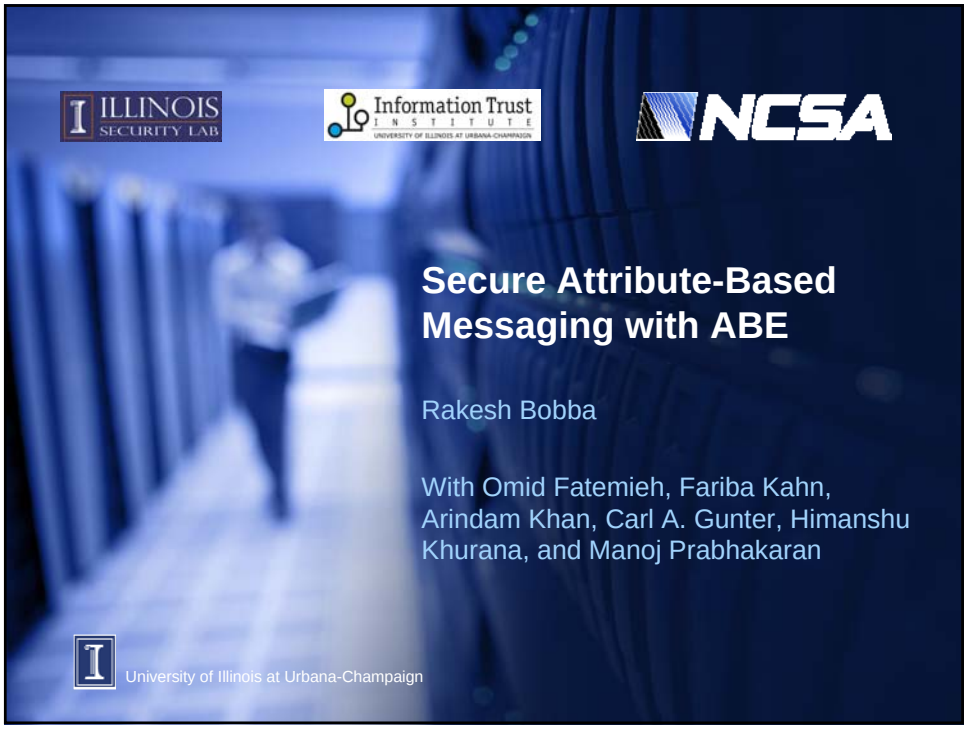


Secure Attribute-Based Messaging with ABE

- 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)

Funded by:

NCSA

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

NCSA

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

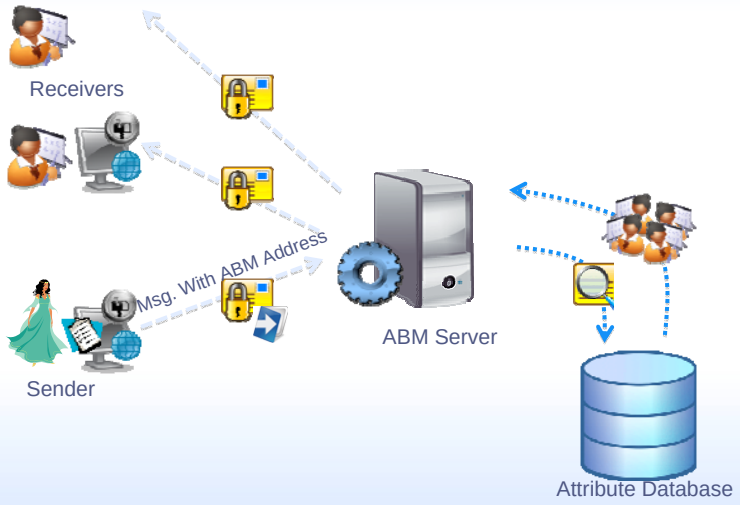
NCSA

Applications

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

NCSA

Strawman Architecture



NCSA

ABM Addresses

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

NCSA

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

NCSA

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

NCSA

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

NCSA

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

NCSA

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

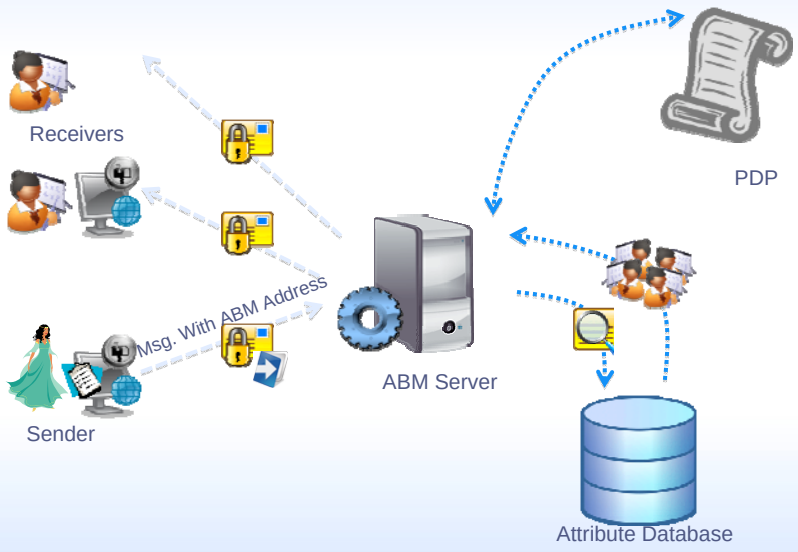
NCSA

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

NCSA

Strawman Architecture



NCSA

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 posses 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

