Module 2.5
SSL Man-in-the-Middle Attack

Ravi Sandhu

Spring 2021
1-way SSL MITM

Client (Browser) <https> Server

RSA encryption certificate
SSL Lock Icon Evolution by Browser

IE:
- v5.6
- v7.8
- v9

Firefox:
- v2
- v3.4
- v3.4 (OSX)

Chrome:
- v3.4

Safari:
- OSX
- Win

Opera:
- 

Konqueror:
- √

http://elie.im/blog/
1-way SSL MITM

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

http -> https

RSA encryption certificate
1-way SSL MITM

Client (Browser) → MITM → Server

https → https

RSA encryption certificate
1-way SSL MITM

Client (Browser) → MITM → Server

- https
- fake server certificate
- RSA encryption certificate

World-Leading Research with Real-World Impact!
Server-Side Masquerading

Bob
Web browser

1 way SSL

www.host.com
Web server

Ultratrust
Security Services

www.host.com
Server-Side Masquerading

Bob
Web browser

www.host.com
Web server

1-way SSL

BIMM Corporation

Mallory’s Web server

Ultratrust Security Services

www.host.com

www.host.com
Server-Side Masquerading

Bob
Web browser

1-way SSL

www.host.com
Web server

1-way SSL

Mallory’s
Web server

Ultratrust
Security
Services

www.host.com

BIMM
Corporation

Ultratrust
Security
Services

www.host.com
1-way SSL MITM

Client (Browser) → MITM → Server

https

fake server certificate

RSA signature certificate

fake client certificate

RSA encryption certificate