Lecture 10:

Design of Global Security System for ODP Environments

Subjects / Topics:
1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control / authorization
Lecture 10:

Design of Global Security System for ODP Environments

Subjects / Topics:

1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control/authorization

ODP – overall situation
Communication / socket level security

User → Client → Network → Server

Protected  →  Unprotected

Applications/document level security

User → Client → Network → Server

Protected  →  Unprotected
Smart cards: End-to-end security

Local login

User

Client

Network

Server

Remote Server

User ID:

Password:

Sec DB

Login
Remote login / authentication

Authorization in ODP systems

Identity

Attrib cert

John Smith
3423342
Certification in distributed systems

Lecture 10:

Design of Global Security
System for ODP Environments

Subjects / Topics:

1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control / authorization
Security modules – Login

User

UserID : Password :

Sec DB

Login

Server

Security modules – Sec Administration

User

UserID : Password :

Sec DB

Login

Sec Admin

Server
Security modules – Crypto/Smart cards

User

UserID : Password :

Login
Sec Admin

Crypto/SC

Security modules – X.500 Registration

User

Country : Organization : Org Unit : Common Name :

X.500
Dir

Login
Sec Admin

Crypto/SC

X.500
Regist
Security modules – Certification protocols

Security modules – Certification trust
Security modules – Communication security

Security modules – SSL
Security modules – Documents security

User interface
Login – Authentication Authority
Security Administration

Security Platform
Crypto/SC modules
Certification modules

Communication modules
Encapsulation
SSL security

Sec Infrastructure
X.500 (LDAP)
Certification protocol

Page 11
Lecture 10:

Design of Global Security System for ODP Environments

Subjects / Topics:
1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control / authorization

Smart cards – multiple applications

- Designing
- Formatting
- Loading (Initialization)
- Protection
Situation with smart card technologies

Applications using smart cards

Multiple APIs

Multiple drivers

Multiple readers

Multiple smart cards

Smart cards – PC/SC

ICC-Aware Application

PC/SC Service Provider Reference Interfaces

PC/SC RM Interface

Resource Manager

PC/SC IFD Handler Interface

Drivers

Smart Card Readers

Smart Cards
Smart cards – PIV

Remote login / authentication

SASL Token

User

Remote Server

Login
Lecture 10:

Design of Global Security
System for ODP Environments

Subjects / Topics:

1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control / authorization
Multi-party transactions

1. Simple client/server model
2. Mainly communication services
3. Static allocation of code

1. Multiple senders
2. Multiple recipients
3. “Chained” transactions

PKCS#7 – Signed data

SignedData

<table>
<thead>
<tr>
<th>Version</th>
<th>Digest Algorithm</th>
<th>ContentInfo</th>
<th>Certificate</th>
<th>CRLs</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>sha1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ContextType</th>
<th>Content</th>
</tr>
</thead>
</table>

Certificates needed to verify the signature

DataToBeSigned (DER Encoded)

SignedInfo

<table>
<thead>
<tr>
<th>Version</th>
<th>SourceName</th>
<th>DigestAlgorithm</th>
<th>AuthenticDataAttributes</th>
<th>SignatureAlgorithm</th>
<th>EncryptedDigest</th>
<th>AuthenticationAttributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
<td>sha1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| sourceName | Certificate
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(From signer's Certificate)</td>
<td></td>
</tr>
</tbody>
</table>
Lecture 10:

Design of Global Security System for ODP Environments

Subjects / Topics:
1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control / authorization
Authorization in ODP Systems

- PKI is for authentication
- Authorizations can be seen as attributes
- Problematic to include attributes in a PKC
- The solution is a separate attribute certificate
- Attribute Authority

Attribute certificates

- Holder (Alice)
- Issuer (Bob)
- Validity period (1999-2001)
- Attributes (bank manager)
- Signature (by the Issuer)
Delegated authorization

![Diagram showing Delegated authorization process]

Lecture 10:
Design of Global Security
System for ODP Environments

Subjects / Topics:
1. Components of a global security system
2. Modules at user workstations
3. Authentication protocol
4. Transactions/documents security
5. Access control / authorization
Questions