Module 2.2
Internet Security Protocols

Ravi Sandhu
Spring 2021
Internet Security Protocols

TCP RFC 793
Sept. 1981
IPv4 RFC 791
Sept. 1981

Where to inject security?
Internet Security Protocols

TCP RFC 793  
Sept. 1981
IPv4 RFC 791  
Sept. 1981

IPsec, 1998
SSL, 1994
SET, 1996
Internet Security Protocols

- IPsec, 1998
- SSL, 1994

Some successes
Many failures

Dozens of other security protocols

Half successful
SSL, 1994

Largely failed
IPsec, 1998
1-way vs 2-way SSL

1-way SSL

Client (Browser)  1-way SSL  Server

2-way SSL

Client (Browser)  2-way SSL  Server
1-way vs 2-way SSL

1-way SSL

- Client (Browser)
- 1-way SSL
- Server
- RSA encryption certificate

2-way SSL

- Client (Browser)
- 2-way SSL
- Server
- RSA encryption certificate
- RSA signature certificate
1-way vs 2-way SSL

1-way SSL

Client (Browser) -> 1-way SSL -> Server

LESS SECURE
Phishing
Man-in-the-middle

2-way SSL

Client (Browser) <-> 2-way SSL <-> Server

MORE SECURE
Phishing
Man-in-the-middle
1-way vs 2-way SSL

1-way SSL

Client (Browser) 1-way SSL Server

LESS SECURE
Phishing
Man-in-the-middle

MASS DEPLOYMENT

2-way SSL

Client (Browser) 2-way SSL Server

MORE SECURE
Phishing
Man-in-the-middle

MINIMAL DEPLOYMENT
The SSL Lesson

- Client-less trumps client-full
- Start-ups (SSL) trump committees (IPSEC)