Lecture 11:

CryptoNET:
Security Management and
Protocols

Subjects / Topics:
1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNET
   2. Authentication
      - Local Authentication
      - Remote Authentication (Strong Authentication)
      - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

Background & Motivation

- Traditional software development
  - Focus on functional requirements

- Consideration of security features
  - Add-on
  - Security patches
  - Added as non-functional features
  - May introduce other bugs or vulnerabilities

- Increase Complexity:
  - Crypto Service Provider
  - Development complexity
  - Configuration complexity

- Data protection standard
  - Different applications different standards
  - Compatibility

If IT resources are strongly protected than we can protect our environment from mobile code, malicious software, intruders, insiders’ attacks and incorrect operations.
Objective

Design, implement, test, and deliver high assurance information infrastructure for cryptographically protection of IT resources and operations in some data processing environment

Modules

- Security Provider
- Integrated Secure Workstation
- Software Protection
- Secure Network Communication Protocols
- Generic Secure Servers
Security standards and protocols:

- **Authentication**: FIPS 196, SAML Single Sign On
- **Authorization & Access Control**: SAML-AuthenticationRequest & Response Protocol, XACML policies
- **Secure Communication**: SSL/TLS, Secure Session
- **Credentials**: X.509 Certificate, SAML Ticket
- **Smart card**: FIPS-201 (PIV)
- **Encapsulation**: PKCS7SignedAndEnvelopedData, S/MIME
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects/Tops:

1. CryptoNet
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

CryptoNET: Local Authentication

- User name/password based authentication
- PIN / PIN plus fingerprint based authentication (FIPS-201)
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

The identities of networked users, clients and servers are verified without transmitting passwords over the network.
CryptoNET: Strong Authentication

- Entity Authentication using Public Key Cryptography
- Unilateral Authentication
  Single challenge-response protocol
- Mutual Authentication
  Two challenge-response protocols
- Random number is a time variant parameter

Strong Authentication: Unilateral Authentication protocols

Client

SA Server

[Auth Request]

Token ID|Token BA

Token ID|CertA|Token AB
Strong Authentication: Mutual Authentication protocols

Client → SA Server
[Auth Request]
Token ID|Token BA

Token ID|CertA|Token AB
Token ID|CertB|Token BA

Strong Authentication: Improvements

Client → SA Server
[Cert A]
Verify Cert A
Verify Identity

Token ID|Token BA
Token ID|Token AB
Token ID|CertB|Token BA

LCA
IDMS
Strong Authentication: Improvements

Client

[Cert A]

Token ID|Token BA

Token ID|Token AB

Token ID|Cert B|Token BA

Verify Cert A

LCA

Verify Identity

Verify Cert B

Verify Identity

IDMS

Strong Authentication: Message Format

MessageAB1 = CSM(MCL/SMA RCV/alice ORG/bob TVB/e69d6b21ff051a3)

MessageABAT = CSM(MCL/SMA RCV/alice ORG/bob TVB/e69d6b21ff051a3)

MessageAB = CSM(MCL/SMA RCV/bob ORG/alice TVB/e69d6b21ff051a3 TVA/e7287bc4352b9436 SGA/b7f87f7d1de3e5dadd1af3f334e34390c3619389696d02fe28a7736015e081a39f86d33b44c)

MessageAB2 = CSM(MCL/SMB RCV/alice ORG/bob TVB/e69d6b21ff051a3 TVA/d647bc433299436 GSB/c26alce2a253d5c349962d1a78a225d27e2aa15b934b2604e6facca2c2334af5bbede60a5b282f8 CRB/ )
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

CryptoNET: Single Sign On

A single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords.
Single Sign On

Client

Policy Enforcement Point

SAML Identity Assertion

Authentication Result

Secure Session

SAML Authentication Request

SAML Authentication Response

SAML Policy Server

SAML Policy Point
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System
CryptoNET: Secure Session

- Secure Communication between Client and Application Server
  - Key exchange certificate
  - Session ID
  - Session Key

Secure Session

SAML based SSO

Key Exchange Certificate

Session ID | Session Key
Lecture 11:

CryptoNET: Security Management and Protocols
Subjects / Topics:

1. CryptoNet
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

Example: CryptoNET: Secure Email System

Features
- Strong Authentication
- Single Sign On
- Secure Session
- Encrypted Address Book
- Address Book Key Management
- Signed and Enveloped Email
- Efficient Handling of Attachments
- Email Confirmations
- Elimination of Spam
Current E-mail System

The Concept of The Extended Secure E-mail System
Lecture 11:

CryptoNET: Security Management and Protocols

Subjects / Topics:

1. CryptoNET
2. Authentication
   - Local Authentication
   - Remote Authentication (Strong Authentication)
   - Single Sign On
3. Secure Session Protocol
4. Example: Secure E-mail System

Extended Security Features

- User and Server Registration
- Certificate Distribution
- Single Sign-on
- Authorization policies and Access Control
- Authorization to activate applications
- Protection of messages (confidentiality and integrity)
- Traffic protection (replay, lost messages, etc)
- Authenticity of a sender for each transaction (digital signatures)
- Authenticity of a recipient for each transaction (enveloping)
- Application Specific Security Requirements:
  - Secure multi-party transactions and protocols
  - Secure group transactions
  - Protection of user data
References

- "Entity Authentication Using Public Key Cryptography", National Institute of Standards and Technology, 1997 February 18

Questions