IPsec and Virtual Private Networks (VPNs) for Network-Layer Security: Part 1

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

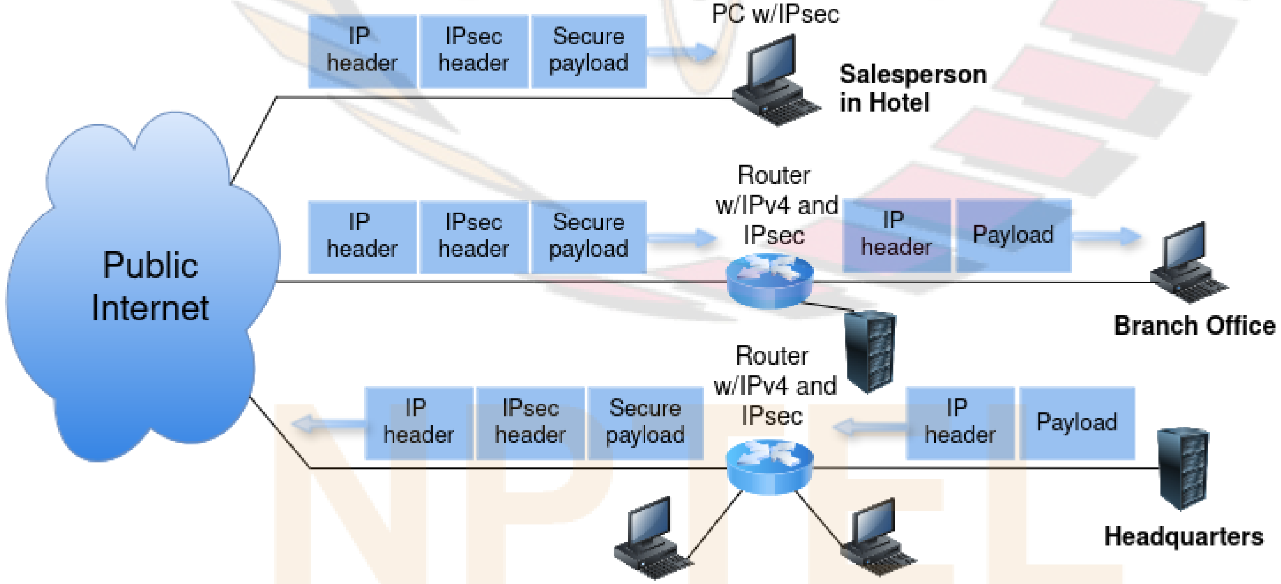
- J. Kurose, K. Ross, “*Computer Networking: A Top Down Approach*”, Sixth Edition, Pearson Education, 2013
- A. Tanenbaum, D. Wetherall, “*Computer Networks*”, Fifth Edition, Pearson Education, 2012.
- L. Peterson, B. Davie, “*Computer Networks: A Systems Approach*”, Fifth Edition, Morgan Kaufmann, 2012.
- 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

Overview of IPsec

- IPsec can be used to establish a secure connection between the network layer entities at two nodes (hosts or routers)
- Provides the following security services:
  - ❑Confidentiality:
    - o the payload (*e.g.*, transport layer header and application layer data) encrypted
  - ❑End-point Authentication
  - ❑Message Integrity
  - ❑Receiver can detect duplicate packets that attacker may insert and deletion or reordering of packets

Overview of Virtual Private Networks

- IPsec widely used to establish Virtual Private Networks, *e.g.*:
  - ❑ suppose a company has offices at multiple locations and wants to securely connect together all the machines in all the offices via public Internet
  - ❑ also wants to connect end systems of employees not currently in office (*e.g.*, salespersons, employees working from home) to office network
  - ❑ Virtual Private Network can be used to achieve this
  - ❑ *connectivity is over public Internet; however, from users' point of view, just like a private network using leased lines*



