Week 10: Applications of Cryptography III

Dr. Qublai Ali Mirza

University of Gloucestershire

qalimirza@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

Overview

Virtual Private Network (VPN)

- allow a private network to run over a public network providing several security properties.
- Provide confidentiality, integrity and authentication.
- There are two categories of VPN, namely:
  - Remote Access VPN
  - Site-to-Site VPN

Remote Access VPN

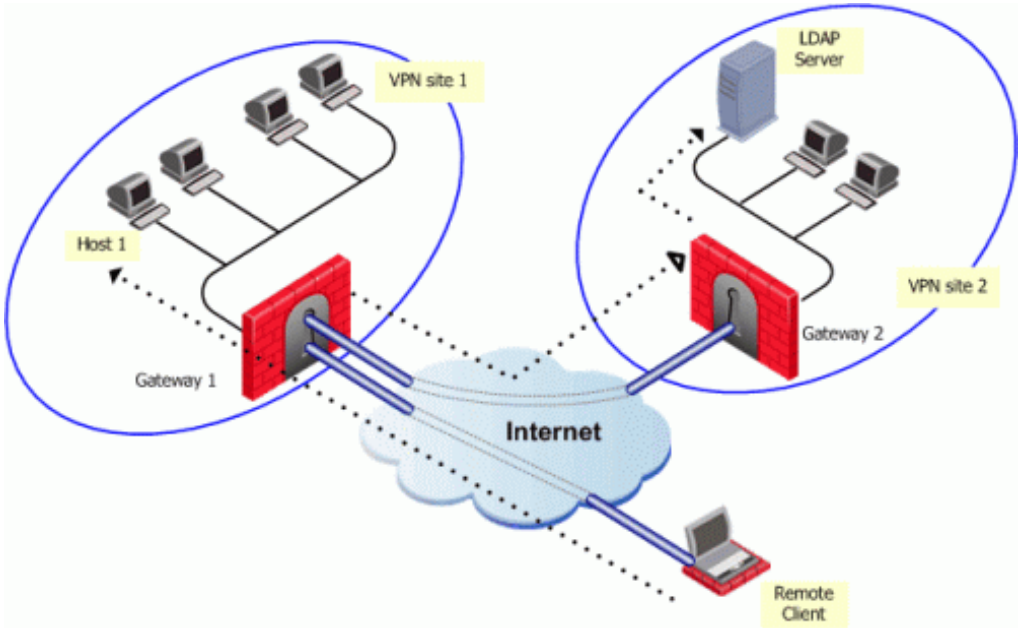

Figure: Remote access VPN, from [**checkpointVPN**]

