Implementing Attribute-Based Encryption in Web Services

Song Luo, Jianbin Hu* and Zhong Chen
Institute of Software, School of Electronics Engineering and Computer Science, Peking University
Key Laboratory of High Confidence Software Technologies (Peking University), Ministry of Education
Beijing, China
Email: {luosong, hjbin, chen}@infosec.pku.edu.cn

***Abstract*—Web services are now widely used in web-based applications. To protect the information in web services, many security specifications have been proposed. Attribute-based Encryption (ABE) provides us a brand new cryptographic primitive for access control. This paper sets out to examine an unexplored area to date – how attribute-based encryption might be used to provide privacy and security for web services. We try to implement ABE in web services. The implementation and performance evaluation demonstrate that ABE is efficient and feasible in web services.**

***Keywords*-Attribute-Based Encryption; Web Services; Privacy; Access Control; Security**

I. Introduction

Web services are now widely used in web-based applications. It enables more dynamic, loosely-coupled and asynchronous interactions between inter-domain applications, compared to traditional approaches. To protect the information in web services, many applications use SSL/TLS protocol to transfer web services. But SSL/TLS can only provide transport-level security or peer-to-peer security which may not necessarily be appropriate for securing web services messages. Furthermore, web services should provide access control to service requestors. Thus, web services must consider not only transport-level security but also message-level security. Many relevant security specifications have been proposed, such as XML Encryption and Signature, WS-Security, SAML, XACML, XKMS, etc.

Attribute-Based Encryption (ABE) is a novel mechanism by which we can realize such access control policy in a cryptographic way. There are two kind of ABE schemes, key policy ABE (KP-ABE) and ciphertext policy ABE (CP-ABE) schemes. In the key policy ABE schemes [1], ciphertexts are associated with sets of attributes and users' secret keys are associated with access control policies. On the other hand, in the ciphertext policy ABE schemes [2], each ciphertext is associated with an access control policies. The access control policies are described with the attributes and therefore the concept of CP-ABE is closely related to Role-Based Access Control (RBAC [3]) and Attributed-Based Access Control (ABAC [4]). So it's natural for us to choose CP-ABE as the underlying cryptographic primitive in order to ease the private key management and enable the web service providers to exert the access control policy defined by himself over service requestors.

Our Contribution. Since web services adopt XML Encryption to provide confidentiality and XACML to provide access control mechanisms, it may be also an example of such beneficiary from ABE. We try to implement ABE in web services to provide security and privacy preservation mechanism. Compared with using XML Encryption and XACML, it may be a lightweight security solution for web services.

*Corresponding Author

II. Using ABE in Web Services

A. Model

Figure 1 depicts the model of using ABE in web services. In a scenario that a service requestor wants to invoke a secure web service enhanced by ABE from a service provider, the working flow is as follows:

- The service requestor registers to the key authority with her attributes. The key authority returns her private key.
- The service requestor sends a web service request to the service provider. The provider gets the corresponding access control policy, encrypts the information by using ABE under the policy and sends back to the requestor.
- The requestor decrypts the message by her private key if her attributes satisfy the policy contained in the returned message.

Figure 2 shows how ABE information is used in SOAP messages. To encrypt a SOAP message with ABE, we make the following modifications in SOAP message:

- Create a <wsabe> header and an <EncryptionMethod> subelement of the <wsabe> element to indicate the adopted encryption algorithm;
- Create a <KeyInfo> subelement of the <wsabe> element and the <KeyInfo> contains a subelement <PubKey> which contains the public key needed in encryption and decryption;
- Create an <EncryptedData> element and <CipherData> subelement . The <CipherData> contains two subelements: <Policy> defines the access control policy and <CipherValue> contains the raw encryption result.