Overview of IPsec Operation

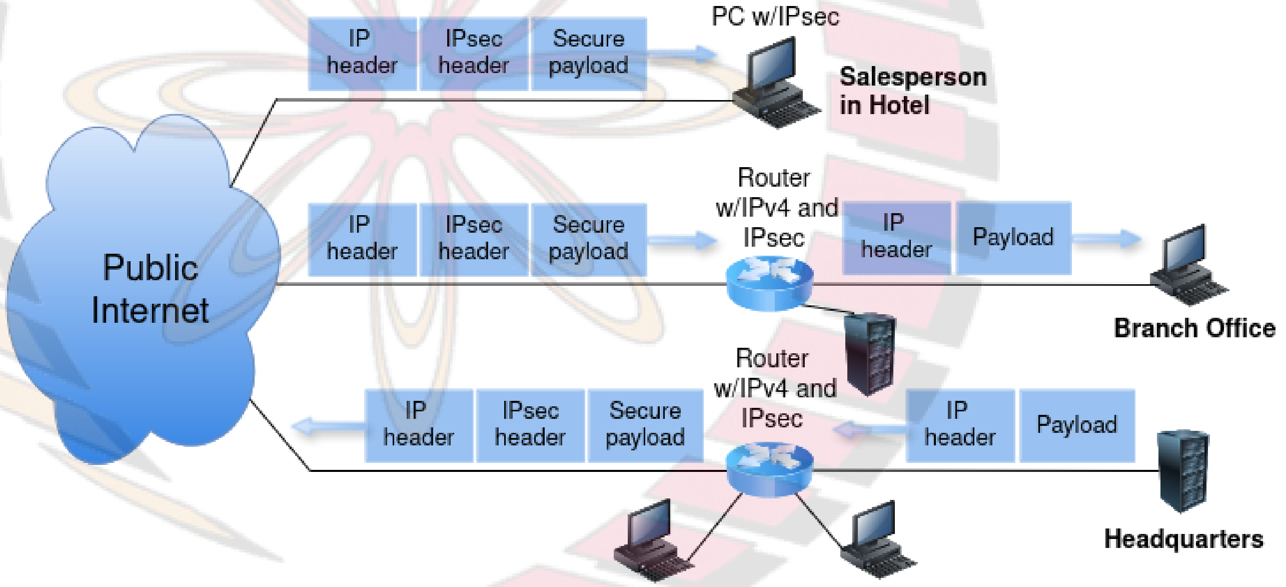
- Suppose a secure connection between the network layer entities at two nodes, R1 and R2, is to be created
- Two network-layer logical connections (one in each direction), called *Security Associations (SA)* are established over which data can be securely exchanged
- To establish an SA from router R1 to router R2 (or R2 to R1), they first need to authenticate each other, agree on the encryption and message integrity algorithms and keys
  - ❑this is done by R1 and R2 by executing the **Internet Key Exchange (IKE)** protocol

Security Association (SA)

- IPsec packets are sent between the network layer entities at two nodes (hosts or routers)
- Before sending IPsec packets from a source entity to destination entity, a network-layer logical connection, called SA, is established
- An SA is simplex, *i.e.*, unidirectional from source to destination
- If both entities want to send secure packets to each other, then two SAs, one in each direction, need to be established

Example

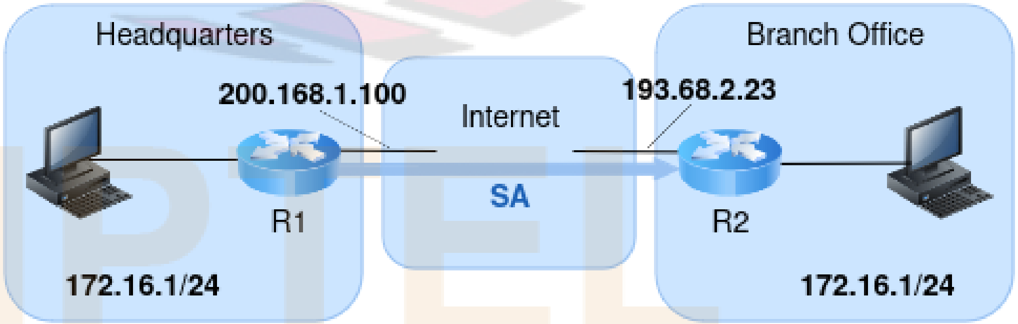
- The corporate VPN in fig. consists of a headquarters office, a branch office and n traveling salespersons
- Suppose there is bi-directional IPsec traffic between headquarters and branch office and between the headquarters and each of the salespersons
- Total no. of SAs:
  - ❑ $2n+2$



- *Note*: in this e.g., not all traffic sent into Internet by gateway routers or by salespersons' laptops will be IPsec secured
  - ❑*e.g.*, if a host in headquarters accesses a Web server owned by Amazon or Google, would use SSL and not IPsec

State Information About an SA

- Consider an SA from router R1 to router R2
- Routers R1 and R2 maintain the following state information about this SA:
  - A 32 bit identifier called Security Parameter Index (SPI); the pair (SPI, destination IP address) uniquely identifies an SA
  - The origin interface (e.g., 200.168.1.100) and destination interface (e.g., 193.68.2.23)
  - The algorithm to be used for encryption (*e.g.*, 3DES with CBC)
  - The encryption key
  - The algorithm to be used for MAC computation (*e.g.*, MD5)
  - The authentication key
- An IPsec entity typically maintains state information for many SAs; in above example, the headquarters gateway router maintains state information for $(2n + 2)$ SAs
  - stored in a database called **Security Association Database (SAD)**
- Whenever router R1 needs to construct an IPsec packet for forwarding over above SA, it accesses state information of the SA to find out how it should encrypt packet and compute the MAC
  - similarly, router R2 uses state information to find out how it should decrypt packet and verify the MAC for a packet that is received over the SA



Key Management in IPsec using the Internet Key Exchange (IKE) Protocol

- To establish an SA from router R1 to router R2, they first need to authenticate each other, agree on the encryption and message integrity algorithms and keys and SPI
- Done using IKE protocol
- Has following similarities with SSL handshake:
  - ❑the two entities exchange certificates (containing their public keys) for authentication
  - ❑negotiate encryption and MAC computation algorithms
  - ❑exchange key material, from which the encryption and authentication keys are derived
- Some differences from SSL handshake (details later)