Single Sign-On Scheme based on XML for Media Device Control in the Ubiquitous Home Network Running the OSGi

Dongkyoo Shin and Dongil Shin

Department of Computer Engineering, Sejong University
98 Gunja-Dong, Gwangjin-Gu, Seoul 143-747, Korea
{shindk, dshin}@sejong.ac.kr

Abstract

A single sign-on scheme is proposed in which a user offers his credential information to a home network running the OSGi (Open Service Gateway Initiative) service platform, to obtain user authentication and control a remote device through a mobile device using this authentication scheme, based on SAML (Security Assertion Markup Language). Single sign-on profile is defined to overcome the handicap of the low computing and memory capability of the mobile device and automated user authentication is applied to control a remote media device using a mobile device in a ubiquitous home network based on the OSGi.

Keywords: *single sign-on, SAML, home network, OSGi, device control*

1. Introduction

In the OSGi service platform [1], every service bundle in the gateway operator requires user authentication. By the result, a user should complete authentication repeatedly whenever the user wants to access several number of services. This causes potential security problems as well as the difficulty of user access.

First of all, the main security problem with a home network environment based-on the OSGi service platform is that the security infrastructure is distributed and these architectures usually require that key security features be built into all parts of the system. In addition, a user must memorize usernames and passwords for each service. Additionally, the system's administrator manages many passwords in the database and is faced with potential insecure system problems due to the frequent transmission of these passwords at the sites [2]. SSO (Single Sign-On) is a good alternative to solve these problems. SSO is a security feature that allows a user to log into the many different services offered by the distributed systems while only needing to provide authentication once, or at least always in the same way [3].

In this paper, we propose a single sign-on scheme using SAML (Security Assertion Markup Language) for home network service environment based on the OSGi service platform. We simulated this environment by proposing and verifying a messaging scenario through implementation, and defined a profile to implement SSO through mobile devices with small memory capacities in distributed OSGi environments, which should exchange and verify a key to authenticate a user.

2. Background

Release 4 of the OSGi service platform defines a "User Admin Service" but only offers authentication for each service unit [4]. For this reason, when a user wants to access various services, a home network environment using the OSGi service platform

may have the same primary security problem experienced in a mobile or Web Services environment. SSO can be implemented by exchanging and reusing a user's authentication information, including the fact that the user has previously been authenticated by a specific method among different security domains. We specified the information in a uniform and unified way based on SAML.

2.1. OSGi (Open Service Gateway Initiative) framework

The OSGi service platform is divided into two parts: the OSGi Service Framework and OSGi Service [1]. The OSGi framework supports registry and life-cycle management for an OSGi service in Java runtime environment. As a bundle, an OSGi service such as HTTP, Logging, and Device Access Service is defined by Java Interface. A bundle is the minimum unit for managing a framework. A framework manages installing, uninstalling, resolving, stopping, starting, and active life cycle for bundle.

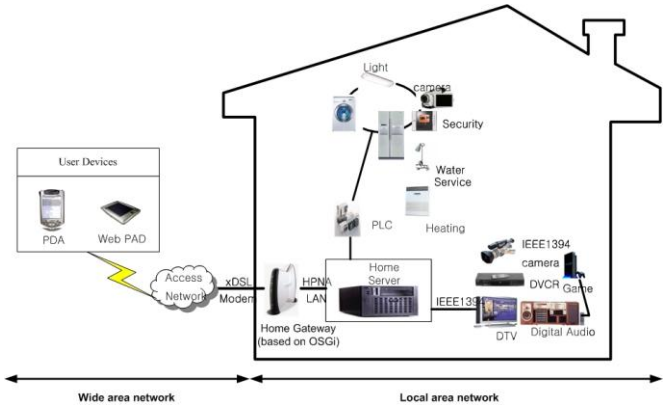

Figure 1. The OSGi Architecture

Figure 1 shows the OSGi framework, which connects the wide area network and the local area network. When a user wants to control a device in the local area network, he can control the device through the service being managed by the gateway operator in the wide area network. If there is a trust-relationship between the services, a user who has been authenticated from a service in the gateway operator can avoid any redundant authentication required to use other services.

