Scribe: Cryptography and Network Security (Week-6 Class-1 Part-1)

Smayan Das

08-Oct-2020

1 Introduction

Network defense is a term that loosely translates to a set of processes and protective measures that use computer networks to detect, monitor, protect, analyze and defend against network infiltrations resulting in service/network denial, degradation and disruptions.
This lecture focuses on understanding the various kinds of attacks that are possible in a computer network and designing defenses as a countermeasure to those attacks.

2 Protocol Level Mitigation

2.1 DDoS Mitigation: IP Traceback

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet IP traceback is critical for identifying sources of attacks and instituting protection measures for the Internet. Most existing approaches to this problem have been tailored toward DDoS attack detection.

- **Recording Route**
  People came up with the idea of having a record route option in the IP so that it can be known exactly which server the packet came from even though IP spoofing has been done by the attacker.
  A recorded route is composed of a series of internet addresses. Each IP address is 32 bits in size. If the pointer is greater than the length, the recorded route data area is full. The originating host must compose this option with a large enough route data area to hold all the address expected.

- **Packet Marking**
  Due to high storage requirements of Record Route feature in IP protocol there was a need for optimization and Savage et al suggested probabilistically marking packets as they traverse routers through the Internet.
  The idea stemmed from the fact that we did not need every single IP in

every single packet. They proposed that the router mark the packet with either the router's IP address or the edges of the path that the packet traversed to reach the router.
Algorithms were designed to enable the victim to reconstruct entire path using sampling and compression algorithms.
In 2001, Song and Perrig proposed the following traceback scheme: encoding the IP address into an 11 bit hash and maintain a 5 bit hop count, both stored in the 16-bit fragment ID field. This is based on the observation that a 5-bit hop count (32 max hops) is sufficient for almost all Internet routes. This led to better handling of DDoS attacks and minimization of false negatives.

2.2 Protection against IP spoofing: IPSec

The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.
IPSec is the security extension of IPv4 and IPv6 protocols.
It consists of the following three parts:

- **IP Authentication Header**
  Ensures the authentication and integrity of the payload and the header.It also provides data integrity, anti- replay protection but not encryption. The anti-replay protection protects against unauthorized transmission of packets.

- **IP Encapsulation Security Protocol (ESP)**
  It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
  It is a transport layer security protocol designed to function with both the IPv4 and IPv6 protocols. It takes the form of a header inserted after the Internet Protocol or IP header, before an upper layer protocol like TCP, UDP, or ICMP, and before any other IPSec headers that have already been put in place.

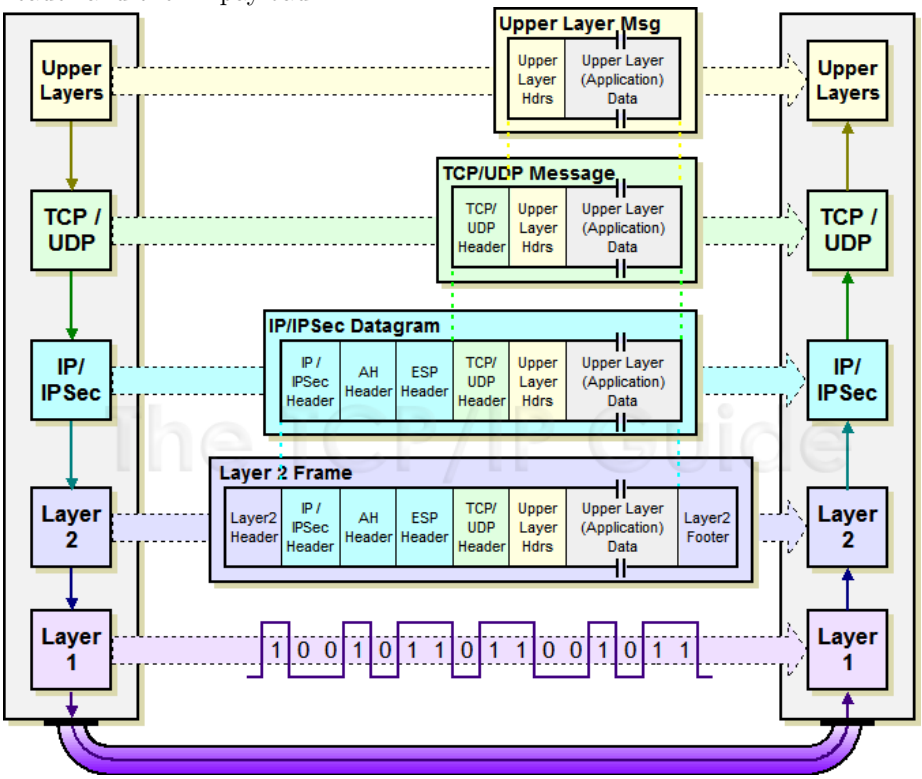
- **ESP with ICV(Integrity Check Value)**
  The ESP also contains the Authentication Data field, which holds the Integrity Check Value (ICV), and a message authentication code for verifying both the sender's identity and the message's integrity. The ICV is calculated with respect to the ESP header, the payload data, and the ESP trailer. ICV, thus ensures confidentiality, integrity and integrity of the payload.

