Module 2.5
SSL Man-in-the-Middle Attack

Ravi Sandhu

Spring 2021

World-Leading Research with Real-World Impact!

**Client
(Browser)** ←——————————— https ———————————→ **Server**

RSA encryption
certificate

World-Leading Research with Real-World Impact!

SSL Lock Icon Evolution by Browser

http://elie.im/blog/

```
┌──────────────┐         ┌──────────────┐         ┌──────────────┐
│   Client     │◄───────►│    MITM      │◄───────►│   Server     │
│  (Browser)   │         │              │         │              │
└──────────────┘  http   └──────────────┘  https  └──────────────┘
```

RSA encryption
certificate

Client
(Browser)   ←→   MITM   ←→   Server

https   https

RSA encryption
certificate

Client (Browser) ←———— https ————→ **MITM** ←———— https ————→ **Server**

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

Bob
Web browser

www.host.com
Web server

1-way SSL

1-way SSL

Ultratrust
Security
Services

Mallory's
Web server

BIMM
Corporation

www.host.com

www.host.com

I·C·S
The Institute for Cyber Security

UTSA

Client (Browser) ←→ https ←→ MITM ←→ https ←→ Server

fake server certificate

RSA encryption certificate

RSA signature certificate

fake client certificate