IPsec and Virtual Private Networks (VPNs) for Network-Layer Security: Part 2

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2013
- A. Tanenbaum, D. Wetherall, "*Computer Networks*", Fifth Edition, Pearson Education, 2012.
- L. Peterson, B. Davie, "*Computer Networks: A Systems Approach*", Fifth Edition, Morgan Kaufmann, 2012.
- B.L. Menezes, R. Kumar, "*Cryptography, Network Security, and Cyber Laws*", Cengage Learning India Pvt. Ltd., 2018
- W. Stallings, "*Cryptography and Network Security: Principles and Practice*", Pearson Education, 7th edition, 2016

Encapsulating Security Payload (ESP)

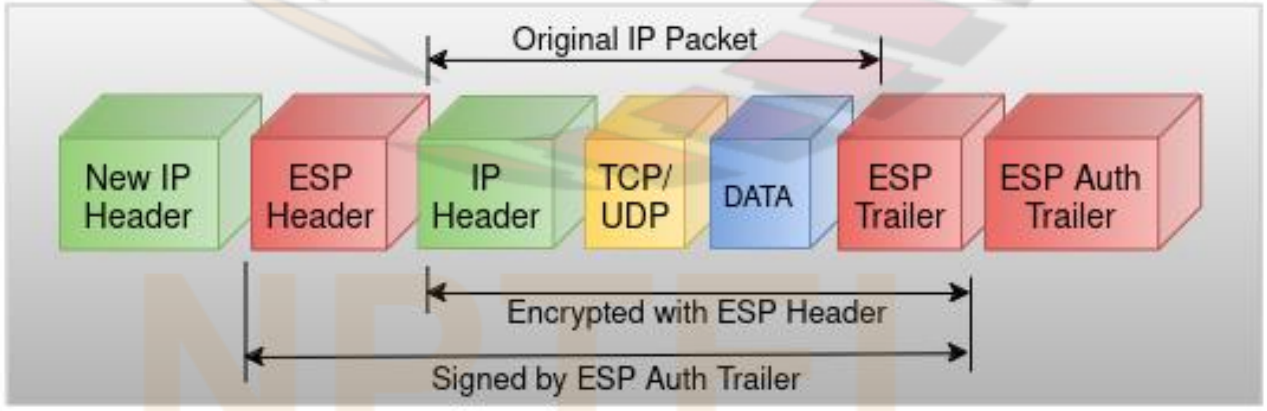
- ESP is an IPsec protocol that provides confidentiality, message integrity and detection of deleted, duplicate or reordered packets
- Confidentiality is provided using encryption
- Message authentication code (MAC) added to packet for message integrity
- Sequence number used to detect addition, deletion or reordering of packets by intruders
- ESP adds a header containing SPI, sequence number, MAC and some other fields to the packet

IPsec Modes

- IPsec supports the **transport mode** and the **tunnel mode**
- Each SA operates in one of these modes
- Transport mode:
  - ESP's payload data is a message for a higher layer such as UDP or TCP
  - IPsec acts as an intermediate protocol sub-layer, just as SSL does between TCP and application layer
  - when an ESP packet is received, its payload is passed to higher layer

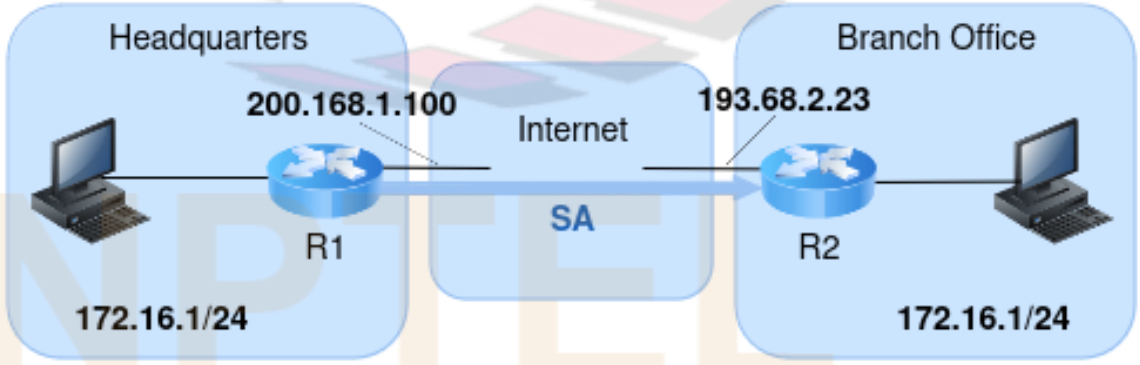
Tunnel Mode

- Commonly used for creating VPNs
- ESP's payload data is itself an IP packet
  - ❑source and destination of inner IP packet may be different from those of outer IP packet
- When an ESP tunnel mode packet is received by a node, its payload is forwarded on as a normal IP packet



