INFS 767

Secure Electronic Commerce

Lecture 7

PKI and Trust

Prof. Ravi Sandhu

PUBLIC-KEY INFRASTRUCTURE PKI

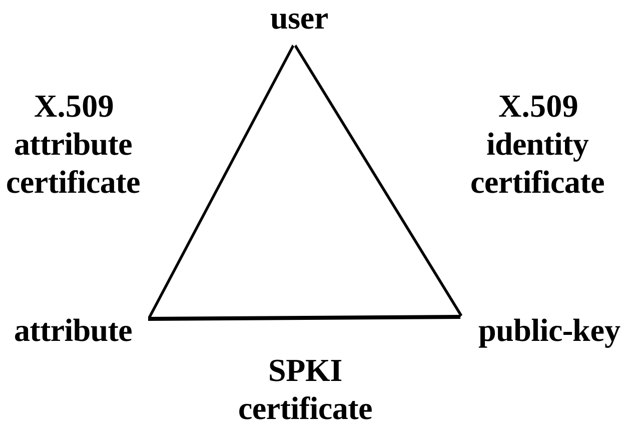
- **“The goal of a public-key infrastructure (PKI) is to enable secure, convenient, and efficient discovery of public keys.”**

  -- Radia Perlman, IEEE Network, Nov/Dec 1999
- **Rather say usage instead of discovery**
  - **Discovery may be the long term problem**
  - **Current problem is usage**

PUBLIC-KEY USAGE

- In most cases public-key “discovery” is achieved by explicit transport of certificate chains
  - SSL for example
- Public-key “discovery” as such is required only for non-interactive protocols (email) for
  - Public-key encryption
  - Public-key key agreement

