SSL
SECURE SOCKET LAYER
In The Protocol Architecture

- Application
- Presentation
- Session
- Transmission
- Network
- Data link
Features

- Endpoint authentication
- Secure transport session
  - Encrypted
  - Authenticated
- TLS: Transport Layer Security
Widely Deployed

- POPS, Secure IMAP, Secure SMTP, HTTPS, SFTP
- Usually different port
- HTTP: 80, HTTPS: 443
- Possibly same: STARTTLS
SSL Handshake

Is cert OK?

ClientHello

^YS>D”_)*#NS

Generate symmetric key

Session key encrypted with server public key
Parameter Negotiation

→ Client offers
  → List of cyphers
  → Parameters
→ Server
  → Picks cyphers
  → Might requests client cert
Security Features

➤ Only hello and server cert are in clear
➤ A pair of sessions keys per direction
   ➤ Encryption
   ➤ Authentication
➤ Periodically changed
SSL Record Protocol

- Header
- Authentication (MAC)
- Max 32KB
- Same data protection as IPsec
- No IP header protection