In order to apply the SSO scheme to the home network as shown in Figure 1, the services extended from core services provided by the OSGi framework should be developed and deployed onto the OSGi framework. Figure 2 shows core services provided by the OSGi framework and extended services [5].

For experimental purposes, we implemented following extended services:

- Camera Control Service provides functionality for controlling a surveillance camera, such as camera view, camera on/off, and camera zoom in/out.
- Projector Control Service provides functionality for controlling a projector in a conference room or meeting room, such as projector on/off and adjusting.
- Single Sign On Service makes XML-based queries for user authentication. Also it plays the role of exchanging artifacts between the user and an Authentication Agent. After authenticating the user successfully, it leads the user to the destination service.

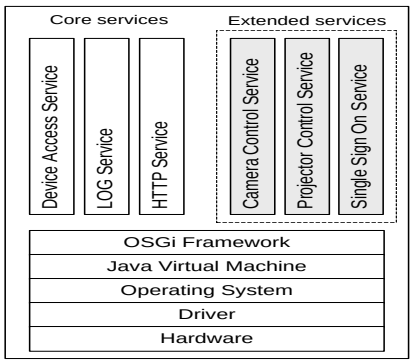

Figure 2. OSGi Framework and Extended Services

2.2. SAML (Security Assertion Markup Language)

SAML defines the request-response protocol using a subset of XML, by which systems accept or reject subjects based on assertions [6]. An assertion includes the statements generated by the SAML authority, conveying them and verifying that they are true. SAML defines three types of assertions: Authentication Assertion, Attribute Assertion, Authorization Assertion.

The SAML authority can be classified as authentication authorities, attribute authorities, and policy decision points according to the type of assertions included. SAML defines an artifact mechanism when the authentication request is too long for an HTTP redirect. The artifact has the role of a token. It is created within a security domain and sent to other security domains for user authentication. To achieve single sign-on, a mobile device keeps its artifact, which verifies that the mobile user has been authenticated once by the SAML authority in the system.

3. Single Sign-On Architecture for Ubiquitous Home Network Service Environment

The role of a security domain is to manage and control resources ruled by a specific access control policy. When a subject within a security domain requests resource from another security domain, the subject must be defined in the first security domain and a mutual trust-relationship must exist between the first security domain and the second security domain [7]. Specifically, OSGi recommends the HTTP service to offer users access to the services on the Internet and other networks [8]. Therefore we strongly suggest SSO as a core security scheme to improve user accessibility and security performance in home network environments exploiting the HTTP service.

The concept of the proposed Single Sign-On architecture is shown in Figure 3, in which the OSGi delivers certain services offered by service providers to the end user regardless of the system environments. In our implementation, a mobile user gains access to services being managed by a gateway operator with the SAML-based information related to his own authentication in order to control a remote camera and projector. A mobile user keys in his username and password to a mobile device in order to access the Camera Control Service in the gateway operator of the Wide Area Network. This user credential information is transferred to the SSO Service through the gateway operator, which connects the mobile device and Wide Area Network.

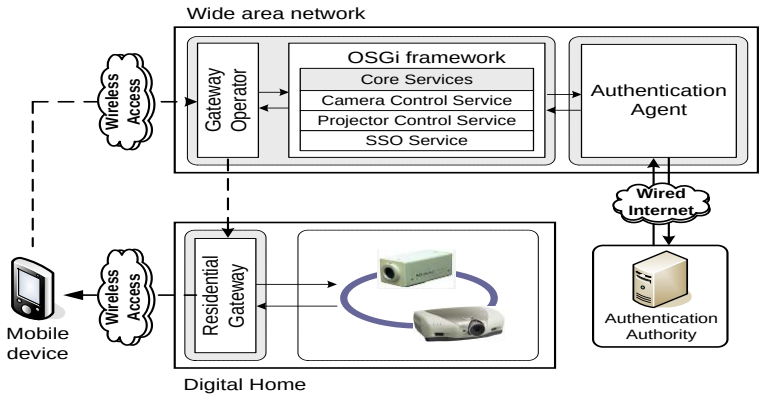

Figure 3. Proposed Single Sign-On Scheme

The user authentication procedure for the architecture is presented in the form of a sequence diagram in Figure 4, where each box in the diagram denotes an entity involved in this process. Figure 4 explains the messages between entities applying a user's single sign-on among services, in which there are mutual trust relationships.