THE CERTIFICATE TRIANGLE



user

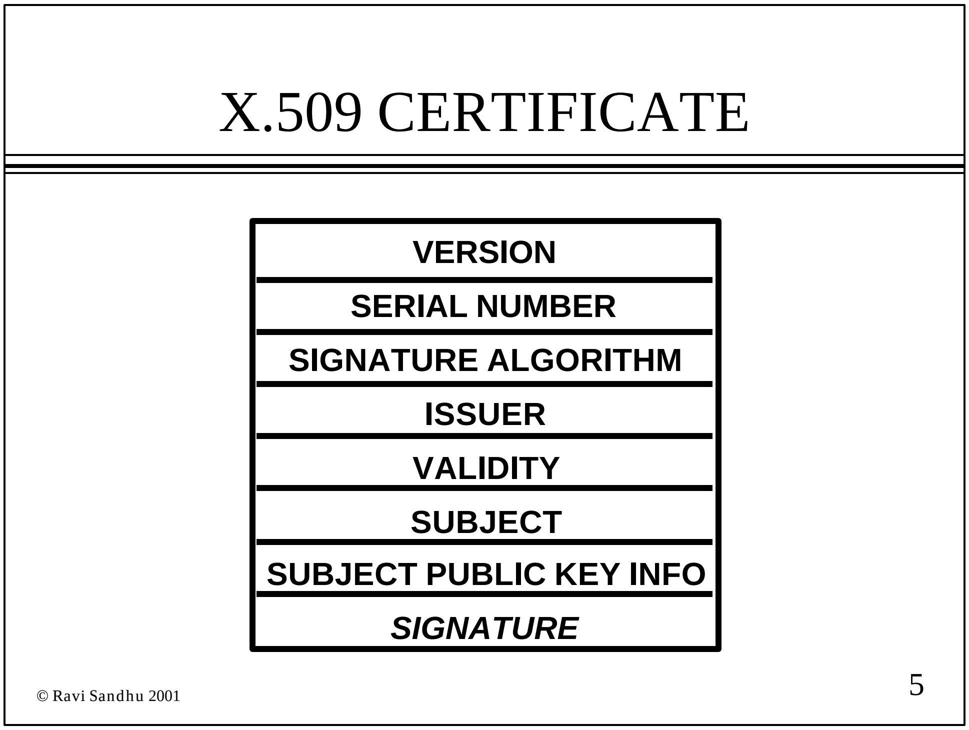
X.509 attribute certificate

X.509 identity certificate

attribute

public-key

SPKI certificate



X.509 CERTIFICATE

VERSION

SERIAL NUMBER

SIGNATURE ALGORITHM

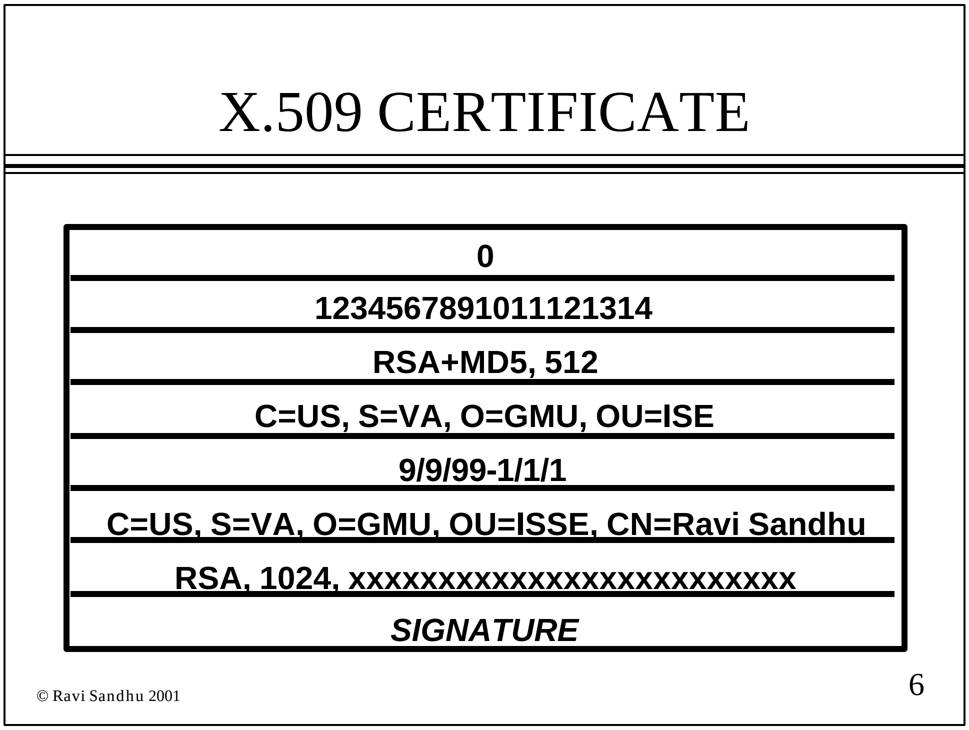
ISSUER

VALIDITY

SUBJECT

SUBJECT PUBLIC KEY INFO

SIGNATURE



X.509 CERTIFICATE

0

1234567891011121314

RSA+MD5, 512

C=US, S=VA, O=GMU, OU=ISE

9/9/99-1/1/1

C=US, S=VA, O=GMU, OU=ISSE, CN=Ravi Sandhu

RSA, 1024, xxxxxxxxxxxxxxxxxxxxxxxxx

SIGNATURE

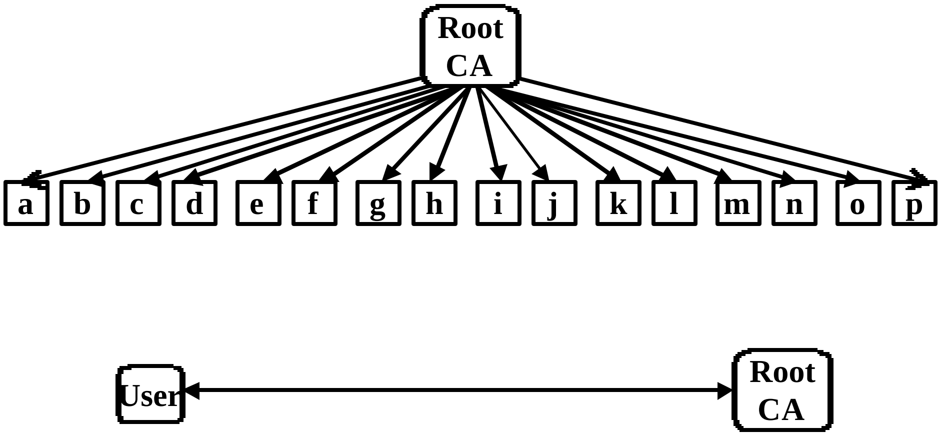
SERVER-SIDE SSL (OR 1-WAY) HANDSHAKE WITH RSA

```
                Client                                      Server

                ClientHello              -------->
                                                       ServerHello
Handshake                                              Certificate
Protocol

                                         <--------     ServerHelloDone

                ClientKeyExchange

                [ChangeCipherSpec]
                Finished                 -------->
                                                    [ChangeCipherSpec]
                                         <--------            Finished
----------------------------------------------------------------------
                Application Data         <------->    Application Data
Record
Protocol
```

CLIENT-SIDE SSL (OR 2-WAY) HANDSHAKE WITH RSA

```
                Client                                      Server

                ClientHello              -------->
                                                       ServerHello
Handshake                                              Certificate
Protocol
                                                    CertificateRequest
                                         <--------     ServerHelloDone
                Certificate
                ClientKeyExchange
                CertificateVerify
                [ChangeCipherSpec]
                Finished                 -------->
                                                    [ChangeCipherSpec]
                                         <--------            Finished
----------------------------------------------------------------------
                Application Data         <------->    Application Data
Record
Protocol
```