Working of Transport mode IPSec

As its name suggests, in transport mode, the protocol protects the message passed down to IP from the transport layer. The message is processed by

AH/ESP and the appropriate header(s) added in front of the transport (UDP or TCP) header. The IP header is then added in front of that by IP.

Another way of looking at this is as follows. Normally the transport layer packages data for transmission and sends it to IP. From IP's perspective, this transport layer message is the payload of the IP datagram. When IPSec is used in transport mode, the IPSec header is applied only over this IP payload, not the IP header. The AH and/or ESP headers appears between the original, single IP header and the IP payload.



3 Perimeter Level Defense

3.1 VPN: Virtual Private Network

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments

Modes of VPN

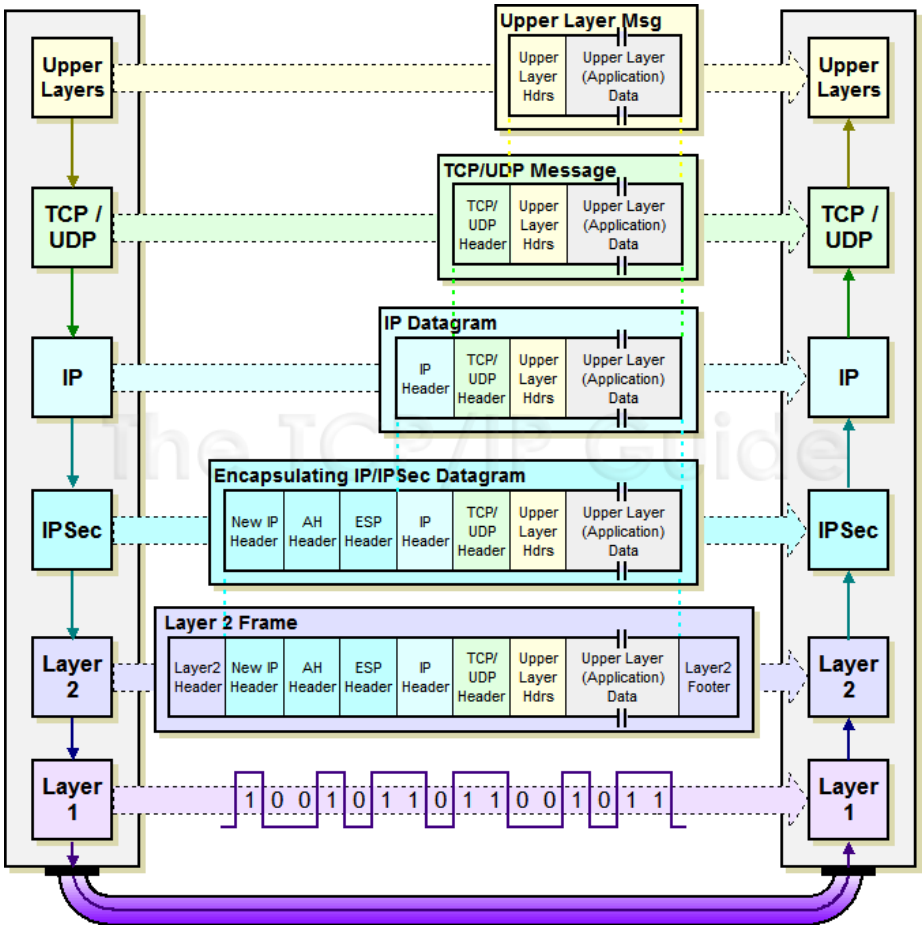
- **Remote Access Client's Connection**
  Remote access VPNs connect the user to a secure remote server in order

to access a private network. The added encryption ensures that security isn't compromised.

- **LAN to LAN internetworking**
  LAN to LAN internetworking works in a different manner. It's used when a connection between two separate intranets is required, but without the possibility of one accessing the other directly

- **Controlled access within an Intranet**
  Their main goal is providing multiple users in various fixed locations with the ability to access each other's resources.

3.2 Tunnel Mode IPSec as VPN



Tunnel mode works only for IP-in-IP packets. In tunnel mode, IPsec policy is enforced on the contents of the inner IP packet. Different IPsec policies can be enforced for different inner IP addresses. That is, the inner IP header, its next header, and the ports that the next header supports can enforce a policy. Unlike transport mode, in tunnel mode the outer IP header does not dictate the policy of its inner IP packet.

Therefore, in tunnel mode, IPsec policy can be specified for subnets of a LAN behind a router and for ports on those subnets. IPsec policy can also be specified for particular IP addresses, that is, hosts, on those subnets. The ports of those hosts can also have a specific IPsec policy. However, if a dynamic routing protocol is run over a tunnel, do not use subnet selection or address selection because the view of the network topology on the peer network could change. Changes would invalidate the static IPsec policy.

