An User-Centric Attribute Based Access Control Model for Ubuquitous Environments

Fei Li[1], Dasun Weerasinghe[1], Dhiren Patel[2], and Muttukrishnan Rajarajan[1]

[1] Centre for Cyber & Security Sciences,
School of Engineering and Mathematical Sciences,
City University London, Northampton Square, London, EC1V 0HB
{Fei.Li,R.Muttukrishnan}@city.ac.uk
[2] Computer Engineering, NIT Surat, India, 395007
dhiren29p@gmail.com

Abstract. The recent developments in mobile platforms are significant, both on the hardware and software fronts. With the huge success of the iPhone and Android phones, more and more companies are entering the mobile application market. However, there are increasing security threats for mobile phone users due to the new generation of attacks targeted purely on mobile environments. Several solutions have been proposed to date, which can generally handle consent in a fixed and coarse-grained way. However, with the increasing usage of mobile devices for high value transactions, the future access control from mobile devices should be based on 'user-centric' challenge response techniques based on the freatures of mobile platforms.The authors present the MLive© framework, a novel approach to establish mutual authentication between the users and the service providers using unique mobile based attirbutes to solve the threats in the mobile environments.

Keywords: Attributes based access control, XACML, privacy, security, mobilepolicy.

1 Introduction

The number of mobile applications based on Android and iOS platforms has an increasing presence in the mobile application stores over the last five years. Online social networks (OSNs) like Facebook, YouTube, and MySpace are encouraging the users of the latest smartphones to download applications onto their handsets to add extra functionalities. These OSNs make the user to be the content producer and are encouraging new users to join the OSNs. Currently there are more than 250 million active users accessing Facebook through their mobile devices [1]. People that use Facebook on their mobile devices are twice as active on Facebook than non-mobile users [1]. Today mobile clients are becoming dominant platform for web browsing and accessing OSNs. The OSN providers collect a large number of users' data. Users usually share their location (including home address, work place etc.) with their friends. These sensitive data should not be collected by the OSN providers. Users

J.Y. Zhang et al. (Eds.): MobiCASE 2011, LNICST 95, pp. 361–367, 2012.

should have the right to decide whether to disclose these data to the others. Hence privacy should be preserved in the OSNs' environments.

Security, privacy and trust as well as the closely related issue of identiy management are considered as important in the mobile user-generated services. The security framework for mobile platform should be flexible, scalabe and interoperable. The Attributes Based Access Control (ABAC) based on XACML (eXtensible Access control Markup Language) can substantially improve the security and management of access control rights on sensitive data. The large adoption of XACML in the access control systems shows the huge success of XACML [2].

In this paper, we present our novel MLive© framework that achieves mutual authentication between both the user and the online service providers. At the same time, users are able to define their personal policies for disclosure of sensitive data, which is a flexible and user-centric approach. Section 2 presents the related work on mobile web-services security. Section 3 describes the MLive© framework in detail. Section 4 discusses the evaluation of the architecture. Section 5 summarizes the work presented in this paper with a short.

2 Related Work

Ubiquitous e-business is one of major topics in intelligent manufacturing system. Ubiquitous e-business environment requires security features including access control. An Ubi-RBAC model [3] which is based on the RBAC model adds new components such as space, space hierarchy, and context constraints. The Ubi-RBAC covers the context awareness and mobility of subjects (human users), which are the key issues of access control in the ubiquitous e-business environment.

There are three major widely used identity management solutions, namely the Liberty Alliance, OpenID and CardSpace from Microsoft. Ahmed et al. [4] analyzed 3GPP standardized OpenID with Generic Bootstrapping Architecure (GBA) protocol which allows cellphone users to use OpenID services based on SIM credentials. The security analysis suggests that the inter-networking of OpenID with GBA is secure in the ProVerif model [5]. However, the protocol breaks under strong adversarial model. The authors in [6] discuss how telecom operators can be part of a mobile security evolution and exploit it commercially by facilitating the adoption of OpenID. They propose a service architecture where the operator is able to exploit the growing acceptance and user base of OpenID by combining it with SIM-authentication.

The CardSpace is a browser and operating system extension that presents a particular user login experience using a wallet-and-identity-card metaphor. However, most of the browsers installed on the cellphones do not have complete functions.

The Liberty Alliance specifications like the Liberty Identity Federation (ID-FF), Identity Web Services Framework (ID-WSF) and Identity Service Interface Specification (ID-SIS) are mainly concerned on federated identity of Internet applications in the current wireless technology especially in mobile networks [7]. Other than OpenID and CardSpace, the Liberty Alliance is based on the notion of federated identity. A federation context is represented by a circle of trust that is constituted by service providers (SPs) and Identity Providers (IdPs) having mutual trust relations. In 2009, it moved to a new organization named Kantara.