SINGLE ROOT CA MODEL



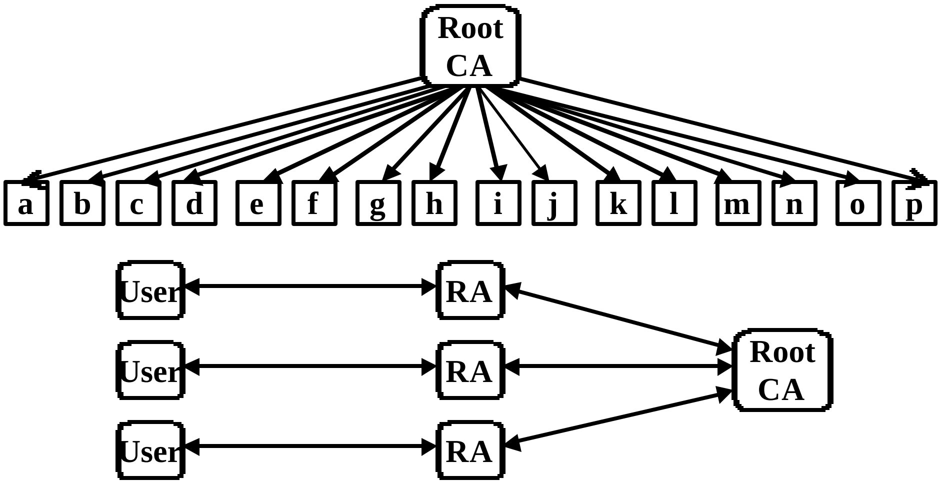
Root CA

a b c d e f g h i j k l m n o p

User

Root CA

SINGLE ROOT CA MULTIPLE RA’s MODEL



Root CA

a b c d e f g h i j k l m n o p

User

User

User

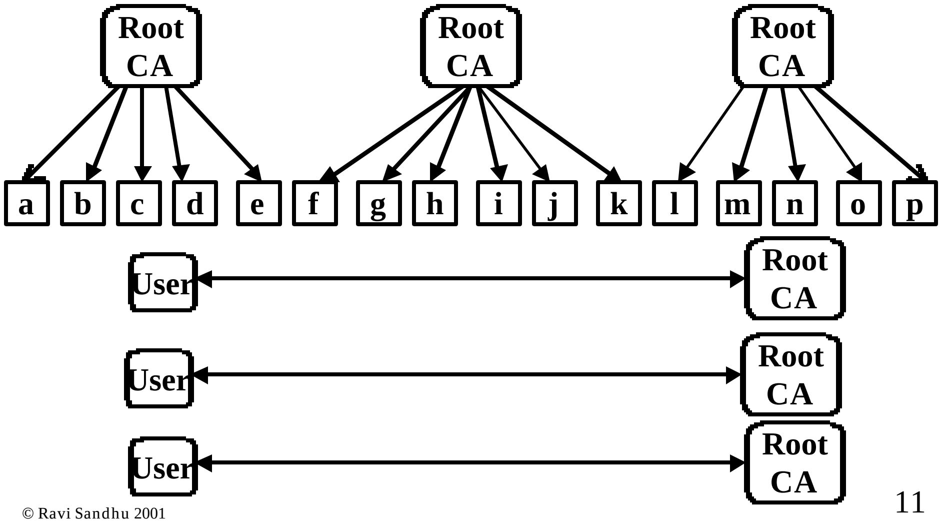
RA

RA

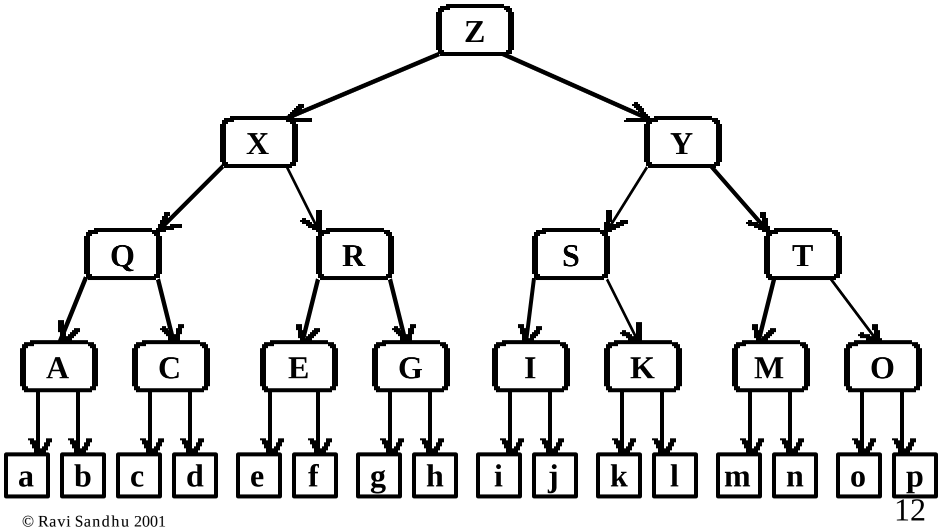
RA

Root CA

