Secure Attribute-Based Messaging with ABE

Rakesh Bobba

With Omid Fatemieh, Fariba Kahn, Arindam Khan, Carl A. Gunter, Himanshu Khurana, and Manoj Prabhakaran

Secure Attribute-Based Messaging with ABE

• Aim:
  • Demonstrate the usefulness and feasibility of attribute-based encryption
  • Illustrate practical challenges faced by ABE - securing a novel messaging paradigm, Attribute-Based Messaging (ABM)
ABM Concept

- ABM – sends messages, e.g., email, to parties described in terms of a collection of attributes.
- Similar to a listserv, but recipients are determined dynamically using one or more enterprise databases
- An ABM address is a database query.
- Ex: female grad students in engineering who have passed their qualifying exams

Advantages

**Efficiency:** people who do not need an email do not receive it
- Ex: all of the faculty on sabbatical

**Exclusivity:** sensitive messages can target more limited groups
- Ex: all tenured faculty serving on conflict of interest committees

**Intensionality:** often easier to describe recipients than list them
- Ex: Smith’s attending and ordering physicians
Applications

• Enterprise Communication
• Alerts and Emergency Communication
  • Disease outbreak monitoring and alerts – CDC
• Health care
  • Messaging oriented - exploring improving convenience and security with ABM
ABM Addresses

- Addresses are disjunctive normal forms
- Ex: ((Position = Faculty) and (Salary > 150000)) or (Position = Graduate Director)
- Defines receiving policy

Challenges

**Access Control**: on what attributes should a party be allowed to route?
- Ex: All faculty who make more than $150,000/year

**Confidentiality**: if the senders do not know their specific recipients, how can they encrypt end-to-end?

**Privacy**: what are senders and recipients allowed to know
Implementation, Use, and Management Challenges

• Interoperation with existing systems
  • Webmail easiest
  • Aim to work with existing Mail User Agents (MUAs) or Mail Transfer Agents (MTAs)
  • Application integration may be necessary
• Efficiency of
  • Access control decisions
  • Encryption
• Manageability
  • Policies must be easy to manage and use

Approach – Attribute-Based Security

• Attribute-Based Access Control (ABAC)
  • “Policy specialization” provides attributes that can be used for routing
• Attribute-Based Encryption (ABE)
  • New public key system provides end-to-end confidentiality
ABAC

- Grants access based on user attributes
- Many established ideas for how to use attributes in AC
  - X.509 attribute certificates
  - Much implicit use in application servers
- New approaches
  - Attributes in dynamic tokens as in Shibboleth
  - Trust negotiation
  - ABE, Secret Handshakes

ABAC for ABM

- Attribute-Based Access Control (ABAC)
  - Uses same attributes used to target messages
  - More flexible rules than with RBAC
- Access policy
  - Sending rules are disjunctive normal forms specified using XACML
  - The sending rules collectively define the sending policy

- Ex: (Position = Faculty) AND (Designation = Director) => (Position = Faculty)
- Sun’s XACML engine is used for policy decision
ABAC for ABM

- Issues
  - Need a sending rule per ABM address
  - Usability – loss of messaging semantics

- Solution
  - One rule per <attribute,value>
    - Any address can be formed with allowed attributes
  - Policy specialization
    - Specifies per user sending policy
    - List of attributes a user is allowed to route on

Strawman Architecture
ABE

• Emerging pairing-based cryptosystems that allow encryption and decryption using attributes (rules)
• Ciphertext Policy ABE (CP-ABE) [BSW07]
  • A pairing-based cryptosystem that allows encrypting data with attribute rules
  • Only users who possess keys for attributes that satisfy the attribute rule can decrypt the data
  • Supports string and numerical attributes and monotonic attribute rules
• Protects against collusion

ABE for ABM

• Encrypt using “attribute rules” and public parameters
  • Use the same attributes used to target messages
• Attribute rules are disjunctive normal forms and define reading policy
• \{Reading policy\} = \{Receiving policy\} – correctness
  • Translate receiving policy into a reading policy
• Ex: (“Position_val_Faculty”) AND (Salary > 150000)
• An Attribute Authority (AA) issues attribute keys to each user based on the enterprise database
  • E.g., “Faculty” attribute has a key
ABE for ABM

• Issues
  • No Revocation
  • Key Management

• Solution
  • Short-lived keys
  • One expiry attribute per user [BSW07]. Key Validity period is maximum tolerable vulnerability window
Protocol Steps