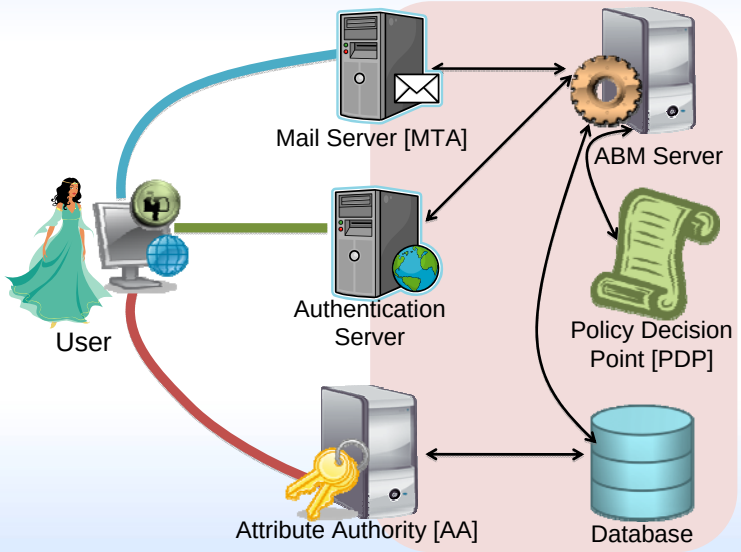
- {Reading policy} = {Receiving policy} – correctness
  - Translate receiving policy into a reading policy
- Ex: (“Position_val_Faculty”) AND (Salary > 150000)
- An Attribute Authority (AA) issues attribute keys to each user based on the enterprise database
  - E.g., “Faculty” attribute has a key

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

NCSA

High Level Architecture



NCSA

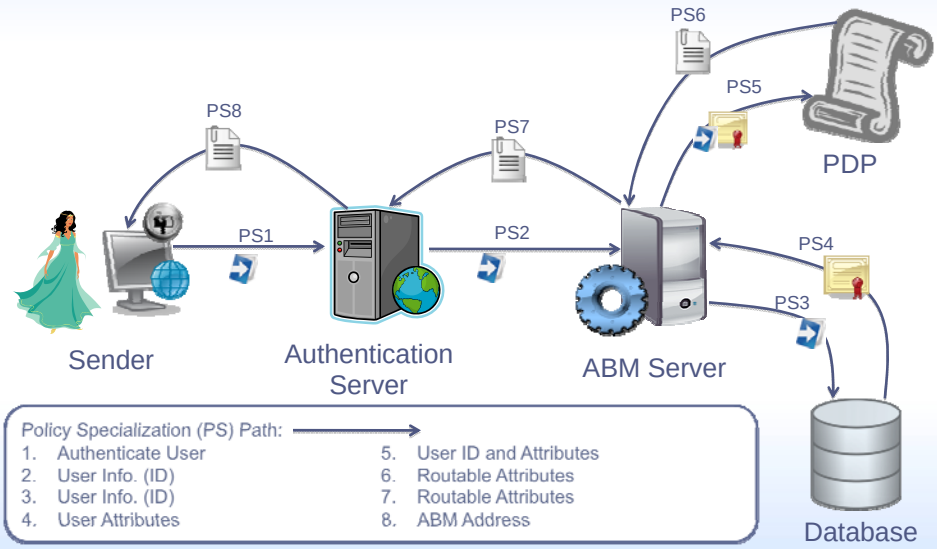
Protocol Steps

The protocols for the ABM system are given in terms of three “paths”

- Policy specialization path
- Messaging and address resolution path
- Attribute keying path