Site-to-Site VPN

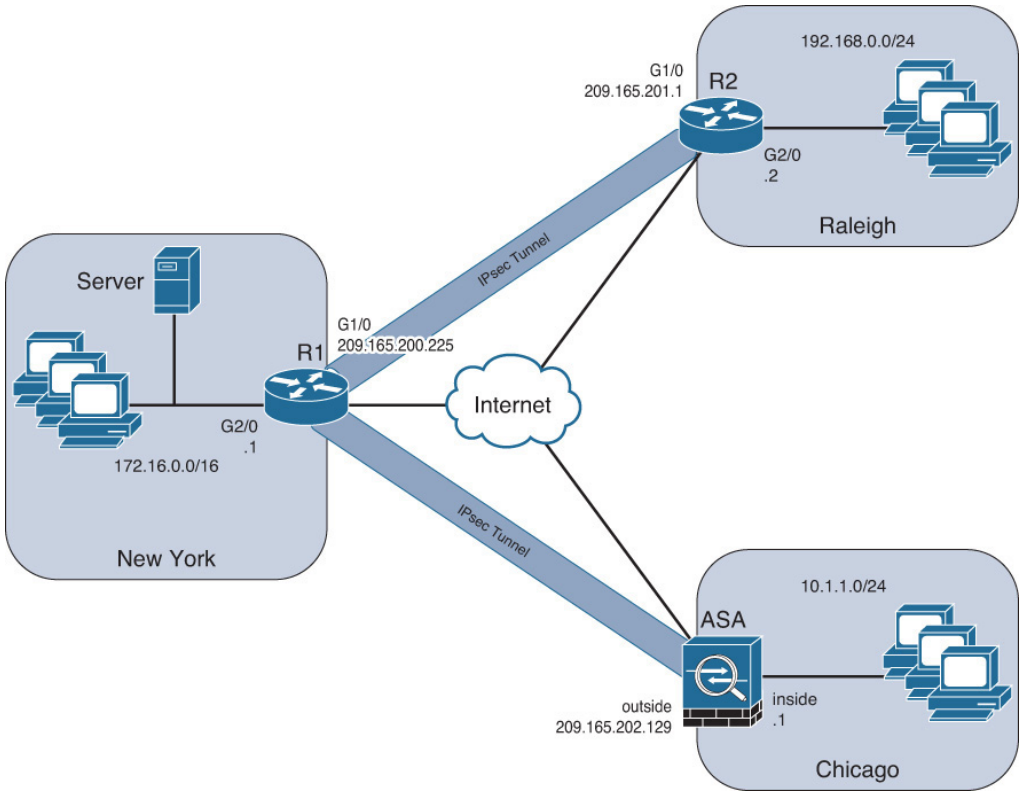

Figure: Site-to-Site VPN, from [**safaribooksVPN**]

VPN Protocols

- Point-to-Point Tunnelling Protocol (PPTP);
- SSL;
- TLS;
- Layer 2 Tunnelling Protocol (L2TP);
- Internet Protocol Security (IPSec).

Point-to-Point Tunnelling Protocol (PPTP)

- Modified version of Generic Routing Encapsulation (GRE)
- Uses TCP port 1723.
- Defined in RFC 2637.
- Supported on Windows, MacOS and Linux.

Layer Two Tunnelling Protocol (L2TP)

- Released in 1999. RFC 2661.
- Latest version L2TPv3 provides additional security.
- Implemented using UDP.
- Uses UDP ports 500, 1701 and 4500.

Overview

- A framework of open standards developed by the Internet Engineering Task Force (IETF)
- Designed to support secure and authenticated communications over IP networks
- Mandatory for *IPv6*, but optional for *IPv4*

IPSec overview

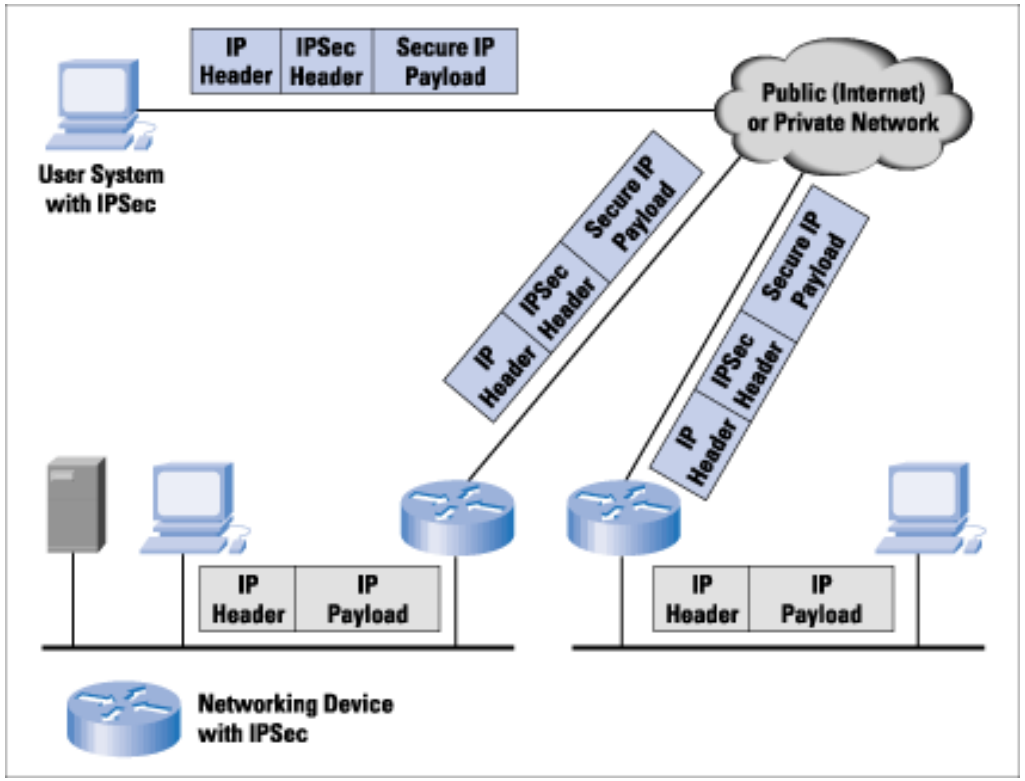

Figure: IPSec overview, from [**stallings2006cryptography**]

