Prof. Sead Muftic

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
Cloud Environment

CAP – Communication Access Point
AAP – Applications Access Point

Communication / Socket-Level Security

Unprotected
Protected
Unprotected
Applications / Documents-Level Security

Smart Cards: End-to-end Security
**Local Login – PIV Card**

**Remote Login**

- Cloud → Central Security Server
  - CA Server
  - Smart Card Server
  - PACS Server
- Internet

- User → Cloud Station
  - User
  - Cloud Station
Authorization in ODP Systems

Identity

Attributes cert

Documents

Payments

Sensitive info

Certification in Distributed Systems

Bridge CA

Top CA

Policy CA

User CA

User

Server

Top CA

Policy CA

User CA

User

Server
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

Login

Sec DB

Server

Server

Server
Security Modules – X.500 Registration

Country: Organization: Org Unit: Common Name:

User → Login → Sec Admin → Crypto/SC → Sec DB

X.500 Dir → Server

Security Modules – Certification Protocols

CA Server

User → Login → Sec Admin → Crypto/SC → Sec DB

X.500 Dir → Server
Security Modules – Certification Trust

User

Sec DB

Cert DB

X.500

Dir

Login

Sec Admin

Crypto/SC

Cert modules

CA

Server

Security Modules – Communication Security

User

Sec DB

Cert DB

X.500

Dir

Login

Sec Admin

Crypto/SC

Cert modules

CA

Server
Security Modules – Conclusions

User Interface
- Login – Authentication
- Authorization
- Security Administration

Sec Infrastructure
- X.500 (LDAP)
- Certification protocol

Communication
- Encapsulation
- SSL security

Security Platform
- Crypto/SC modules
- Certification modules

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

- Reserved (Directory)
- Appl - 1
- Appl - 2
- Appl - 3

User Area (Files, Keys, Data)

- Designing
- Formatting
- Loading (Initialization)
- Protection

Diversity of Smart Card Technologies

- Multiple APIs
- Multiple drivers
- Multiple readers
- Multiple smart cards

Applications using smart cards
Remote Login / Authentication

SASL Token

John Smith
3423342

User
Login

Remote Server

Remote Login / Authentication

Single Sign On (SSO) – Embedded SASL Tokens

From user
Internet
Firewall
Server 1
Server 2
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

1. Multiple senders
2. Multiple recipients
3. “Chained” transactions
PKCS#7 – Signed Data

PKCS#7 – Enveloped Data
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 the flow from user to Appl Server via Internet and Firewall]

From user

Internet

Firewall

Auth Server

Appl Server
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