INFS 767
Secure Electronic Commerce

Lecture 7
PKI and Trust

Prof. Ravi Sandhu

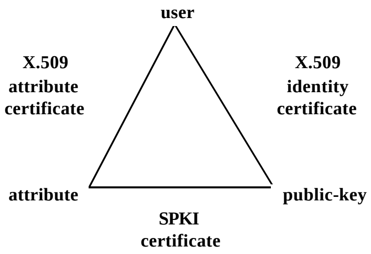
PUBLIC-KEY INFRASTRUCTURE PKI

- **“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



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

Handshake Protocol

```
Client                                          Server

ClientHello                 ------->
                                           ServerHello
                                           Certificate

                            <--------  ServerHelloDone

ClientKeyExchange

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

Record Protocol

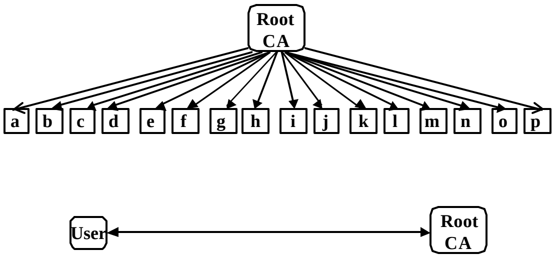
CLIENT-SIDE SSL (OR 2-WAY) HANDSHAKE WITH RSA

Handshake Protocol

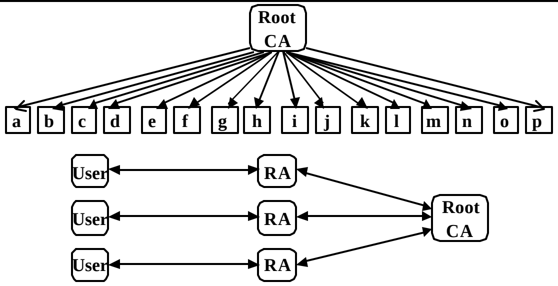
```
Client                                          Server

ClientHello                 ------->
                                           ServerHello
                                           Certificate

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

Record Protocol

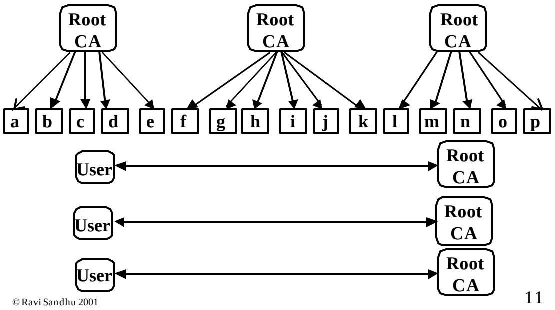
SINGLE ROOT CA MODEL



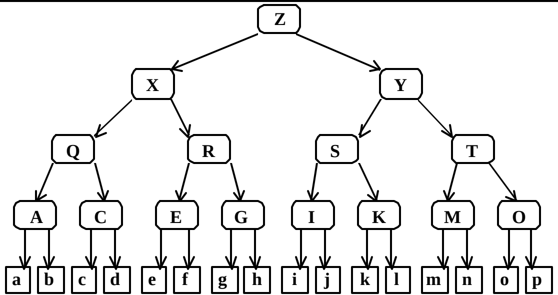
SINGLE ROOT CA MULTIPLE RA's MODEL



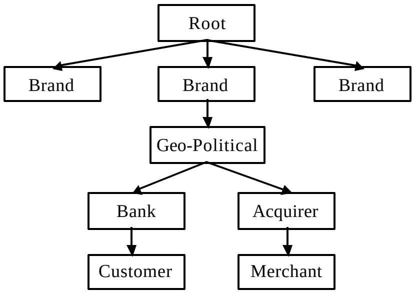
MULTIPLE ROOT CA's MODEL



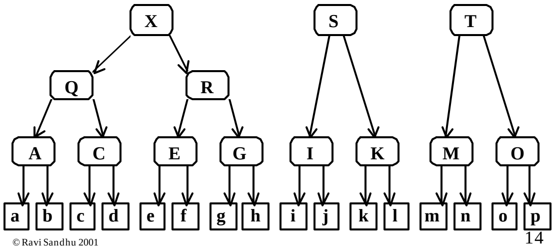
ROOT CA PLUS INTERMEDIATE CA's MODEL



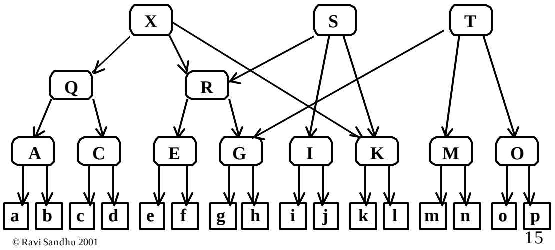
SECURE ELECTRONIC TRANSACTIONS (SET) CA HIERARCHY



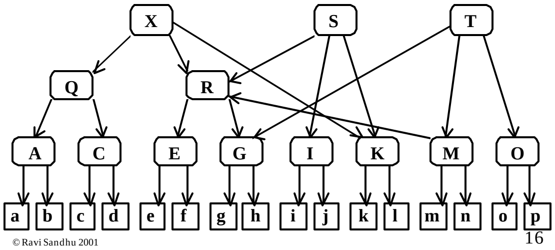
MULTIPLE ROOT CA's PLUS INTERMEDIATE CA's MODEL



