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

attribute

SPKI certificate

X.509 identity certificate

public-key
X.509 CERTIFICATE

<table>
<thead>
<tr>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERIAL NUMBER</td>
</tr>
<tr>
<td>SIGNATURE ALGORITHM</td>
</tr>
<tr>
<td>ISSUER</td>
</tr>
<tr>
<td>VALIDITY</td>
</tr>
<tr>
<td>SUBJECT</td>
</tr>
<tr>
<td>SUBJECT PUBLIC KEY INFO</td>
</tr>
<tr>
<td>SIGNATURE</td>
</tr>
</tbody>
</table>

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, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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

Client Hello ----> Server Hello
Certificate

Handshake Protocol

ClientKeyExchange

[ChangeCipherSpec]
Finished

<-------- ServerHelloDone

Application Data <-> Application Data

Record Protocol

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

Client Hello ----> Server Hello
Certificate
CertificateRequest

Handshake Protocol

ClientKeyExchange
CertificateVerify

[ChangeCipherSpec]
Finished

<-------- ServerHelloDone

Application Data <-> Application Data

Record Protocol

© Ravi Sandhu 2001
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

- 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

ClientHello

Certificate

ClientKeyExchange

[ChangeCipherSpec]

Finished

Application Data

Record Protocol

Server

ServerHello

Certificate

ServerHelloDone

[ChangeCipherSpec]

Finished

Application Data
SERVER-SIDE MASQUARADING

Bob
Web browser

www.host.com
Web server

Server-side SSL

Mallory’s
Web server

Server-side SSL

Ultrasound
Security
Services

BIMM Corporation

www.host.com

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

Client

Server

ClientHello

ServerHello

Certificate

CertificateRequest

ServerHelloDone

Certificate

Certificate

Certificate

Certificate

[ChangeCipherSpec]

[ChangeCipherSpec]

Finished

[ChangeCipherSpec]

Finished

Application Data

Application Data

Record Protocol

Handshake Protocol

Certificate

ClientKeyExchange

CertificateVerify

[ChangeCipherSpec]

Finished

[ChangeCipherSpec]

Finished

Application Data

Application Data

Record Protocol

© Ravi Sandhu 2001
MAN IN THE MIDDLE
MASQUARADING PREVENTED

ATTRIBUTE-BASED CLIENT SIDE MASQUARADING
ATTRIBUTE-BASED CLIENT SIDE MASQUARADING

Alice@SRPC
Web browser

Client-side SSL

SRPC

Alice@SRPC

BIMM.com
Web server

Ultratrust
Security Services

BIMM.com

Bob@PPC
Web browser

Client-side SSL

PPC

Bob@PPC

BIMM.com
Web server

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