SECURE SERVICE COMPOSITION IN SENSOR WEB

Genong (Eugene) Yu, Liping Di

Center for Spatial Information Science and Systems, George Mason University, 6301 Ivy Ln, Suite #620, Greenbelt, MD 20770, USA

1. INTRODUCTION

Geospatial Web Services have been populated. Interoperability at the service level becomes realistic. One level is the composition of geospatial Web services in a workflow environment. For example, the workflow can be scripted in Business Execution Language (BPEL) and get executed at a BPEL execution engine. Interoperation raises the concern of security to Web services and data. Certain information and services need to be restricted to limited users. Access should be protected using some security measures. This is not just limited to user/password authorization, but data integrity and rule-based access control. A workflow needs to access several services in one execution. If many of the services need authorization and data protection, the BPEL execution engine need to be a participant in the secured workflow to allow the data and services to passed along. Several special issues for workflow security arise. One is if there are many authorization keys and how the workflow gets these keys without breaking the rules of desired security. Feeding all the authentications into the workflow is not a good choice since they may expose a security issue itself. Another is how to protect the workflow engine itself in executing a secured workflow. These are the foci for this study.

2. RELATED WORK

OGC has two geospatial security extensions. One is GeoXAML which is an extension to OASSIS XAML. It supports "Click-through" and access control[1]. Another is GeoRM for data use control[2]. The OGC Web Services 6 (OWS 6)is developing the public key infrastructure (PKI) for geospatial Web services. This should resolve the problem of authorization specifically for geospatial web services.

Security concern for Sensor Web has emerged during OWS 6. Sensor Web enablement services enable the live connection between sensors and end users. The access to the original sensors in many cases has to be secured for safety. Authorization is required. Also, the data integrity should be protected. The amount of data relayed through the Internet and leaves many places to be attacked and tampered en route. These threats can be tampering and forgery of data, illegal copy and distribution of data, unauthorized service, refusing of access privilege, exposure of confidential information, data error, tampering and deletion of data, and failure of interoperability of system. These can be roughly grouped into two main groups: authorization and authentication. OpenID provides one alternative route to allow users to login once and access any of the services s/he is entitled to[3-5]. This is what the workflow engine needs to enable a secure execution of workflow that involves many services.

3. METHODOLOGY

This study focused on the enablement of security for geospatial workflow.

3.1. Specifications

Studied specifications include OGC GeoXAML, GeoRM, WS-Security, and OpenID.

3.1. Implementation

The specific workflow engine is a BPEL engine. The security is enabled by securing the engine itself and allowing the engine to access secured geospatial Web services. Figure 1 shows a general architecture to use OpenID infrastructure.

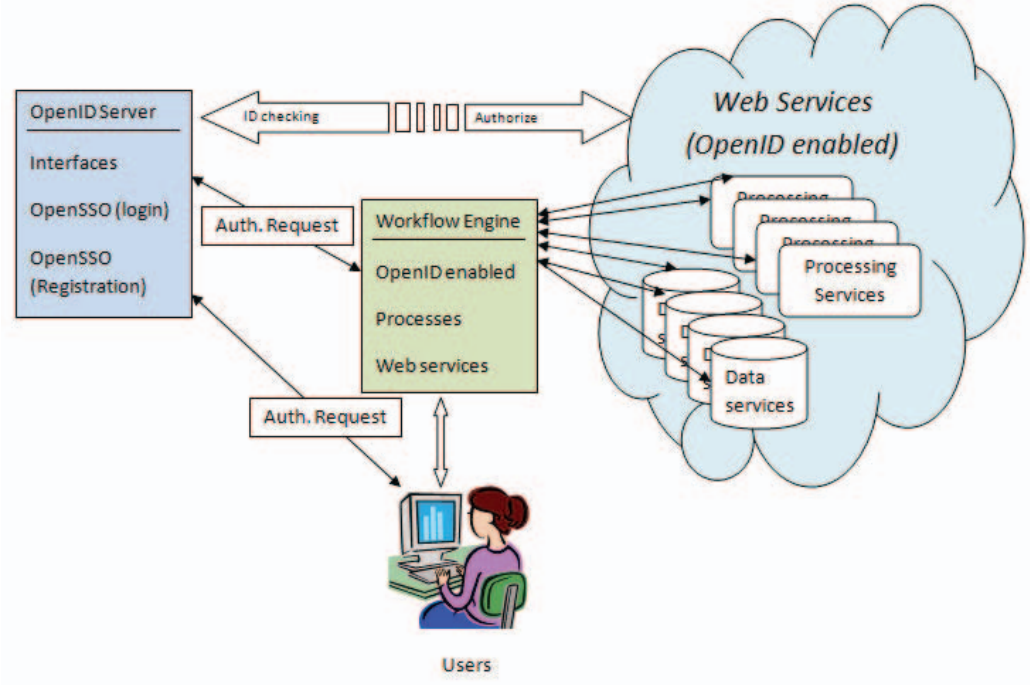

Figure 1. OpenID-enabled Secure Workflow

4. RESULTS AND DISCUSSIONS

An OpenID scenario was implemented and tested. The OpenID approach worked well for saving the engine to deal with multiple authorization keys. The approach leaves less opportunity for leaking of secured keys. However, OpenID requires all services are OpenID-enabled. Users may have their preference in security measures. This leads to the future direction of efficiently dealing with multiple measures in a workflow.

5. CONCLUSION

A secure geospatial workflow execution environment was implemented and demonstrated. The OpenID approach ensures the security while it simplifies the authorization process, only if services are OpenID-enabled.

Future directions are to examine alternative security measures and to support multiple security measures in one workflow.

11. REFERENCES

[1] A. Matheus and J. Herrmann, "Geospatial eXtensible Access Control Markup Language (GeoXACML) ": Open Geospatial Consortium Inc. , 2008, p. 55.

[2] G. Vowles, "Geospatial Digital Rights Management Reference Model (GeoDRM RM)," Open Geospatial Consortium Inc. , 2006, p. 129.

[3] OAuth, "OAuth Core 1.0." vol. 2008, 2007.

[4] OpenCA, "Introduction to OpenCA LABS." vol. 2008, 2008.

[5] OpenSSL, "The OpenSSL Project." vol. 2008, 2008.