SECURE SERVICE PUBLISHING WITH UNTRUSTED REGISTRIES

Securing Service Discovery

Slim Trabelsi and Yves Roudier
Institut Eurecom, 2229 route des Cretes, BP 193, 06904 Sophia-Antipolis, France
trabelsi@eurecom.fr, roudier@eurecom.fr

Keywords: Security, Service Discovery, Attribute Based Encryption, Trust, Privacy, Untrusted registry.

Abstract: Service Discovery becomes an essential phase during the service deployment in Ubiquitous system. Applications and services tend to be more dynamic and flexible. Users need to adapt in order to locate these pervasive applications. Service mobility introduces new security challenges relating to trust and privacy. Existing solutions to secure the service discovery cannot provide any solution without relying on a trusted third party. In this paper we purport to use Attribute Based Encryption so as to protect the publishing and binding messages with untrusted registries.

1 INTRODUCTION

Service Oriented Architectures (SOA) introduce a loosely coupled interaction model for protocols and procedures interconnecting different systems or software components. SOA consists mainly of services, which are application elements providing elaborate functions (database access, data processing, business logic …), useful for clients requesting such services. Orchestration of such services is becoming an essential feature in increasingly pervasive systems. Service discovery is a basic component of orchestration that allows the dynamic detection of previously unknown services available in the network. Service mobility introduces new security challenges regarding trust and privacy. Private data exchanged during the discovery process can be re-used for illegal purposes. Failures in the discovery protocol can ease denial of service attacks. Most of the existing solutions to secure discovery rely on trusted third party such as security modules, secure proxies, or trusted registries in charge of the encryption and of trust establishment among users. Such additional modules are not deployable on a large scale nor realistic for pervasive computing scenarios where mobile clients and services do not have any a-priory knowledge of the ambient environment. This paper suggests a new approach based on attribute based encryption to enable secure service discovery without trusting registries.

This paper is organized as follows. Section 2 introduces service discovery and its threat model. Section 3 details how to secure service discovery using Attribute Based Encryption. Section 4 finally compares our approach with related work.

2 SERVICE DISCOVERY AND SECURITY THREATS

With the emergence of new dynamic networks and services where devices are ubiquitous, discovery techniques are being adapted in order to find mobile services rather than devices. Centralized discovery approaches rely on a registry which plays the role of yellow pages, which clients can refer to. A service advertises its capabilities to the registry, which then stores them for a certain amount of time. A client solicits the registry to find a service by sending a request containing service preferences. The registry tries to match the requested service with the most suitable provider. In that approach, registries have to be considered by the services and the clients as a trusted third party. An alternative approach exists that relies on peer to peer advertisements between services and clients. This paper only addresses the registry based model.

Securing service discovery encompasses addressing the following threats:

- Client's intention: A malicious registry can establish an "intentional" profile about each user, and re-use it for commercial purposes (without any authorisation). It may thus act like a spyware in an infected computer.
- Illegal competition: service providers may want to prevent potential commercial competitors or malware from gathering information about their offers too easily.
- Wrong matching: A malicious registry can perform wrong matching with the client's request in order to re-direct it to malicious services (or other services that do not have anything to do with the client's wish).
- Fake registrations (fishing): Fake services have the possibility to register and trap putative clients. A service could register as a banking service in order to obtain from users their confidential banking numbers.

These threats lead to the following essential security requirements:

- Confidentiality: Exchanged data must be protected against any external access
- Privacy: Private data related to clients and services must be disclosed only to authorized entities.
- Authentication: Every entity must be able to authenticate the capabilities of its counterpart before disclosing personal data.
- Access Control: Services should restrict their discoverability only to a restricted class of clients. Clients must also be able to limit the scope of their discovery request to trusted (certified) services.
- Integrity: All exchanged messages must be checked to verify the authenticity of the content and detect illegal modifications.

Usually, during the service discovery execution a lot of private information like identities, location, addresses, URI, owner, or domain are exchanged and exposed to illegal uses (profiling, phishing). The protection of such information, as well as the assurance to obtain a correct response to service discovery entirely depends on the trust clients and services can put into the registry and its authentication capabilities. Users can then protect their communications by encrypting exchanged messages using a PKI. Still, registries belonging to unknown domains cannot always be trusted.

3 SECURING SERVICE DISCOVERY

(Trabelsi, 2006) used an extension of the Identity Based Encryption (IBE) (Boneh, 2001) called Attribute Based Encryption (ABE) (Sahai, 2005) in order to secure the Web Service Discovery in a P2P setting. This section describes how to extend multiple registries with a similar mechanism.

