SSL
SECURE SOCKET LAYER
In The Protocol Architecture

Application
Presentation
Session
Transport
Network
Data link

Telnet
FTP
SMTP
HTTP

RTP
SNMP
NFS
XDR
RPC

TCP
UDP
Routing protocols
IP
ARP
IGMP
ICMP

Data link
Network
Transport
Session
Presentation
Application
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

1. ClientHello
2. ServerHello
3. Certificate
4. Session key encrypted with server public key
5. Generate symmetric key
6. Is cert OK?

^YS>D"_)*#NS

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