Zeutro LLC
Encryption & Data Security

April 17, 2018

An Introduction to Attribute-Based Encryption

Attribute Based Encryption

Encryption is a method of encoding data that protects the confidentiality of its contents from unauthorized attackers. Traditionally, encryption has been viewed as a tool to enable secure communication between a sender (encryptor) and a targeted recipient of information. For example, one might wish to store a message such that it can only be decrypted by the user `bob@yahoo.com`.

While "point to point" encryption has many uses, this view of encryption is too rigid to meet all of the information sharing demands of today's cloud environments. Consider, for example, if we had a database of encrypted images that were labeled with the date/time, location, source and keywords related to the image. Further suppose an authority later decided to give an analyst the ability to examine all images in the region of "Santa Monica Pier" between 9am and 3pm on December 1, 2015. If the image database were encrypted under a traditional public key encryption scheme, the authority would have two choices. One is to not give the analyst the private key and thus not gain needed access to the information. The second is to give the analyst the key and thus give him the ability to decrypt all images in the database — including those outside of the scope. Clearly, both choices result in an undesirable outcome and both are direct products of the "all or nothing" power of traditional encryption/decryption systems.

Attribute-Based Encryption (ABE) is a new vision of encryption that moves beyond such traditional restrictions by allowing for flexible policy-based access control that is cryptographically (or mathematically) enforced. Let's return to our above example, but this time assume that images in the database were encrypted in an ABE system. In this scenario when each image was encrypted the data would be associated with a set of attributes (selected by the encryptor); these could include attributes such as the time the image was taken, GPS location along with other selected meta data. Later on if such an analyst came to an authority, the authority could create a private key for the analyst that was restricted to only be able to decrypt ciphertexts whose attributes matched the policy of "Location:Santa Monica Pier" AND "Time: in 9am - 3pm, December 1, 2015. This private key could decrypt any ciphertext whose attributes matched this policy, but would be worthless in decrypting any that did not. Crucially, the security of the system is based on mathematically hard problems and the security holds even if an attacker manages to corrupt the storage and obtain any ciphertext of his choosing.

While our motivating example focused on an encrypted database there are many examples of data that we wish to share in a flexible manner such as: email, network packets, sensor data. Furthermore the contexts where such data sharing is desired can vary from military/intelligence applications, to social networks, commercial sales data.

Types of Attribute-Based Encryption

In order to understand the capabilities of Attribute-Based Encryption, it helps to organize logically into three variants.

In an ABE system any string can potentially serve as an attribute. In addition, attributes can be numeric values and policies can contain ranges over these values. The set of attributes used will depend on the designated application.

Content-Based Access Control In an ABE system for content-based access control attributes will be associated with a ciphertext when encrypting sensitive data. On the flip side a private key will be associated with a policy over these attributes; typically the policy will be expressed as a boolean formula. (In academic literature this variant is sometimes referred to as "Key-Policy" ABE.) For example, in an system the encrypts emails we might extract the To: and From: addresses along with the time sent and subject as attributes, while encrypting the body of the email as secret data. A private key is generated by an authority, that is used to express what types of ciphertexts the key can decrypt. For example, a private key might allow for decryption of all emails that meet the policy of To:`engineering@corporation.com` OR (subject:casade-project AND Date $>$ Jan 1, 2015. [1] A private key can decrypt a ciphertext if and only if its policy (boolean formula) is satisfied by the attributes of the ciphertexts.

Role-based Access Control An ABE system for role-based access control "flips" the semantics of content-based access control. In such a system, attributes will be associated with a private key and a policy (or boolean formula) associated with the ciphertext. In such systems the attributes will often be associated with the credentials of a private key holder. (In academic literature this variant is sometimes referred to as "Ciphertext-Policy" ABE.) For instance, in an ABE system for a corporation a user might have a private key associated with the attributes Legal Department, Start:February, 2013, SECRET Clearance or a software developer could have attributes for each project she has worked on. When encrypting a ciphertext one will associate a policy to the ciphertext. For example, one could restrict a ciphertext only to employees who have been with the company since 2012 and worked on the "HALE" software project.

Multiauthority Role-based Access Control One issue with role-based access control is that in many applications we would like to write access control policies that span across different administrative boundaries. One difficulty with standard ABE is that it requires one authority to hand out private keys. However, in many applications it is natural for different authorities to manage different attributes. For instance, a company like Experian could distribute attributes about a user's credit score, while an HSCB might vouch for the insurability of an individual. A multi-authority ABE system allows one to associate a ciphertext with a policy written across attributes issued by different authorities.

Limitations of Alternative Solutions

We briefly go over some alternative solutions to ABE and discuss their limiations.

Identity-Based Encryption In standard public key cryptography, one encrypts to a user such as `bob@yahoo.com`, by first retrieving their key from a public key repository. In an Identity-Based Encryption (IBE) system this step can be skipped and one can encrypt with only the

[1] The image database example given above is another example of Content-Based Access Control ABE.

knowledge the a string (e.g., email address) of the targeted recipient. While removing the step of key retrieval is useful in some circumstances, IBE still follows the traditional model of point to point encryption where a ciphertext is targeted to a single identified user and does not support more flexible or expressive access control.

Server Enforced Access Control A final alternative is to utilize a trusted storage server to enforce flexible access control. In such a setup a trusted server will store information in unencrypted form. When a client contracts the storage server, it will send its (signed) access credentials, the server can then determine if they are authorized to access a particular data item and if so send this back. This solution will allow for flexible access control, but has several drawbacks.

- If the storage server is compromised, then data confidentiality is lost.
- The client must have continuous network access to a trusted server to access sensitive data.
- The client must contact the server for each data item it wishes to access.
- This solution does not translate to the multi-authority setting as one party must be responsible for managing the trusted server.
- For robustness it is desirable to store encrypted data at untrusted sites.

Taken all together, an Attribute-Based Encryption enables very expressive access control that is cryptographically enforced. This allows for flexible access sharing without relying on the a trusted third party per access.

Zeutro and Attribute-Based Encryption

Zeutro is the leader in providing access control solutions for Attribute-Based Encryption. For more information, please visit us on the web at http://www.zeutro.com or send us an email at info@zeutro.com.