Contents

1 IP security

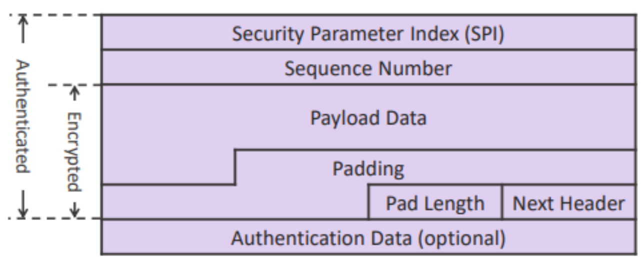
- IP is connectionless and stateless
  - Best effort service
  - No delivery guarantee
  - No order guarantee
- IPv4 No guaranteed security support
- IPv6 security support is guaranteed - IPSec.

1.1 IPSec

- Optional in IPv4, mandatory support in IPv6
- Two major security mechanisms
- IP Authentication Header (AH). (Not really used, because it's not to useful)
- IP Encapsulation Security Payload (EPS). We both encrypt and authenticate data
- Does not contain any mechanisms to prevent traffic analysis.

2 Encapsulation Security Payload (ESP)

Includes an additional header within the IP packet that describes what encryption and authentication is in use

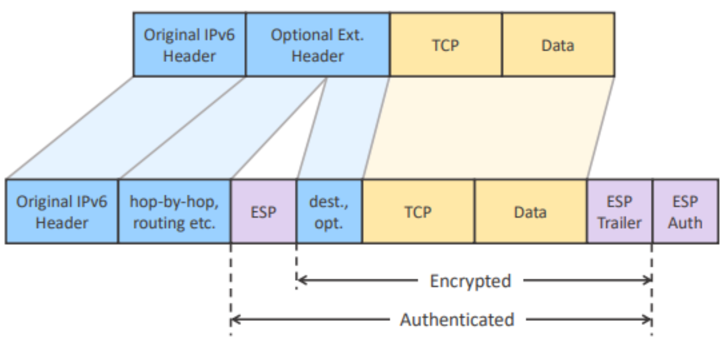


2.1 Security parameter index

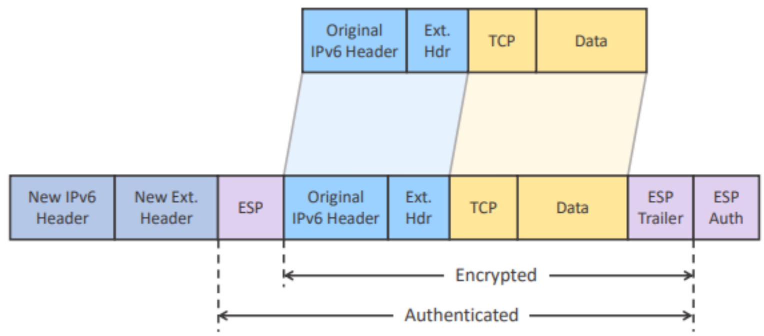
- Stores security parameters e.g. crypto protocol and keys
- Established by Internet security association and key management protocol (ISAKMP) during the Internet Key Exchange (IKE) handshake
- Uses Diffie-Hellman for key exchange
- The SPI references the entry in a table that corresponds to this sessions parameters

2.2 ESP in Transport Mode

ESP uses either Transport or Tunnel modes



2.3 ESP in tunnel mode



2.4 Transport vs tunnel modes

- **Transport mode** simply encrypts packets, providing **host-to-host encryption** but using the original header
- Prevents contents being read, but doesnt stop traffic analysis or manipulation of the header
- **Tunnel mode** (usually gateway-to-gateway) protects some segment of a channel with encryption
- Provides some resistance to traffic analysis, and completely protects manipulation of the payload
- VPNs are commonly implemented this way