3.3 IPSec can be broken

IPSecc uses IKE(Internet Key Exchange) protocol for doing key exchange and for making the process faster they resused keys for different modes and versions of IKE. An attack happened in 2018 which proved that IPSec can be broken and presented a detailed execution of the process.
IKE consists of two phases, where Phase 1 is used to establish initial authenticated keying material between two peers. Phase 2 is used to negotiate further derived keys for many different IP-based connections between the two.
The proof-of-concept targets only Phase 1 in IKEv1 and IKEv2, where the attacker impersonates an IKE device.
Once attackers succeed with this attack on Phase 1, they share a set of (falsely) authenticated symmetric keys with the victim device, and can successfully complete Phase 2 – this holds for both IKEv1 and IKEv2.
In IKEv1, four authentication methods are available for Phase 1: Two RSA encryption-based methods, one signature-based method, and a pre-shared key (PSK)-based method.
In IKEv2, Phase 1 omits the encryption-based authentication methods, leaving only signature- and PSK-based authentication methods.
The attacks are based on Bleichenbacher oracles – a 20-year-old protocol threat that has been used through the years to break the confidentiality of TLS when used with RSA encryption. The researchers have now found that these same oracles "can very efficiently be used to decrypt nonces," which breaks the RSA-encrypted authentication in IKE's Phase 1.

3.4 VPN: Protocols

- **IKEv2/IPSec**
  Internet Key Exchange version 2 is a common VPN tunneling protocol that provides a secure key exchange session. Similar to L2TP (and IKEv1), IKEv2 is normally paired with IPsec for encryption and authentication.

This protocol is very good at re-establishing the link after temporary connection loss and excels at switching connections across network types (from WiFi to cellular, for example).

- **L2TP/IPSec**
  Layer 2 Tunnel Protocol is a replacement of the PPTP VPN protocol. This protocol does not provide any encryption or privacy out-of-the-box and is frequently paired with security protocol IPsec. Once implemented, L2TP/IPsec is extremely secure and has no known vulnerabilities.

- **OpenVPN**
  OpenVPN is an open source protocol that allows developers access to its underlying code. This protocol has grown in popularity due to its use of (virtually unbreakable) AES-256 bit key encryption with 2048-bit RSA authentication and a 160-bit SHA1 hash algorithm.

3.5 Does IPSec work with NAT ? How?

NAT and IPsec are incompatible with each other, and to resolve this issue, NAT Traversal was developed. NAT Traversal performs two tasks of detecting if both ends support NAT-T and detecting NAT devices along the transmission path (NAT-Discovery)

Step one occurs in ISAKMP Main Mode messages one and two. If both devices support NAT-T, then NAT-Discovery is performed in ISKAMP Main Mode messages (packets) three and four. THe NAT-D payload sent is a hash of the original IP address and port. Devices exchange two NAT-D packets, one with source IP and port, and another with destination IP and port. The receiving device recalculates the hash and compares it with the hash it received; if they don't match a NAT device exists.

If a NAT device has been determined to exist, NAT-T will change the ISAKMP transport with ISAKMP Main Mode messages five and six, at which point all ISAKMP packets change from UDP port 500 to UDP port 4500. NAT-T encapsulates the Quick Mode (IPsec Phase 2) exchange inside UDP 4500 as well. After Quick Mode completes data that gets encrypted on the IPsec Security Association is encapsulated inside UDP port 4500 as well, thus providing a port to be used in the PAT device for translation.

4 Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

4.1 Packet Filtering

Packets arriving are inbound, and those leaving are outbound. Filtering inbound packets protects the internal network from the Internet. Filtering outbound packets allows awareness and partial control of data sent out and services accessed, e.g., to enforce a security policy restricting allowed protocols and services, and to detect unauthorized transfers (data extrusion or exfiltration) from compromised internal machines or insiders—rogue employees or individuals abusing resources from within.
A packet-filter firewall is configured by an administrator. It contains a list of rules of the form ¡condition, action¿. In a "firstmatching rule" firewall, the action taken for a packet is that specified by the first rule whose condition it satisfies. The primary actions are:

- ALLOW (permit packet to pass);
- DROP (silently discard the packet—a type-1 deny); or
- REJECT (drop but also try to inform the source—a type-2 deny).

This might result in sending a TCP RST (reset) packet, or for UDP an ICMP "destination unreachable". In addition to one of the above, a second action may log the packet, e.g., using the syslog general system-logging service. For efficiency, most packet-filter matching rules are based on five TCP/IP header fields (src addr, src port, dst addr, dst port, prot),1 and if ICMP then ICMP type and code. Other header fields (packet size, flags) are sometimes used. More complex rules, and so-called intelligent packet filtering, may involve payload data, e.g., an allow or deny decision based on a payload URL—but examining application payloads is generally beyond the scope of packet filters.

5 References

- http://www.acm.org/sigs/sigcomm/sigcomm2000/conf/paper/sigcomm2000-8-4.pdf
- https://www.sciencedirect.com/science/article/pii/S0167404817301773?via%3Dihub
- https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-felsch.pdf
- https://community.cisco.com/t5/security-documents/how-does-nat-t-work-with-ipsec/ta-p/3119442