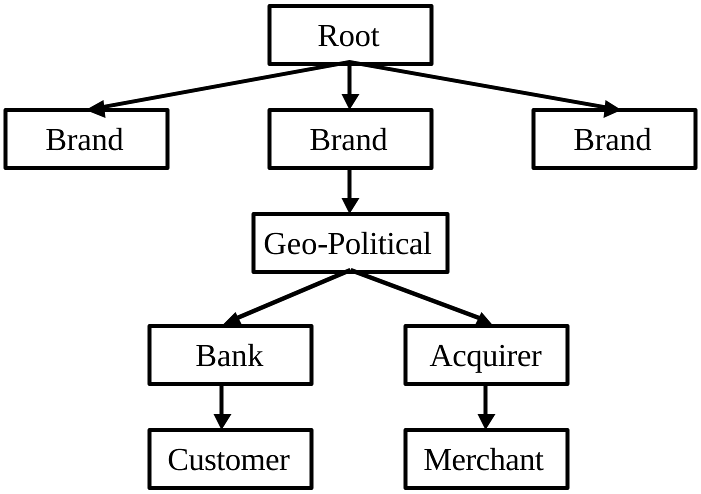
MULTIPLE ROOT CA's MODEL



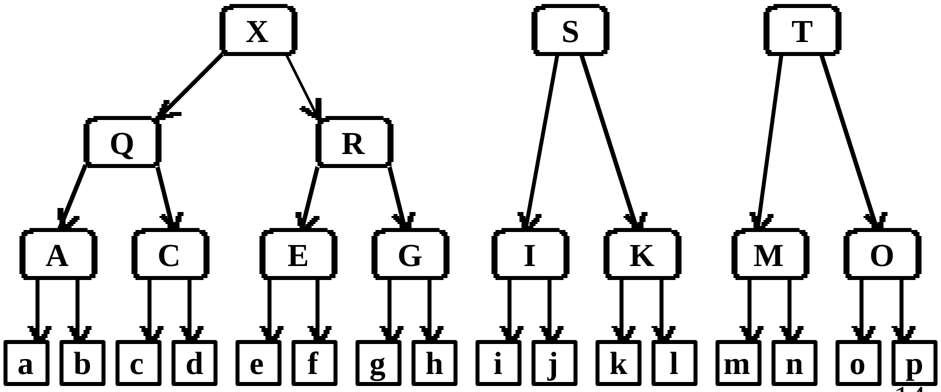
ROOT CA PLUS INTERMEDIATE CA's MODEL



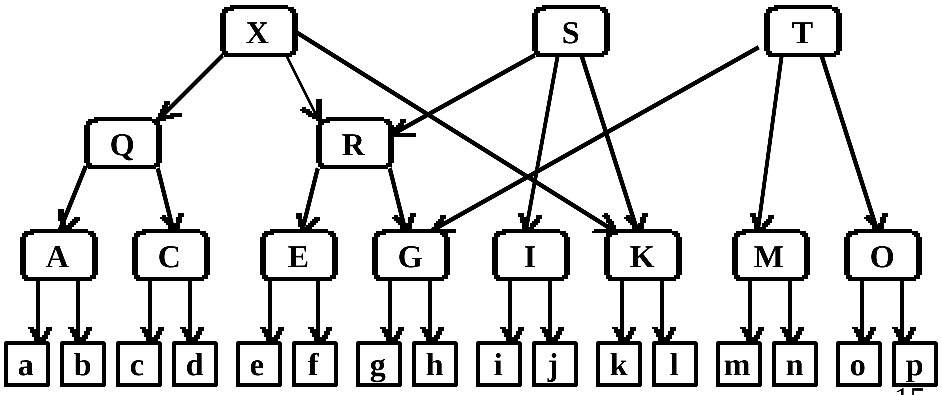
SECURE ELECTRONIC TRANSACTIONS (SET) CA HIERARCHY



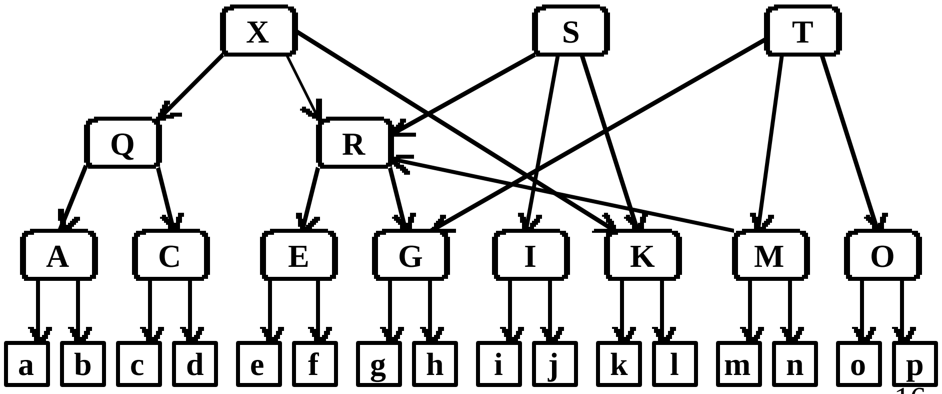
MULTIPLE ROOT CA's PLUS INTERMEDIATE CA's MODEL