978-0-7695-4128-0/10 $26.00 © 2010 IEEE
DOI 10.1109/ICWS.2010.82

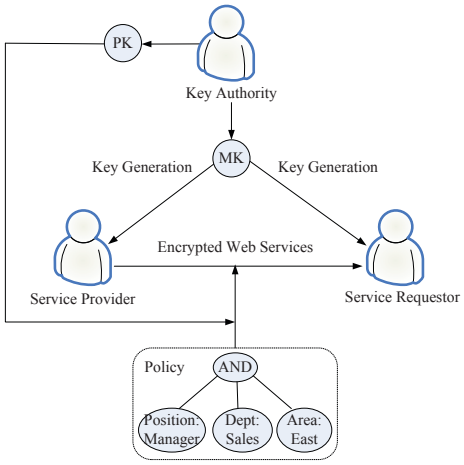

Figure 1. Model of Using ABE in Web Services

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="...">
    <SOAP-ENV:Header>
        <wsabe>
            <EncryptionMethod Algorithm="cp-abe">
            <KeyInfo>
                <PubKey>
                    ...
                </PubKey>
            </KeyInfo>
        </wsabe>
    </SOAP-ENV:Header>
    <SOAP-ENV:Body>
        <EncryptedData>
            <CipherData>
                <Policy>
                    ...
                </Policy>
                <CipherValue>
                    ...
                </CipherValue>
            </CipherData>
        </EncryptedData>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Figure 2. SOAP Message with Using ABE

The modifications are compatible with the specification in WS-Security so we can easily add ABE into WS-Security, if necessary.

B. Implementation

We use the open source web services tookit gSOAP [5], [6] and the Pairing Based Cryptography (PBC [7]) to implement our ABE scheme in web services. We implement an ABE scheme [8] by PBC and add it to the gSOAP stack using a plug-in.

We evaluate the performance of the scheme on a HP laptop running Windows XP SP2 with Intel(R) Core 2 Duo(R) CPU 1.66GHz and 1GB RAM. Table I shows the times of system setup, key generation, encryption and decryption when the number of attributes is from 10 to 50 with 2 values per attribute. The value is the average time of 20 different experiments. Each experiment randomly choose the random 256 bits AES key and a ciphertext policy. From the experimental results, we can conclude that our ABE scheme is feasible with desirable performance in web services.

Table I
EVALUATION RESULTS

Number of attributes	10	20	30	40	50
System Setup	0.51s	0.88s	1.26s	1.67s	2.09s
Key Generation	0.88s	1.75s	2.66s	3.68s	4.64s
Encryption	0.21s	0.39s	0.58s	0.80s	1.01s
Decryption	0.63s	1.20s	1.79s	2.46s	3.09s

III. CONCLUSIONS AND FUTURE WORK

ABE provides normal encryption and extra access control function. ABE is more efficient, flexible and suitable than other cryptographic techniques and may be a lightweight security solution for web services. We implement ABE in web services. The experimental results show that our scheme is efficient and feasible. The future work is to integrate ABE to WS-Security and unearth other potential advantages of attribute-based techniques and identify the associated practical and implementation issues.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai and B. Waters, *Attribute-based encryption for fine-grained access control of encrypted data*. In: ACM Conference on Computer and Communications Security, pp. 89-98 (2006)

[2] J. Bethencourt, A. Sahai and B. Waters, *Ciphertext-policy attribute-based encryption*. In: IEEE Symposium on Security and Privacy, pp.321-334 (2007)

[3] R.S.Sandhu, E.J.Coyne, H.L.Feinstein and C.E.Youman, *Role-based access control models*. IEEE Computer, 29(2):38-47, February 1996.

[4] E.Yuan, J.Tong, *Attributed Based Access Control (ABAC) for Web Services*. In: Proceedings of the IEEE International Conference on Web Services (ICWS'05), Orlando, Florida, July 2005.

[5] Robert A. van Engelen and Kyle Gallivan, *The gSOAP Toolkit for Web Services and Peer-To-Peer Computing Networks*, In: Proceedings of the 2nd IEEE International Symposium on Cluster Computing and the Grid (CCGrid2002), pp.128-135, May 21-24, 2002, Berlin, Germany.

[6] gSOAP, http://www.cs.fsu.edu/~engelen/soap.html.

[7] PBC: The Pairing-Based Cryptography Library, http://crypto.stanford.edu/pbc/.

[8] S. Luo, J. B.Hu, Z. Chen, *A flexible ciphertext policy attribute-based encryption scheme*. In: Technical Report, Peking University, 2009.