

Secure Socket Layer (SSL) and Transport Layer Security (TLS)

Raj Jain

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

<http://www.cse.wustl.edu/~jain/cse571-09/>



- ❑ History and overview of SSL/TLS
- ❑ Products and Implementations
- ❑ Datagram Transport Layer Security (DTLS)
- ❑ Current TLS Issues and Extensions
- ❑ Secure Remote Password (SRP)

First part from the textbook. Remainder from Wikipedia and IETF

Key Features

- ❑ User level \Rightarrow Not operating system specific
- ❑ Uses TCP \Rightarrow Reliable transmission
(No retransmissions at application layer)
- ❑ Features:
 - Crypto negotiation
 - Key Generation for encryption and Integrity
 - Authentication:
 - ❑ Servers use Certificates
 - ❑ Clients use password or certificates