MULTIPLE ROOT CA’s PLUS INTERMEDIATE CA’s MODEL



MULTIPLE ROOT CA’s PLUS INTERMEDIATE CA’s MODEL



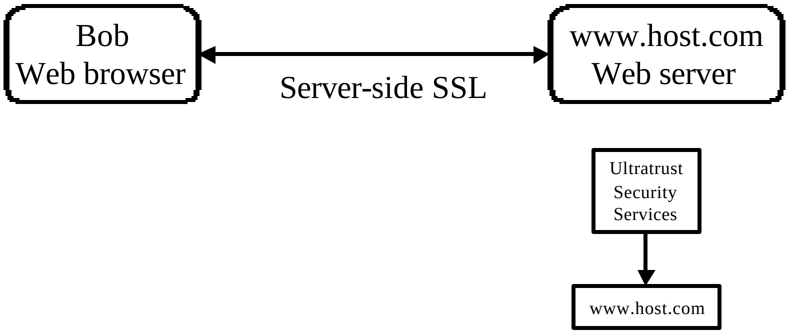
MULTIPLE ROOT CA's PLUS INTERMEDIATE CA's MODEL

- ❖ Essentially the model on the web today
- ❖ Deployed in server-side SSL mode
- ❖ Client-side SSL mode yet to happen

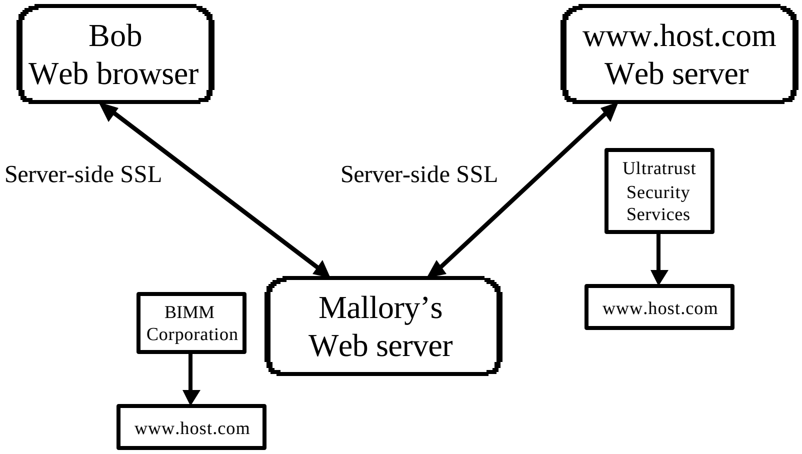
SERVER-SIDE SSL (OR 1-WAY) HANDSHAKE WITH RSA

```
                Client                                               Server

                ClientHello                 -------->
                                                                ServerHello
Handshake                                                       Certificate
Protocol

                                            <--------        ServerHelloDone

                ClientKeyExchange

                [ChangeCipherSpec]
                Finished                    -------->
                                                         [ChangeCipherSpec]
                                            <--------              Finished
-----------------------------------------------------------------------------
                Application Data            <------->      Application Data
Record
Protocol
```