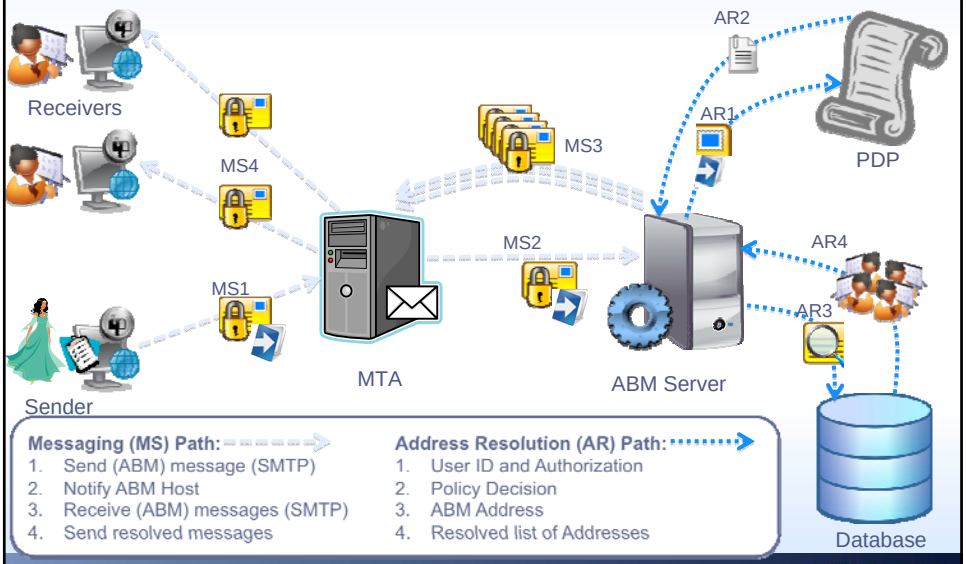
NCSA

Policy Specialization Path



NCSA

Messaging and Address Resolution Path

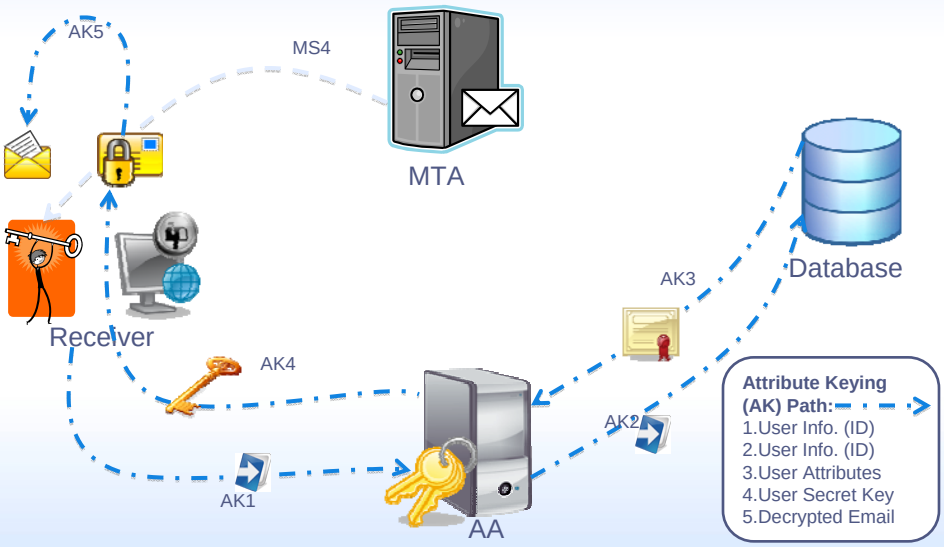


Messaging (MS) Path:
1. Send (ABM) message (SMTP)
2. Notify ABM Host
3. Receive (ABM) messages (SMTP)
4. Send resolved messages

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

NCSA

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

NCSA

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?

NCSA

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].

NCSA

Encryption Time

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

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

Decryption times averaged 352ms.

NCSA

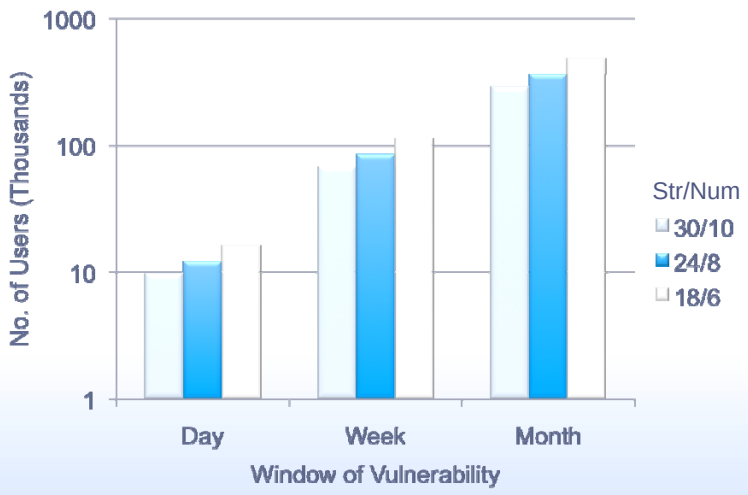
Key Generation Time

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

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

NCSA

AA Scalability



NCSA

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
    - < 400ms for a 60K RDB
    - < 8 seconds for 60K XML DB

NCSA

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.