Applications of IPSec

- Secure connections over the Internet
- Support remote connections
- Improve e-commerce transactions over the Internet

Architecture

- Authentication Header (AH)
- Encapsulating Security Payload(ESP)
- Security Associations (SA)

Authentication Header (AH)

- Provides data integrity and authentication support
- Authenticates both the IP payload *and* all IP header components
- Designed to protect against:
  - Address spoofing
  - Replay attacks
- Features the use of *ICV* (Integrity Check Value) in the Authentication Data field

Authentication Header

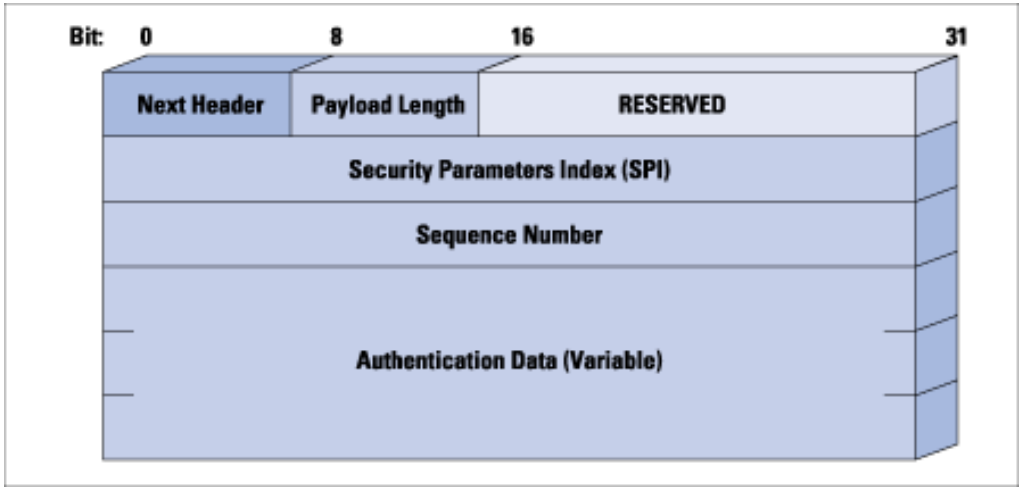

Figure: Authentication Header, from [**ciscoAH**]

Encapsulating Security Payload (ESP)

- Provides confidentiality of data/services
- Achieved through encryption
- Protects only the IP payload, not the IP header
- If enabled, all content after the ESP header is encrypted

Encapsulating Security Payload (ESP)

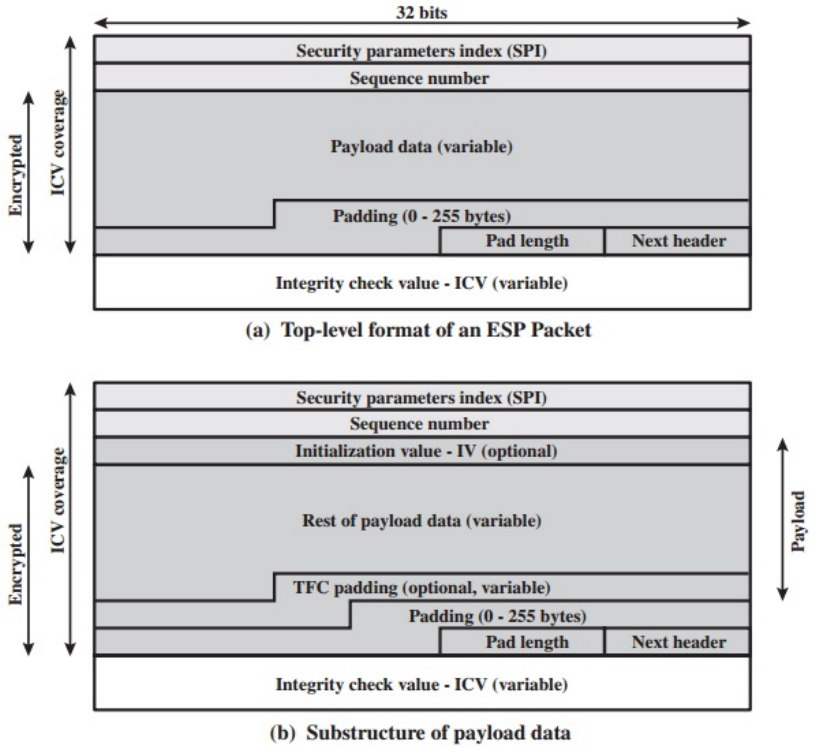

Figure 19.5 ESP Packet Format

Figure: ESP packet format, from [**stallings2006cryptography**]