3.1 Attribute Based Encryption

ABE makes it possible to encrypt a message or a document using a set of attributes characterizing its intended recipient as a public encryption key., without the need for a public key of that recipient. The ABE public key has a semantic meaning (a name, a mail address, an identifier …), and does not require to be verified with a Certification Authority (Figure1).

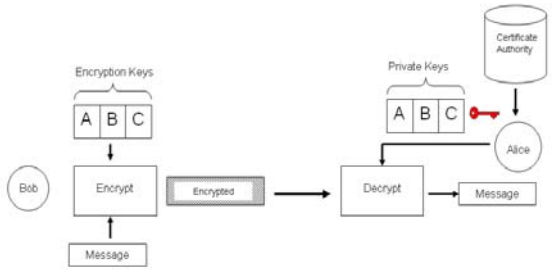

Figure1: Attribute Based encryption

3.2 ABE Extension of WS-Discovery

WS-Discovery is essentially used for web service discovery in a decentralized fashion and initially dedicated to LANs. This protocol relies on a multicast diffusion to locate services connected to a restricted sub-network. Proxies are used to extend the scope of the discovery to other networks. Clients multicast Probe service query messages and relevant services listening to the same multicast address will respond directly to the requester with a ProbeMatch response message containing the information to access the service. Services can also announce their existence by multicasting Hello messages containing their description. The WS-Discovery specification

defines two default attributes: Type (an identifier of the service endpoint), and Scope (to organize services into logical groups).

(Trabelsi, 2006) described how, in order to protect and restrict the service binding to only certified servers, a client might encrypt his "Probe" message using Type and Scope attributes as a public key as follows: $Encrypt[ProbeMessage]_{\{Type,Scope\}}$. Only key holders with the correct values of the attributes Type and Scope will be able to decrypt the query message. The same concept is used to protect the service response message which can be restricted to a restricted group of users by encrypting the "ProbeMarch" message with specific attributes. For example, a ProbeMatch message in a university an administrative service might be restricted to professors only: the message sent will correspond to: $Encrypt[ProbeMatch]_{\{Bob,Professor\}}$.

In WS-Discovery one can also rely on a centralized registry called "Proxy" performing the matching. This configuration extends the scope of the discovery to other networks and domains without the necessity to share the same multicast address. The ABE approach exposed above is however end-to-end: if the proxy has no private keys related to the attributes used to encrypt the messages, it will be unable to perform a correct matchmaking. We therefore suggest replacing the encryption of the messages with a partial encryption of the sensitive data structure contained. Only metadata needed by the proxy to forward the message to an appropriate entity will be sent In cleartext, the data remaining themselves protected. In WS-Discovery, such information is limited by default to *Type* and *Scope*, but the data structure can be extended with other attributes. We propose to partially encrypt the publish (Hello) and bind (Probe) messages so that the matching attributes are kept clear for the Proxy.

3.3 New Message Format

In WS-Discovery a "Hello" message is composed of two parts: the header (containing session information related to the protocol) and the body (containing information about the service). Only some attributes of the body are useful for the Proxy. In order to protect its private information and restrict the discovery of its profile to some allowed user, the service provider can encrypt the entire message except for the type and scope attributes (Figure 2).
The "Probe" message, sent by the client to the Proxy in order to query for a service, also contains a header providing session information and client's endpoint reference (for the reply message), and a body describing the attributes corresponding to the requested service.

```
<s:Envelope>
  <s:Header>Encrypt[Header]{Professor}
  </s:Header>
  <s:Body> <d:Hello>
    <a:EndpointReference>
 Encrypt[EndpointReference]{Professor}
    </a:EndpointReference>
    <d:Types>Printer</d:Types>
    <d:Scopes>University</d:Scopes>
    <d:XAddrs>
     Encrypt[XAddrs]{Professor}
    </d:XAddrs>
  </d:Hello></s:Body></s:Envelope>
```

Figure2: Encrypted Hello Message

As seen previously, the client can protect the "Probe" message against unauthorised access by encrypting the sensitive part of the message and keeping the matching attributes in clear (Figure 3). Only services with the correct keys (attributes) will respond.

```
<s:Envelope>
<s:Header...>Encrypt[Header]{Printer,University}
</s:Header>
<s:Body> <d:Probe>
    <d:Types>Printer</d:Types>
    <d:Scopes>University</d:Scopes>
   </d:Probe></s:Body></s:Envelope>
```