3 ARP

- ARP is a protocol used (in IPv4) to obtain physical MAC addresses for given IPs
- It is used prior to constructing IP and TCP packets for communication
- Network layer
- **ARP Cache Poisoning:** we can simply send an unrequested ARP reply, and overwrite the MAC address in a hosts ARP cache with our own

3.1 ARP Protection

- Some OSs ignore **unsolicited ARP requests**, or can be configured to use ARP differently
- Some software, such as intrusion detection packages, will include ARP spoofing detection
- Maintain a log of current MAC:IP assignments and ARP requests / replies
- Allows us to spot suspicious messages such as unsolicited ARP replies

4 DNS

- DNS translates domain names into IP addresses. E.g. nottingham.ac.uk 128.243.80.167
- DNS packets are UDP. Stateless, on the transport layer
- DNS resolvers **will cache** the IPs for a while

4.1 DNS Spoofing

- If we can poison the cache of a nameserver people are using, we can replace a **website lookup with our IP**
- Can be achieved through prior arp cache poisoning, a reply flood or a Kaminsky attack
- **Kaminsky attack**: utilises the fact that cache restrainst, don't apply to sibling domains: (1.google.com, 2.google.com, etc.)
- Attackers can do this and say theyre the official server for www.google.com, telling the nameserver what www. needs to be, and the nameserver will believe the attacker.

4.2 DNS protection

- Random query numbers help protect against spoof replies
- Since the Kaminsky attack, most resolvers now randomise the source port too
- DNSSEC aims to tackle DNS exploits by authenticating the name server and providing integrity for the messages

5 Denial of Service Attacks

- A denial of service attack is an attempt to make a machine or network resource unavailable to its authorised / intended users
- This will usually involve flooding a machine with enough requests that it cant serve its legitimate purpose. E.g. Ping flood
- A distributed denial of service occurs where there is more than one attacking machine

5.1 TCP Syn Flooding

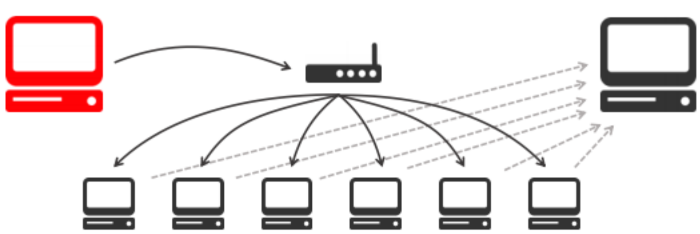
- Attacker initiates a genuine connection but then immediately breaks it
- Attacker never finishes 3-way handshake
- Victim is busy with the timeout
- Attacker initiates large number of syn requests
- Victim reaches its half-open connection limit
- Denial of service

6 Amplification Attacks

- Regular attacks are your bandwidth vs your targets
- Amplification attacks utilise some aspect of a network protocol to increase the **bandwidth of an attack**

6.1 Smurf and Fraggle Attacks

- Smurf attacks broadcast an ICMP Ping request to a router, but with a spoofed IP belonging to the victim
- A Fraggle attack is identical in principle, using UDP echo packets



6.2 DNS Amplification

- Recursive resolvers respond to DNS queries then return a response
- This response can be many times larger than the query
- In an ideal world, all DNS resolvers would:
- Use an authorised list of requesters e.g. and ISP allowing requests from only their customers
- Egress filtering Why is this external IP using my resolver?
- Many DNS servers are set up incorrectly, and will happily amplify your traffic Open Resolvers
- Botnets maintain lists of these open resolvers, and there are projects attempting to shut them down

6.3 NTP Amplification

- NTP is a protocol for synchronising time between machines
- Extremely similar to DNS amplification
- `MON_GETLIST` request returns the list of the last 600 contacts → 200x amplification

7 Low and Slow

- **Slowloris**
- Open numerous connections to a server
- Begin an HTTP request, but never actually finish it
- **R-U-Dead-Yet?**
- Similar to slowloris
- Begin an extremely long HTTP POST, send tiny amounts at a time

Reference section

placeholder