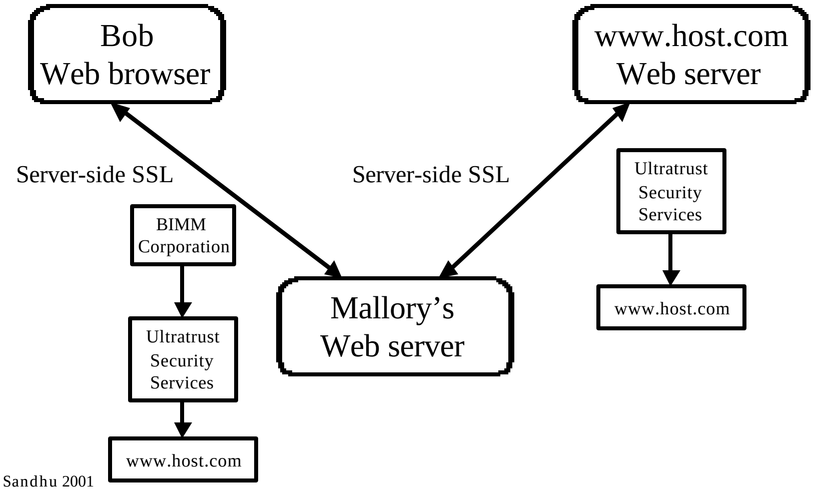
SERVER-SIDE MASQUARADING



SERVER-SIDE MASQUARADING



SERVER-SIDE MASQUARADING



Bob
Web browser

www.host.com
Web server

Server-side SSL

Server-side SSL

BIMM
Corporation

Ultratrust
Security
Services

www.host.com

Mallory's
Web server

Ultratrust
Security
Services

www.host.com

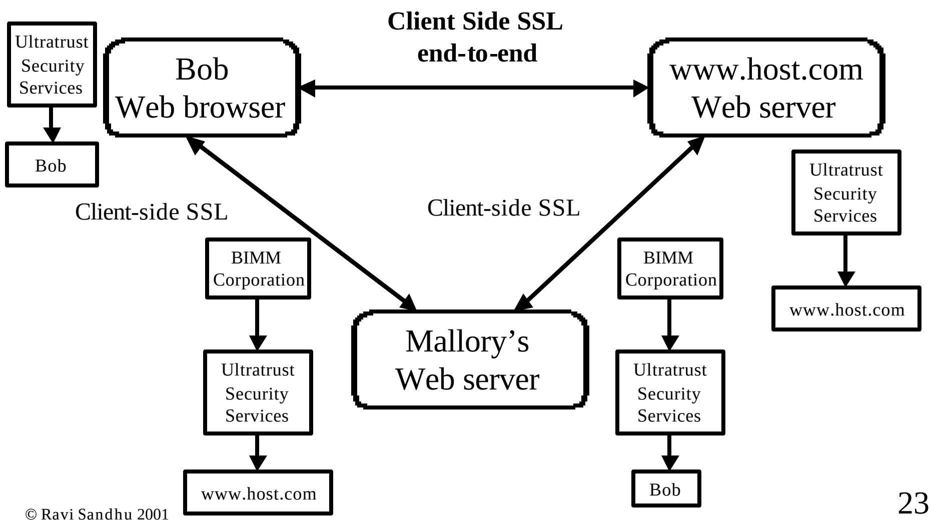
CLIENT-SIDE SSL (OR 2-WAY) HANDSHAKE WITH RSA

Handshake
Protocol

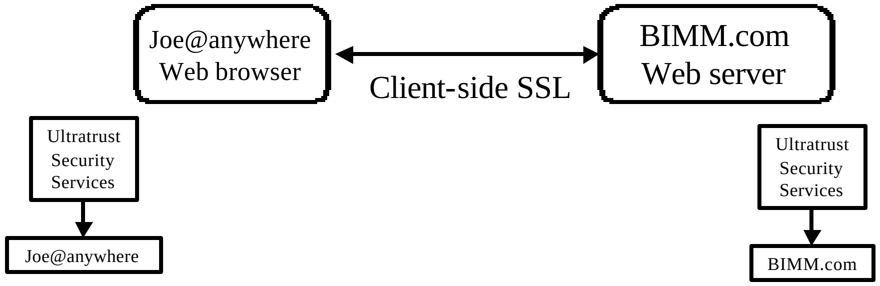
```
Client                                         Server

ClientHello             -------->
                                          ServerHello
                                          Certificate

                                   CertificateRequest
                        <--------     ServerHelloDone
Certificate
ClientKeyExchange
CertificateVerify
[ChangeCipherSpec]
Finished                -------->
                                   [ChangeCipherSpec]
                        <--------            Finished
Application Data        <------->    Application Data
```