Figure3: Encrypted Probe Message

3.4 Towards a Hybrid Solution

After the modification of this part of the WS-Discovery protocol, an efficient large scale service discovery can be performed in a secure manner, without the need to establish a trust relationship with the proxy. In a centralized configuration, if the service does not exist locally, the client will stop sending its binding message or will retry the binding process later. On the contrary, with a proxy-based configuration, if the service is not found locally, the local proxy can forward the query to proxies belonging to other domains and networks. Proxies do not necessarily know one another, but they can communicate via a multicast address. With the proxy based solution, we can avoid bottlenecks on the service side. With the decentralized solution,

when a client multicasts an encrypted probe message, all the servers that are listening to the multicast channel will try to decrypt the message at the same time. During the decryption period, if another client sends another Probe message, it could be dropped or cached until the end of the previous message decryption. This phenomenon generates a bottleneck on the service side that could be avoided with the Proxy-based solution. With this proxy-based solution, the secure service discovery is extended to other LANs and solves the bottleneck problem created by the decentralised solution. This performance improvement is conditioned by a privacy relaxation.

4 RELATED WORK

(Carminati, 2005) raised the privacy issues in Web Services with trusted UDDI-based Discovery Agencies (equivalent to a foreign agency providing a registry service). After describing the privacy requirements related to the discovery mechanisms, they provide five UDDI-based registries scenarios (Internal enterprise application, Portal, Partner catalog, and e-Marketplace). For each scenario, they proposed the application of three privacy enforcement strategies: Access-Control based solution using a third trusted party (a trusted UDDI registry) that is in charge of the access-control policy enforcement to the registry. Cryptographic-Based Solution, also relying on a trusted third party called encryption module in charge of encrypting sensitive data (XML encryption), according to a specific privacy policy provided by clients and services. Hash-Based solution where service providers publish hashed services in an untrusted registry. Compared to our ABE solution, Carminati's solution must rely on a trusted third party or a trusted registry to secure the service discovery; otherwise, they use insecure hash mechanisms.

(Czerwinski, 1999) proposed an architecture relying on an additional component, called Service Discovery Service (SDS), which plays the role of a secure information repository (secure registry). This SDS helps clients and servers set up a trust relationship and secure channels among them: using a PKI, it provides authentication, access control, encryption, signature verification, and privacy protection. The main idea is to create a kind of VPN in which clients, servers and registries could communicate in a secure manner. In order to encrypt the exchanged messages, the SDS uses a hybrid public/symmetric key system. Trust establishment between the SDS and other entities is limited to a simple verification of the SDS public certificate validity. This kind of infrastructure is based only on certificate verification; in this case, every user with a valid certificate is able to discover all existing services without any restriction.

5 CONCLUSION

This paper proposed an encryption-based solution to secure service discovery with multiple registries. The use of an Attribute Based Encryption scheme enables a selective publication and binding without exposing private and sensitive data to an illegal use by a potentially untrusted registry or an outsider. This scheme also couples access control with confidentiality protection. Clients and services can define their security preferences by choosing the appropriate attributes required from the receiver to decrypt the discovery message. Untrusted registries can only match and route discovery messages based on attribute metadata, which are left in cleartext.

REFERENCES

Boneh, D., Franklin, M., 2001, "Identity-based encryption from the weil pairing", 21st Annual International Cryptology Conference on Advances in Cryptology.

Carminati, B., Ferrari, E., Hung, P.C.K, 2005, "Exploring Privacy Issues in Web Services Discovery Agencies", IEEE Security and Privacy .Volume 3, Issue 5

Czerwinski, S.E. et al, 1999, "An Architecture for a Secure Service Discovery Service" , In Proceedings of MobiCom '99.

Martin, D et al, 2004, "Bringing Semantics to Web Services: The OWL-S Approach", Proceedings of the 1st SWSWPC.

Trabelsi, S., Pazzaglia, J.C, Roudier, Y., 2006, "Secure Web service discovery: overcoming challenges of ubiquitous computing", 4th IEEE European Conference on Web Services, ECOWS 2006.

Sahai, A., Waters, B., 2005, "Fuzzy Identity-Based Encryption", Advances in Cryptology-Eurocrypt'05.

WS-Discovery Specifications 2004, http://msdn.microsoft.com/ws/2005/04/ws-discovery/