Security Associations

- Referrs to a connection which is protected through IPSec
- Is a Layer-3 protocol
- May either be end-to-end or link-to-link
- Two modes of packet encapsulation
  - Transport mode
  - Tunnel mode

Transport vs. Tunnel mode

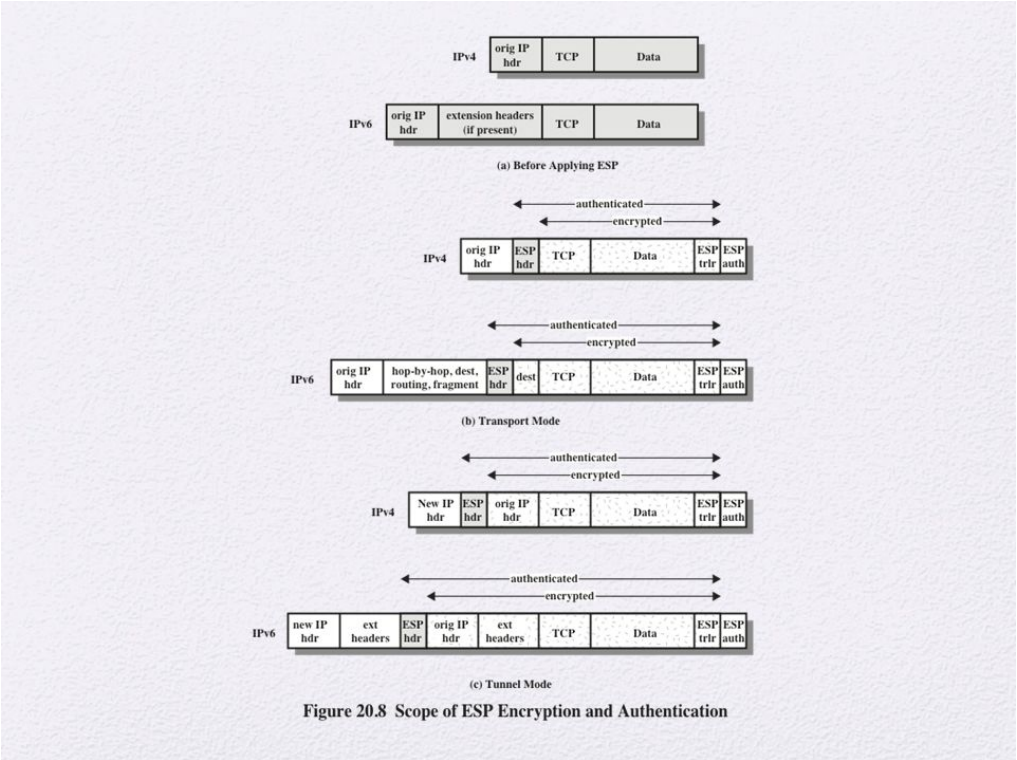

Figure 20.8 Scope of ESP Encryption and Authentication

Figure: Transport vs. Tunnel mode, from [**stallings2006cryptography**]

UNIVERSITY OF GLOUCESTERSHIRE

Secure Socket Layer (SSL)

- Developed by Netscape in 1994
- Features RSA encryption for data encryption
- Operates at the *Transport Layer* (Layer 4) in the OSI model
- Protects the transmission of data over the network