Record
Protocol

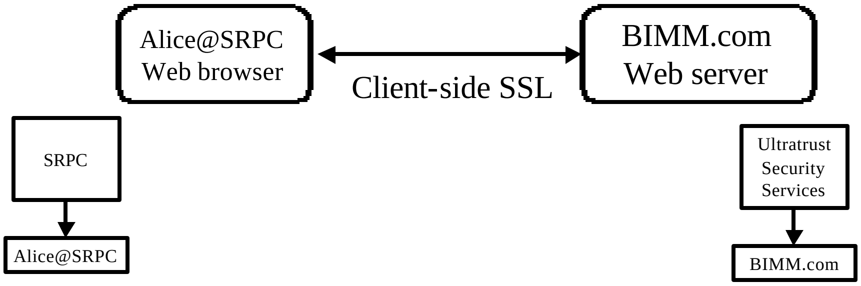
MAN IN THE MIDDLE MASQUARADING PREVENTED



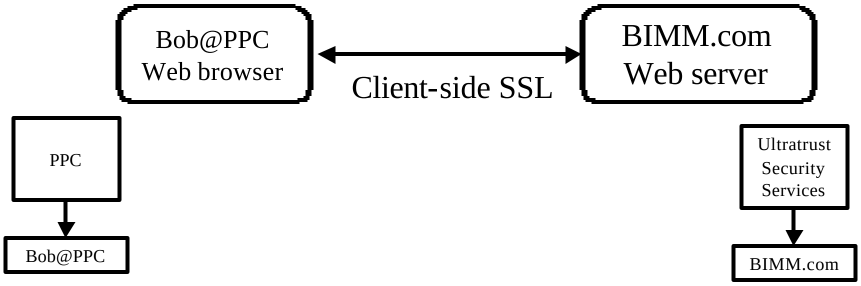
ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



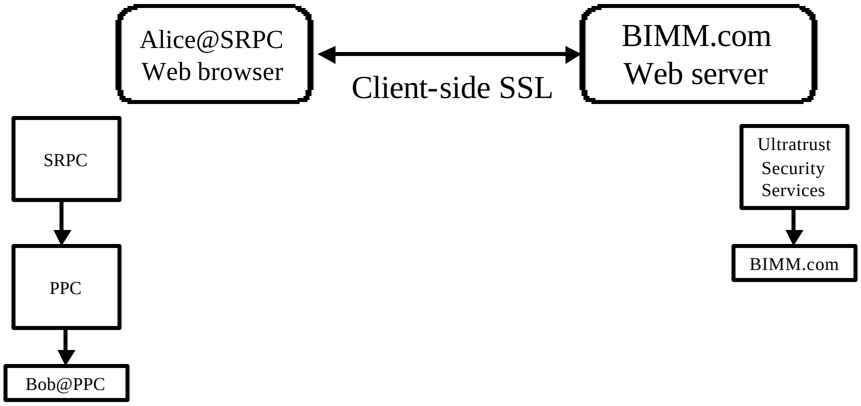
ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



ATTRIBUTE-BASED CLIENT SIDE MASQUARADING


Alice@SRPC
Web browser

BIMM.com
Web server

Client-side SSL

SRPC

PPC

Bob@PPC

Ultratrust
Security
Services

BIMM.com

PKI AND TRUST

- **Got to be very careful**
- **Not a game for amateurs**
- **Not many professionals as yet**