Attribute-Based Authenticated Key Exchange

Choudary Gorantla, Colin Boyd and Juan González Nieto

ACISP 2010
Outline

1. Introduction
2. Attribute-Based Key Exchange
3. Attribute-Based Key Encapsulation
4. AB-AKE from AB-KEM
Outline

1. Introduction
2. Attribute-Based Key Exchange
3. Attribute-Based Key Encapsulation
4. AB-AKE from AB-KEM
What is attribute-based key exchange?

- Users wish to share a new session key for protection of a session
- Users are authorised to participate not due to identity but by possession of appropriate attributes
- Any user with the correct attributes can participate – naturally a group scenario
- Security must prevent collusion between parties who each have partial attributes
Contributions

- Introduce key exchange in the attribute-based setting
- Introduce key encapsulation in the attribute-based setting
- A concrete key encapsulation mechanism in the attribute-based setting
- A generic one-round attribute-based key exchange protocol
Key policy vs. ciphertext policy

- **Key policy**
  - Attributes associated with data
  - Policy associated with private keys

- **Ciphertext policy**
  - Attributes associated with private keys
  - Policy associated with data

- Ciphertext policy systems seem more natural for key exchange; a user can determine a policy for whom it wants to communicate with.
Access structures

- A set of attributes $S$ is defined for the system
- A policy for participation in a key exchange protocol will be defined by an *access structure* $\mathcal{A}$ which is a set of subsets of $S$
- We only allow *monotone* access structures: having more attributes gives more access
Access trees

- AND
  - OR
    - citizen
    - permanent resident
  - 2 of 3
    - bachelor degree
    - special skill
    - age > 30
Outline

1. Introduction
2. Attribute-Based Key Exchange
3. Attribute-Based Key Encapsulation
4. AB-AKE from AB-KEM
Goals of Attribute-Based Key Exchange (AB-AKE)

- An access structure $\mathcal{A}$ is given as input to all the users.
- Any user with attribute set that satisfies $\mathcal{A}$ is a potential participant in the protocol.
- The set of parties whose individual attributes satisfy $\mathcal{A}$ can compute a common session key.
- Collusion resistance.
Security for AB-AKE

- Adversary schedules communication between parties
- Adversary can fabricate messages
- Adversary can obtain session keys from other sessions and also corrupt users to obtain long-term keys
- In order to win the security games adversary must be able to distinguish session key of target session from a random key
Building blocks for our construction

1. Attribute-based key encapsulation mechanism (KEM):
   - public-key primitive allowing any user to send a random secret to the owner of the private key
   - use construction based on attribute-based encryption scheme of Bethencourt, Sahai, Waters

2. KEM-based key agreement:
   - each participant generates a secret and sends it confidentially to other participants
   - session key combines all secrets using a pseudorandom function
   - construction already known to work for two-party ID-based (ACISP 2008) and group certificate-based (ICISC 2009)
Attributes defined to describe users
Users are issued a key according to the set of attributes they hold
Encryptor chooses policy defined over attributes
Users with attributes satisfying policy can decrypt
Useful for protection of remote file storage
Attribute-based key encapsulation

- Like attribute-based encryption but each party gets a random key instead of a message
- Encapsulation algorithm takes as input an access structure $\mathcal{A}$ and outputs a key $K$ and encapsulation value $C$
- Decapsulation takes in $C$ and a private key
- If the owner of the private key has attributes satisfying $\mathcal{A}$ then the decapsulation algorithm returns $K$
Constructing AB-KEM

- Based on ABE algorithm of Bethencourt, Sahai and Waters (2007)
- Uses access tree incorporating AND, OR and threshold
- A new ephemeral secret $s$ is chosen at encryption time
- Idea is to place $s$ at the root of the tree and share it at the next level. Subsequent levels are used to share secrets at the next level up
- Decapsulation recovers $s$ in the exponents of $e(g, g)^r$ where $r$ is unique to the decryptor
- Pairings are used cancel out the random elements
Access trees

AND

OR
- citizen
- permanent resident

2 of 3
- bachelor degree
- special skill
- age > 30
Outline

1. Introduction
2. Attribute-Based Key Exchange
3. Attribute-Based Key Encapsulation
4. AB-AKE from AB-KEM
Group Key Exchange from KEM

- Two-party KEM-KEM generic construction of BCGP at ACISP 2008
- GBGM extended to group case using multi-KEM at ICISC 2009
- Use same idea for group AB-AKE
Generic One-Round AB-AKE

Computation

\((K_i, C_i) \leftarrow \text{Encapsulation}(PK, T)\)

Broadcast

\(U_i \rightarrow * : C_i\)

Key Computation  

Three steps:

1. \(K_j \leftarrow \text{Decapsulation}(sk_i, C_j)\) for each \(j \neq i\)
2. \(\text{sid} = (C_1 \parallel \cdots \parallel C_{\tilde{n}})\), where \(\tilde{n}\) is the number of
   protocol participants
3. \(\kappa = f_{K_1}(\text{sid}) \oplus f_{K_2}(\text{sid}) \oplus \cdots \oplus f_{K_{\tilde{n}}}(\text{sid})\)
   where \(f\) is a pseudorandom function
The generic AB-AKE protocol is AKE-secure assuming that the EP-AB-KEM is IND-CCA secure.
Future Directions

- It would be better if we could add *forward secrecy*
- Also possible to consider additional security properties for AB-AKE:
  - insider security
  - KCI resilience
  - ...
- May not be possible to do this for a one-round protocol