SSL Session establishment

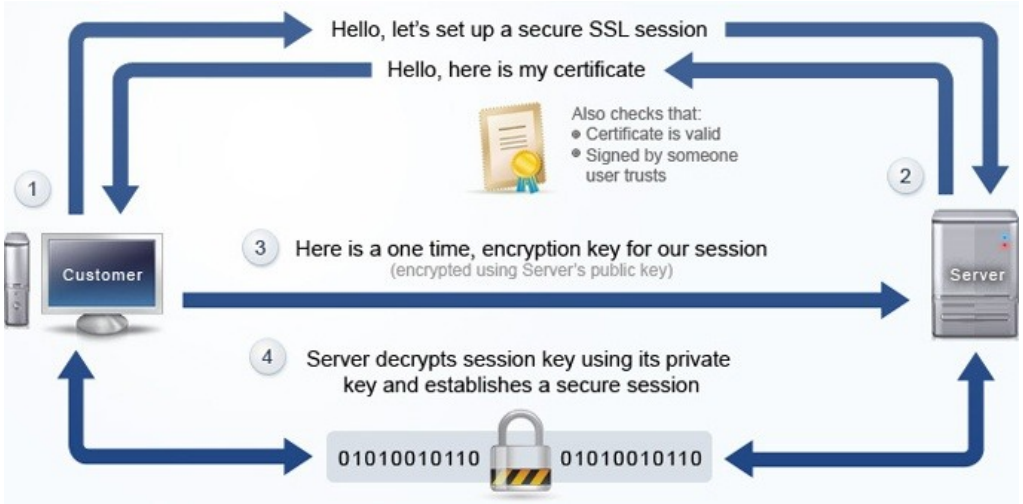

Figure: SSL setup, from [**MScSSL**]

Transport Layer Security

- Also used for securing network traffic between the browser and server
- Operates alongside SSL at the Transport Layer
- Provides encryption, authentication and data integrity
- Protects FTP, SMTP, NNTP and Extensible Messaging and Presence Protocol (XMPP) when used alongside SSL

TLS Operation

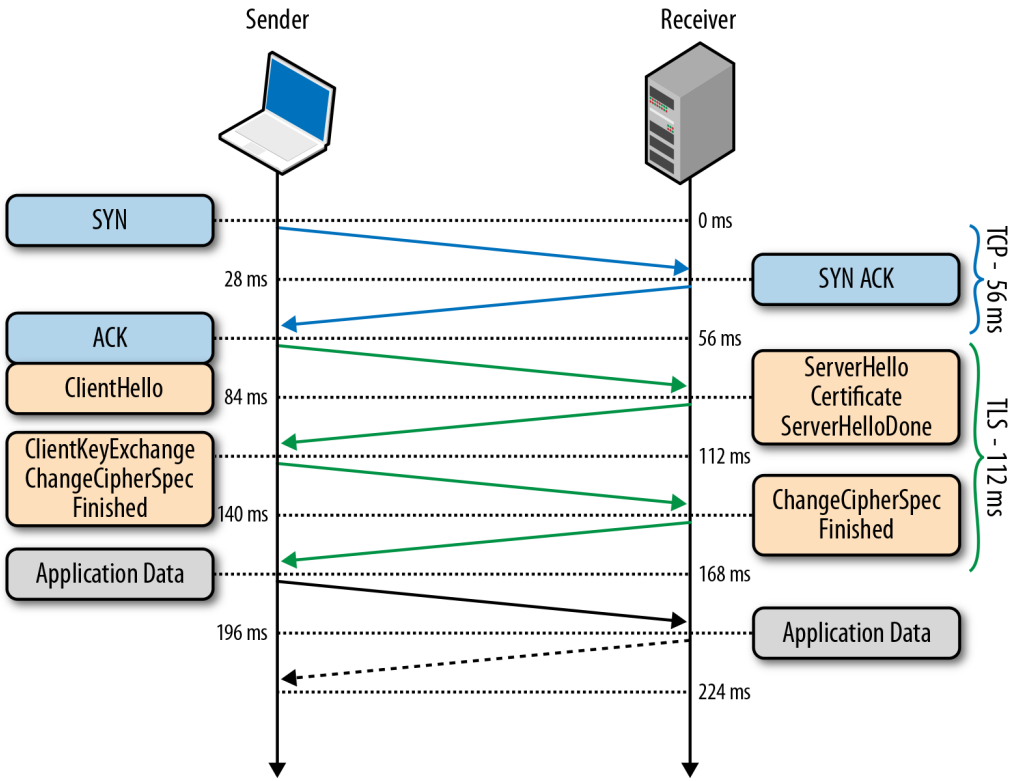

Figure: TLS operation, from [**TLSDiagram**]

Bringing it all together

- Today we looked at *applications of cryptography*
- We looked at how we protect data-in-transit
- We also at approaches such as IPSEC, SSL, and TLS

References I

Q & A