CERIAS

the center for education and research in information assurance and security

Preserving Privacy in Policy-Based Content Dissemination

Mohamed Nabeel, Ning Shang, Elisa Bertino (Purdue University)

What is policy based content dissemination?

A simplified Health Record (HR)

Contact Info

Clinical Record

A doctor can access Clinical Record

Lab Reports

Medical History

A receptionist can access Contact Info

A data analyst can access Lab Reports

Attribute Based Access Control (ABAC)

A simplistic approach using encryption

Only one encryption per node!

A simplified Health Record (HR)

Contact Info

Clinical Record

Lab Reports

Medical History

Issue #1: Privacy of the users is not preserved

"I am a doctor"

"Here are the keys to decrypt Medical Records"

Publisher   Subscriber

1. Need to reveal credentials
2. Need a private communication channel for re-keying

Issue #2: The key management does not scale

Re-keying has $O(n)$ communication overhead (n = number of users)

Requirements for maximal amount of privacy & security

Access Control

Only subscribers satisfying AC policies are allowed to access

Hidden Credentials

Publisher does not learn the attributes of subscribers

Hidden Content Consumption

Publisher does not learn which content subscribers can access

Building blocks: OCBE and BGKM schemes

OCBE: Oblivious Commitment Based Envelope

An encrypted message

Unconditionally hiding and computationally binding $com(m) = g^m h^r$

Commitment ("I am a doctor")

Envelope ("Here are the secrets to decrypt Medical Records")

Publisher   Subscriber

- Publisher does not learn credentials
- User can open the envelope only if her credential satisfies the condition

BGKM: Broadcast Group Key Management

Public Info

$+$

S_1

S_2

S_3

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & & a_{1,m} \\ a_{2,1} & a_{2,2} & & a_{2,m} \\ & & & \\ a_{n,1} & a_{n,2} & & a_{n,m} \end{bmatrix}$$

$\begin{bmatrix} c_{1,1} & c_{1,2} \end{bmatrix} \quad \begin{bmatrix} c_{1,m} \end{bmatrix}$

A random vector from the null space of A

$\begin{bmatrix} K & 0 \end{bmatrix} \quad \begin{bmatrix} 0 \end{bmatrix}$

$\begin{bmatrix} c'_{1,1} & c_{1,2} \end{bmatrix} \quad \begin{bmatrix} c_{1,m} \end{bmatrix}$

ACV – Access Control Vector

Each row is constructed with secret(s) given to each Sub

Public Info

$\begin{bmatrix} a_{r,1} & a_{r,2} \end{bmatrix} \quad \begin{bmatrix} a_{r,m} \end{bmatrix}$

KEV – Key Extraction Vector

$\begin{bmatrix} c'_{1,1} & c_{1,2} \end{bmatrix} \quad \begin{bmatrix} c_{1,m} \end{bmatrix} \cdot \begin{bmatrix} a_{r,1} & a_{r,2} \end{bmatrix} \quad \begin{bmatrix} a_{r,m} \end{bmatrix} = \begin{bmatrix} K \end{bmatrix}$

Putting everything together (OCBE + BGKM)

IdP

IdMgr

Sub

Sub

Pub

Identity Token Issuance

Identity Token Registration

Document Dissemination

Identity Token Issuance

IdP

$\{attr_i, val_i\}$

Sub

$\{attr_i, val_i\}$

$\{Token_i\}$

IdMgr

Identity Token
Pseudonym
Attribute
Commitment
Signature

Certified Identity Attribute
Example: "I am a doctor"

Identity Token Registration

Example: age > 21

$Cond(attr_i, val_i, op)$

Pub

$\{Token_i\}$

OCBE

Sub1

css_i

Conditional Subscription Secret

Document Dissemination

Document

ACV_1

Subdocument$_1$

ACV_2

Subdocument$_2$

ACV_3

Subdocument$_3$

Publish

Consume

Document

Subdocument$_1$ K_1

Subdocument$_2$ K_2

Subdocument$_3$ K_3

ACV_2 KEV_2 K_2

Subdocument2   K2   Subdocument2

Some selected experimental results

Average computation time for running one round of GE-OCBE protocol

Time to generate an ACV for different user configurations

Key derivation time for different user configurations

ACV generation and key derivation for different number of conditions per policy

PURDUE UNIVERSITY

CERIAS

Discovery Park
e-Enterprise Center