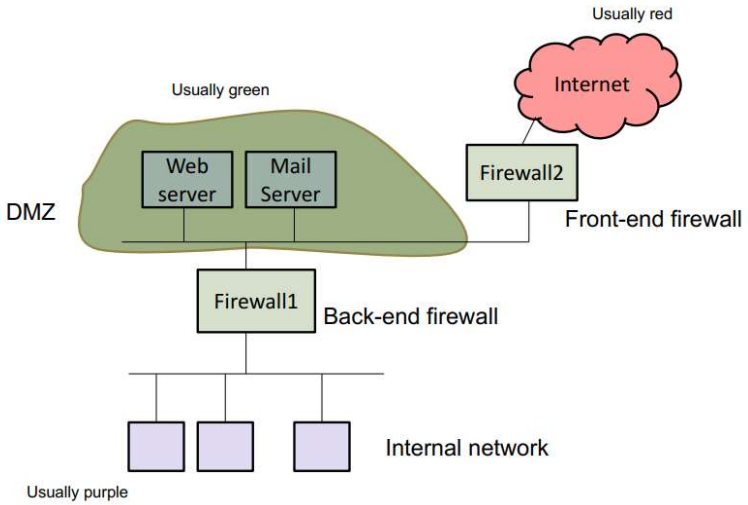
Securing Channel with Cryptography

Which key is owned at which layer? Can only protect upwards

1. SSL = on transport layer (TLS/SSL), used by https
   - Encrpyt-then-mac to preserve integrity (for application layer)
   - Checked again at next SSL layer
   - Alice's data is not visible to others
   - New info added, including IP address/ mac address is not encrypted
2. WPA2 - unclear of exact position, between physical and link layer
   - uses AES
   - WEP -> WPA -> WPA2
   - Key re-installation attack forces nonce reuse in WPA2
3. IPSec
   - Integrity/ authenticity of ip-address, not confidentiality (no spoofing, but possible sniffing)
   - Protection between network and host

Firewall and Intrusion Detection

- Controls traffic (ingress/ egress filtering)
- DMZ: sub-network which exposes external service to (untrusted) internet
- 2-firewall system



- Layered defence to drop packets
  - Have to look through list of "rules" - permit/ deny?
  - Last line = * * * deny
  - E.g. trying to access SQL database directly from internet
- * = any value in regex
- Types of firewalls = packet filters, stateful inspection, proxy

Management

- Monitor and adjust network characteristics
- Wireshark
  - Capturing framework is placed between the NIC driver and higher layer protocols in the

kernel (e.g. TCP/IP)

- Security Operations Center (SOC) - centralised unit, for IT systems and security issues
- Security Information and Event Management (SIEM)
    - Tools for SOC
    - E.g. Splunk

Readings

Splunk - SIEM tool https://www.splunk.com/