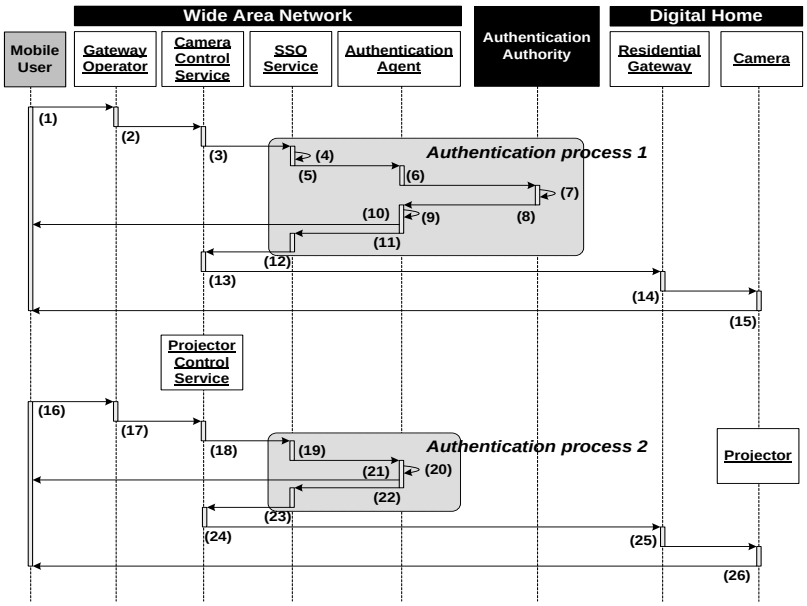

Figure 4. Sequence Diagram of the Proposed Single Sign-on Architecture

A description of each step is as follows:

(1) The mobile user keys his name and password into his mobile device in order to access the Camera Control Service via the gateway operator.

(2) The gateway operator transfers the user's credential information to the Camera Control Service. When the user's password is transmitted, the password must be encrypted.

(3) The Camera Control Service requests user authentication from the SSO Service, providing the user's credential information.

(4) The SSO Service makes a SAML-based authentication query and signs it digitally to be trusted by the Authentication Authority.
(5) The SSO Service sends the signed authentication query to the Authentication Agent.
(6) The Authentication Agent requests user authentication from the Authentication Authority.
(7) The Authentication Authority verifies the signed authentication query, decrypts the user's password, authenticates the user, makes an authentication assertion, and signs it digitally.
(8) The Authentication Authority sends this signed authentication assertion to the Authentication Agent.
(9) The Authentication Agent verifies the signed authentication assertion, evaluates it, and signs the evaluated result digitally. If the result is valid, the Authentication Agent generates an artifact for the mobile user.
(10) The artifact is assigned to the mobile user who wants to access the Camera Control Service.
(11) The Authentication Agent returns the evaluated result to the SSO Service.
(12) The SSO Service leads the mobile user to the Camera Control Service.
(13), (14), and, (15) The Camera Control Service controls the Camera via the Residential gateway in the Digital Home. Before granting access to the Camera, the Residential Gateway must verify the signed result.
(16) The mobile user who wants to access the Projector Control Service via the gateway operator provides the artifact received from the SSO Service (refers to step (10)).
(17) The gateway operator transfers the artifact to the Projector Control Service.
(18) The Projector Control Service requests user authentication from the SSO Service, providing the artifact instead of the user's name and password.
(19) The SSO Service sends the artifact to the Authentication Agent. The SSO Service no longer makes an authentication query.
(20) The Authentication Agent compares the artifact received from the SSO Service (refers to step (10)) with the original artifact (refers to step (9)). If the result is valid, the Authentication Agent removes the original artifact and generates a new artifact for the mobile user.
(21) The new artifact is assigned to the mobile user who wants to access the Projector Control Service.
(22) The Authentication Agent returns the signed evaluated result to the SSO Service.
(23) The SSO Service leads the mobile user to the Projector Control Service.
(24), (25), and (26) The Projector Control Service controls the Projector via the Residential gateway in the Digital Home. Before granting access to the Projector, the Residential Gateway must verify the signed result.