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

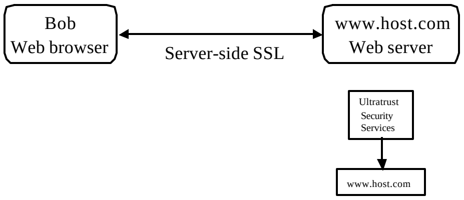
SERVER-SIDE SSL (OR 1-WAY) HANDSHAKE WITH RSA

Handshake Protocol

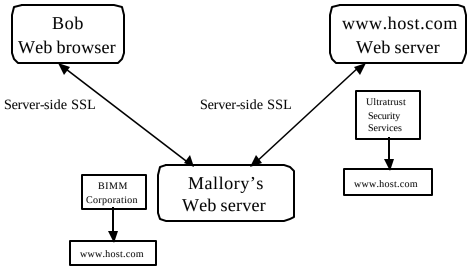
```
Client                                                Server

ClientHello              -------->
                                                 ServerHello
                                                 Certificate
                         <--------           ServerHelloDone
ClientKeyExchange
[ChangeCipherSpec]
Finished                 -------->
                                          [ChangeCipherSpec]
                         <--------                  Finished
Application Data         <------->          Application Data
```

Record Protocol

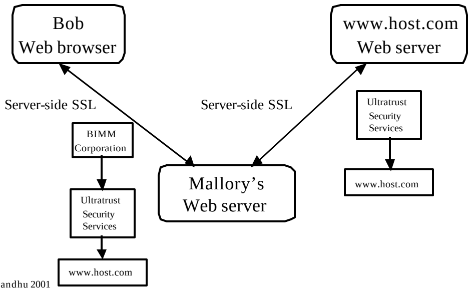
SERVER-SIDE MASQUARADING



SERVER-SIDE MASQUARADING



SERVER-SIDE MASQUARADING



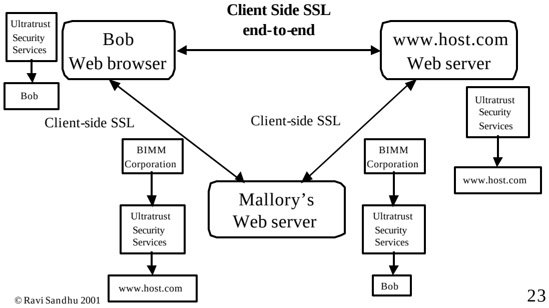
CLIENT-SIDE SSL (OR 2-WAY) HANDSHAKE WITH RSA

Handshake Protocol

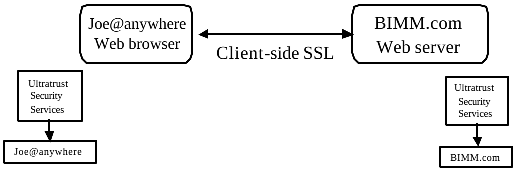
```
Client                                             Server

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

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

Record Protocol

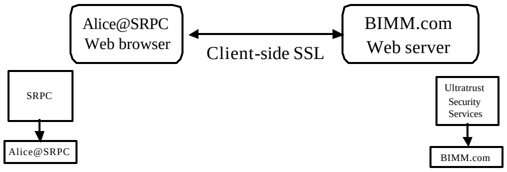
MAN IN THE MIDDLE MASQUARADING PREVENTED



ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



Alice@SRPC Web browser

Client-side SSL

BIMM.com Web server

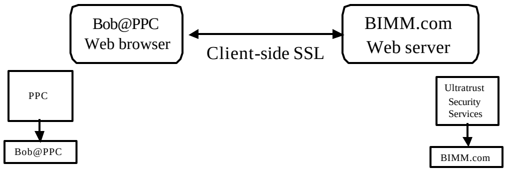
SRPC

Alice@SRPC

Ultratrust Security Services

BIMM.com

ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



Bob@PPC Web browser

Client-side SSL

BIMM.com Web server

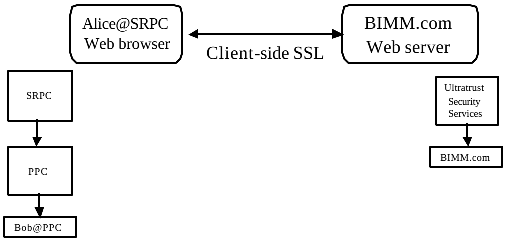
PPC

Bob@PPC

Ultratrust Security Services

BIMM.com

ATTRIBUTE-BASED CLIENT SIDE MASQUARADING



Alice@SRPC Web browser

Client-side SSL

BIMM.com Web server

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**