Example

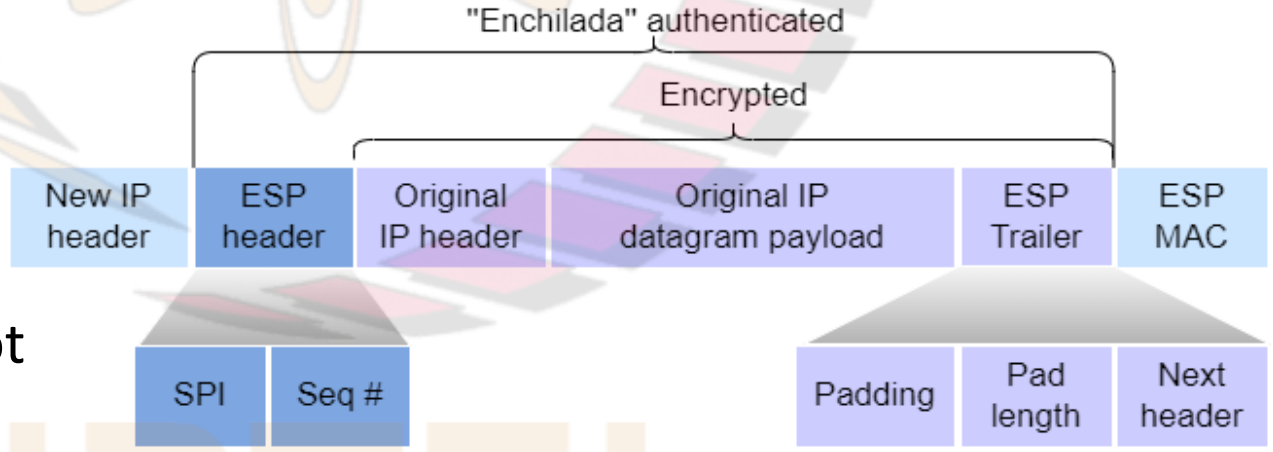
- Consider the VPN in the figure
- Suppose router R1 receives a packet from host 172.16.1.17 (in headquarters network) destined to host 172.16.2.48 (in branch-office network)
- At router R1, this packet becomes the payload of an ESP message sent over the SA to R2
- Router R2 unwraps the payload IP packet and forwards it to 172.16.2.48



ESP Packet Format

- Fig. shows ESP packet when tunnel mode is used
- (Original IP packet + ESP trailer) encrypted using the algorithm and key corresponding to the SA
- ESP header containing SPI and sequence no. added
- A MAC, computed over (ESP header + encrypted information) using the algorithm and key corresponding to SA, added
- Ordinary IP header added
- Recall: sequence numbers not included in packets in SSL; why is sequence number included in ESP?

- ❑ sequence numbers were included in TCP; hence they could be omitted from SSL
- ❑ sequence numbers not included by IP; hence, included by ESP



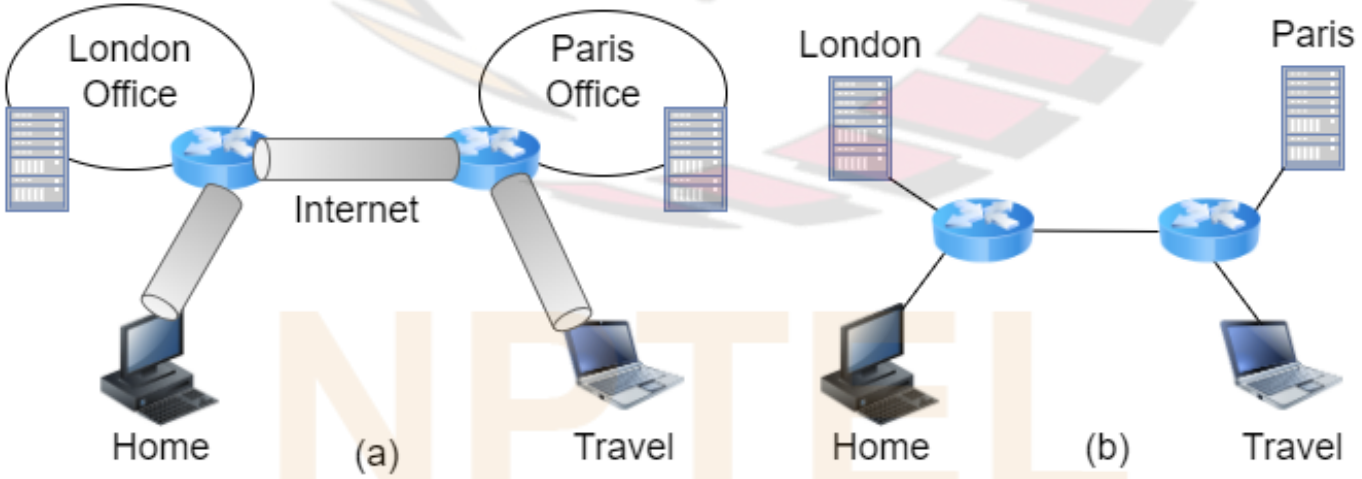
Virtual Private Networks

Private Networks

- Many companies have offices at multiple locations, often in different countries
- Before public Internet appeared, such companies used to lease lines from telephone companies to connect together offices at different locations
- Some companies still do this
- Such a network called a *private network*
- Private networks are very secure
  - ❑ intruders need to physically tap lines to obtain confidential information, which is difficult
- Shortcoming of private networks:
  - ❑ leasing dedicated lines between two points is *costly*
- Hence, when public Internet appeared, companies wanted to use it to connect offices at different locations, but with strong security (as in a private network)
- This led to invention of Virtual Private Networks

Virtual Private Networks

- Common VPN design:
  - ❑ Each office equipped with a gateway router
  - ❑ Tunnels created through Internet between each pair of gateway routers and between gateway routers and employees who are traveling or working from home
    - Tunnel between a pair of nodes created by establishing two IPSec SAs, one in each direction
- VPN is more flexible than a private network built using leased lines:
  - ❑ since tunnels can be set up on demand to any employee (*e.g.*, traveling or working from home) with Internet connection
- However, from the perspective of computers in VPN, topology just like private network case



Virtual Private Networks (contd.)

- Encryption and message integrity achieved since IPsec used
- Also, all traffic between a given pair of gateway routers can be aggregated into two SAs (one in each direction)
- Advantage of doing this:
  - intruders on public Internet cannot find out amount of traffic flowing between any pair of machines
  - hence, VPN defends against “traffic analysis” attacks