The protocols for the ABM system are given in terms of three “paths”
- Policy specialization path
- Messaging and address resolution path
- Attribute keying path

Policy Specialization Path

Policy Specialization (PS) Path:
1. Authenticate User
2. User Info. (ID)
3. User Info. (ID)
4. User Attributes
5. User ID and Attributes
6. Routable Attributes
7. Routable Attributes
8. ABM Address
**Messaging and Address Resolution Path**

**Messaging (MS) Path:**
1. Send (ABM) message (SMTP)
2. Notify ABM Host
3. Receive (ABM) messages (SMTP)
4. Send resolved messages

**Address Resolution (AR) Path:**
1. User ID and Authorization
2. Policy Decision
3. ABM Address
4. Resolved list of Addresses

**Attribute Keying Path**

**Attribute Keying (AK) Path:**
1. User Info. (ID)
2. User Info. (ID)
3. User Attributes
4. User Secret Key
5. Decrypted Email
Security and Privacy Analysis

• Enforcement of sending, read, and receiving policies
  • S/MIME to authenticate sender to ABM server
  • Vulnerability windows: receive subset of read
• Component compromise and collusion
  • MTA or ABM server
  • Clients
• Privacy
  • What should senders and receivers know?

Efficiency Analysis

• Measure costs on each path and try to estimate latencies for mid-size enterprises
• Must conjecture the attributes and types of policies that will be used
• Implementation uses the CP-ABE library [BSW07].
**Encryption Time**

Equality – e.g., (Position = Faculty), Relational – e.g., (Salary > 150000)

<table>
<thead>
<tr>
<th>Number of Equality Literals</th>
<th>Number of Relational Literals</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1.53s</td>
<td>3.00s</td>
<td>4.49s</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>0.05s</td>
<td>1.55s</td>
<td>3.05s</td>
<td>4.56s</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>0.07s</td>
<td>1.57s</td>
<td>3.08s</td>
<td>4.56s</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>0.09s</td>
<td>1.59s</td>
<td>3.09s</td>
<td>4.60s</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>0.12s</td>
<td>1.61s</td>
<td>3.12s</td>
<td>4.61s</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>0.14s</td>
<td>1.65s</td>
<td>3.16s</td>
<td>4.64s</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>0.17s</td>
<td>1.66s</td>
<td>3.17s</td>
<td>4.63s</td>
</tr>
</tbody>
</table>

Decryption times averaged 352ms.

**Key Generation Time**

Boolean – e.g., (Position_VAL_Faculty), Numerical – e.g., (Salary = 150000)

<table>
<thead>
<tr>
<th>Number of Numerical Attributes</th>
<th>Number of Boolean Attributes</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0.05s</td>
<td>0.07s</td>
<td>0.10s</td>
<td>0.12s</td>
<td>0.20</td>
<td>0.17s</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>0.86s</td>
<td>0.87s</td>
<td>0.88s</td>
<td>0.90s</td>
<td>0.93s</td>
<td>0.95s</td>
<td>0.97s</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>1.67s</td>
<td>1.68s</td>
<td>1.69s</td>
<td>1.70s</td>
<td>1.73s</td>
<td>1.76s</td>
<td>1.78s</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>2.44s</td>
<td>2.48s</td>
<td>2.49s</td>
<td>2.52s</td>
<td>2.54s</td>
<td>2.57s</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>3.26s</td>
<td>3.28s</td>
<td>3.29s</td>
<td>3.32s</td>
<td>3.34s</td>
<td>3.35s</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>4.05s</td>
<td>4.07s</td>
<td>4.09s</td>
<td>4.12s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>4.87s</td>
<td>4.89s</td>
<td>4.92s</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AA Scalability

![Bar chart showing AA Scalability](image)

Other Results Summary

- Policy Specialization
  - Latency proportional to number of rules
    - $< 1$ second for 150 rules
    - $< 12$ seconds for 700 rules
- Address Resolution
  - With access control and without confidentiality
    - $< 400$ms for a 60K RDB
    - $< 8$ seconds for 60K XML DB
Conclusions

• Messaging (email) based on attributes collected from an enterprise database is feasible and deployable for mid-size enterprises.
• Access control and confidentiality are manageable using attribute-based security mechanisms.
• Improved ABE schemes with better revocation properties are needed.
• Privacy management of attributes needs to be better understood before deploying ABM and ABE.