4. Conclusion

In home network environments based on the OSGi framework, there are some barriers to distributing automated user authentication due to the limited capabilities of mobile devices. To overcome these problems, we propose a security scheme to exchange user authentication information based on SAML under an OSGi-based home network environment. This scheme supports the efficient and secure transfer of a user's credential information between a mobile device and home networks, for service networks, and offers access to related domains without the burden of a repeated log-in process.

Acknowledgement

This research is supported by Seoul R&BD Program (SS110008).

References

[1] R. P. Diaz Redondo, A. F. Vilas, M. R.Cabrer, J. J. P. Arias, J. G. Duque and A. G. Solla, "Enhancing Residential Gateways: A Semantic OSGi Platform", IEEE Intelligent Systems, Vol. 23, Issue 1, **(2008)** pp. 32-40.

[2] A. Volchkov, "Revisiting single sign-on: a pragmatic approach in a new context", IT Professional, Vol. 3, Issue 1, **(2001)** Jan./Feb. pp. 39-45.

[3] Jian Yang, "An Improved Scheme of Single Sign-on Protocol", Fifth International Conference on Information Assurance and Security (IAS '09), **(2009)** August 18-20; Xian, China, pp. 495-498.

[4] I. Kim, D. Lee, J. Lee and K. Rim, "Extended Authorization Mechanism in OSGi", 2010 International Conference on Information Science and Applications (ICISA), **(2010)** April 21-23; Seoul, Korea, pp. 1-7.

[5] OSGi Alliance Std., OSGi Service Platform Release 4.3, OSGi Alliance, **(2011)**.

[6] OASIS Committee Specification, Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0, **(2005)**.

[7] A. Singhal, T. Winograd and K. Scarfone, "Guide to Secure Web Services", NIST(National Institute of Standards and Technology) Special Publication 800-95, **(2007)**.

[8] OSGi Alliance Std., Secure Provisioning Data Transport using Http, RFC36, **(2002)**.

Authors

Dongkyoo Shin received a B.S. in Computer Science & Statistics from Seoul National University, Korea, in 1986, an M.S. in Computer Science from Illinois Institute of Technology, Chicago, Illinois, in 1992, and a Ph.D. in Computer Science from Texas A&M University, College Station, Texas, in 1997. He is currently a Professor in the Department of Computer Science & Engineering at Sejong University in Korea. From 1986 to 1991, he worked in Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he worked in the Multimedia Research Institute of Hyundai Electronics Co., Korea as a Principal Researcher. His research interests include XML Security, XML based middleware, multimedia application, biological database, mobile Internet and ubiquitous computing.

Dongil Shin received a B.S. in Computer Science from Yonsei University, Seoul, Korea, in 1988. He received an M.S. in Computer Science from Washington State University, Pullman, Washington, U.S.A., in 1993, and a Ph.D. from University of North Texas, Denton Texas, U.S.A., in 1997. He was a senior researcher at System Engineering Research Institute, Deajun, Korea, in 1997. Since 1998, he has been with the Department of Computer Science & Engineering at Sejong University in Korea where he is currently a Professor. His research interests include Mobile Internet, Computer Supported Cooperative Work, Object-Oriented Database, Distributed Database, Data Mining and Machine Learning.