

11/8/06

1. Zeeshan - Problem 1 in Homework 4

2. Chapter 5 & 6 -
Two models.

3. Chapter 17, 18

4. IPsec SSL

A → B:

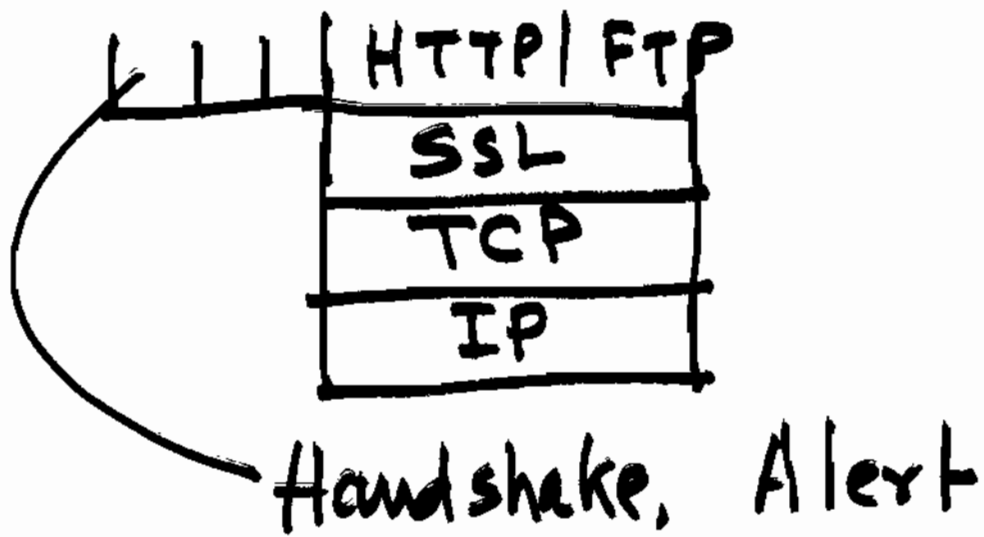
SSL 10/11/06
IPSec - 10/16/06

HTTP	FTP
TCP	
IP	

(1) Security at network level

HTTP	FTP
TCP	
IP/IPsec	

SSL - End-to-End level.



Compression, Encryption,
MAC

Client — Server

client $\longrightarrow$ Server.

client-Hello.

T, N, Cipher Suite, Compression
method

Connection & Session

$$H \parallel E_K [CM[T \parallel N \parallel CS \parallel CM] \parallel \\ MAC[CM[T \parallel N \parallel CS \parallel CM]]]$$