Privacy Preserving Enforcement of Sensitive Policies in Outsourced Environments

Muhammad Rizwan Asghar

Researcher
CREATE-NET
Italy

EPFL, Switzerland
February 13, 2014
Why Outsourcing

- Cost saving
- Scalability
- Efficiency
- Availability
Problem

Policy: Only a dentist may get access from dentist-ward during duty hours (9-17 hrs)

Cloud Service Provider
Amazon S3

Access Request
Requester=Doctor, Location=Doctor-ward, Time=10hrs

Access Request

Policy

Medical Record

Patient

Dentist

Issue: Policy or access request may leak sensitive information
Problem (2)

Cloud Service Provider
Amazon S3

Problem: How to evaluate encrypted policy against encrypted access request
Threat Model

- Cloud Service Providers are **honest-but-curious**
- Requesters (e.g., dentist) are **authorised**
- Admin Users (e.g., patient) are **trusted**
- We assume the following kinds of **collusions**
  - Requester-Requester collusion
  - Requester-Admin User collusion
  - Admin User-Admin User collusion
- Trusted key management authority
  - distributes key material out of the band
  - can stay **offline**
- **Passive** adversaries
ESPOON

- **ESPOON**: Enforcing Security Policies in Outsourced Environments

- **ESPOON protects** queries and policies stored in outsourced environments

- It is capable of **handling complex** policies involving range queries

- It is a **multiuser** scheme in which entities do not share any encryption keys

- A compromised user can be **removed** without requiring re-encryption of policies
ESPOON – Architecture

Policy Store

Admin User

(ii) \(C\{Policy\}\)

{Policy}\_{K,\alpha}\n
K_{\alpha,\alpha} = (A, x_{A2}) \quad K_{\alpha,\beta} = (R, x_{R2})

Key Store

trusted Key Management Authority

Fully-trusted

\(MSK = (x, s)\)

\(Params = (g, h = g^x, H, f)\)

\(x = x_{i1} + x_{i2}\)

Data Store

Admin Point

Outsourced Environment

Cloud Service Provider

Honest-but-curious

PDP

(4) Yes/No

TD\{REQ\}

PEP

(2)

(6) Response

(5) Data

(1)

\{REQ\}_{K,\beta}

Requester

Authorised

Requester

{Policy}\{Policy\}

(3)

C\{Policy\}

Policy

Admin User

Trusted

{(i) \{Policy\}\_{K,\alpha}}
Access Request:
Requester=Dentist
Location=Dentist-Ward
Access Time=10hrs

TD(Requester=Dentist)
TD(Location=Dentist-Ward)

Policy:
Only a dentist may get access from dentist-ward during duty hours (9-17 hrs)

- Yes
- No

Policy Evaluation

AT = Access Time
ESPOON – Overhead

- We developed a prototype using Java

- **Request** generation incurs ~0.15 s
  - 1 numerical attribute (of 5-bit) and
  - 2 string attributes

- **Policy evaluation** takes < 0.1 s
  - A numerical range and
  - 2 string comparisons

- We ran our prototype on a standard **machine**
  - Operating system: *Windows XP*
  - Processor: *Intel Core2 Duo 2.2 GHz*
  - RAM: 2 GB
Performance Analysis: Policy Deployment

- **String Comparison**: For both enc and re-enc: \(O(n)\), \(n\) is the number of string comparisons

- **Numerical Comparison**: For both enc and re-enc \(O(ns)\), \(n\) is the number of numerical comparisons each of size \(s\)
Performance Analysis: Request

- **String Attribute:** $O(n)$, $n$ is the number of string attributes

- **Numerical Attribute:** $O(ns)$, $n$ is the number of numerical attributes each of size $s$
Performance Analysis: Policy Evaluation

- **String Attribute:** $O(nm)$, $n$ is the number of string attributes and $m$ is the number of string comparisons

- **Numerical Attribute:** $O(nms^2)$, $n$ is the number of numerical attributes and $m$ is the number of numerical comparisons each of size $s$
Related Work

- Schemes supporting access control in outsourced environments require re-generation of keys and **re-encryption** of data for any administrative changes [De Capitani Di Vimercati et al. CSAW’07 VLDB’07]

- Schemes supporting queries on encrypted data do **not** support access policies [Dong et al. DBSec’08, Song et al. S&P’00, Boneh et al. EUROCRYPT’04, Curtmola et al. CCS’06, Hwang and Lee LNCS’07, Boneh and Waters TCC’07, Wang et al. SOFSEM’08, Baek et al. ICCSA’08, Rhee et al. JSS’10, Shao et al. Inf. Sci.’10]

- Data encrypted with CP-ABE **reveals policies** [Narayan et al. CCSW’10]

- Hidden credentials schemes do not support complex policies and require parties to be **online** [Holt et al. WPES’03, Bradshaw et al. CCS’04]

- Homomorphic encryption incurs high computational cost
Summary

- We proposed ESPOON that enforces sensitive policies in outsourced environments

- ESPOON supports complex policies including range queries

- ESPOON employs a multiuser scheme where entities do not share keys
Extending ESPOON with RBAC

- We support Encrypted Role-Based Access Control (ERBAC)
- We propose ESPOON_{ERBAC} that offers
  - **RBAC0** – Role assignment and permission assignment
    [Asghar et al. COSE’13, Asghar et al. CCS’11]
  - **RBAC1** – Dynamic constraints (E-GRANT) [Asghar et al. IJIS’13]
    - Dynamic separation of duties
    - Chinese Wall
  - **RBAC2** = RBAC0 + RBAC1 [Asghar Ph.D. Thesis’13]
asghar@create-net.org
http://disi.unitn.it/~asghar/