3 MLive© Framework

There are five main actors: the consumer, the service providers (SPs), policy evaluation component (PEC), attributes authority (AA) and the identity provider (IdP).

In this scenario, AA is the trusted third party that stores all the attributes, including both the SPs' and the consumers' attributes. Usually, if a SP register at the AA, it will be allocated a unique Service Provider Identity (SPID) as an identity stored at AA. In ABAC systems, a user will be granted access for centain resources based on the related attributes. For the mobile customer, several attributes can be used, such as the *International Mobile Equipment Identity (IMEI), the IP Multimedia Private Identity (IMPI), First Name, Last Name, Email Address, Street, City, State, Country/Region, Postal Code, Home Phone, Date of Birth, Gender, Location and Time.*

In some countries, people have a unique number for their own identity verification. In China, there is an identity card number. In the UK, people have the National Insurance (NI) number. These numbers can be used as a personal identifier for the mobile users. This paper introduces a Unique Identity Number (UIdN) as an important attribute for MLive© security framework. The SPs are registered at the AA and allocated with a SPID. The consumers when registering need to exchange their personal attributes including the UIdN. In our architecture, such sensitive information is stored at AA, and users are able to apply user-defined policies to control the access requests from other entities which are considered un-trusted by the users.

The IdP and the AA has an existing trust relationship. The IdP is a trusted third party. The PEC is the core component of the AA. It will format all the requests as XACML request, evaluate the policies, and perform the access decisions.

The consumer is assumed to access the data and services from the service provider. All transmission of the data and web services are performed over HTTP. The consumer invokes the web service from the SP and needs to register with the IdP first. After registration, the user's details including user name and password will be stored in the IdP and the more sensitive attributes will be stored in AA. In this case, UIdN is the attribute that is stored in the AA.

For a registered consumer, the first step of the schema is to login into the system. Once the IdP receives the request, it will authenticate the user with user name and password method. The consumer will generate a response message and send it to the IdP. If the challenge response is successfully verified, the IdP will generate a local security context for the request. The context contains the information for the consumer, the SP, and the requested sources. After the AA receives the request, it will handle and process the request at three stages.

1. Retrieve the information of the SP, query the AA for the attributes of the SP to check the authenticity of the SP
2. Retrieve the information of the consumer, query the AA for the attributes of the consumer for verification
3. Evaluate the request based on the policies stored in the Policy Repository

Figure 1 shows the main framework. For a registered user, the main message flow will be as illustrated in Figure 2.

For most of the e-business transactions, sometimes the consumers will save their credit/debit card details at the online merchants' web sites as a normal payment in order to save time. However, it is a high risk approach as someone who has the account details of the user could easily carry out an online transaction without any consent.

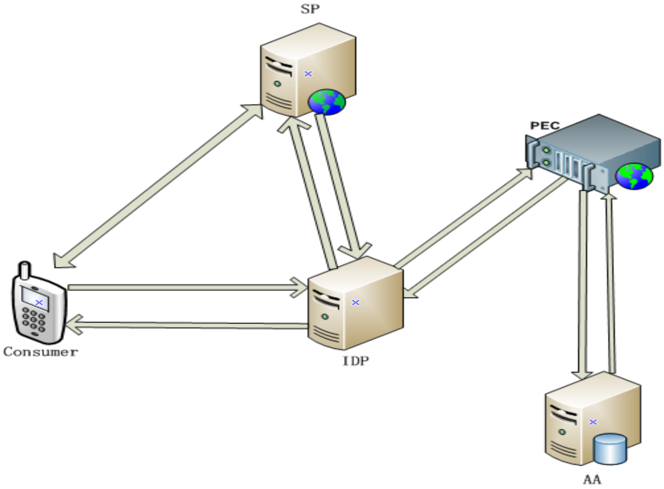

Fig. 1. Proposed Architecture

4 Policy Evaluation

Policy Evaluation Component (PEC) takes charge of XACML policy authentication and authorization. There are 4 main functional components in PEC: the Context Handler (CH), the Policy Enforcement Point (PEP), Validating Point (VP), the Policy Decision Point (PDP), Request Generator (RG), and the Policy Repository.

When a mobile user purchases an item from the SP, he/she needs to request the mobile banking services. Generally, the user is concerned about the authenticity of the SP. At this time, the user needs to check whether it is the real SP that he/she wants to communicate with.

In order to do this, the Validating Point (VP) will compare the attributes of the SP that is received from the IdP and the AA. If the SP is verified, RG will generate a challenge message based on the UIdN received from the AA. PEP will forward the request to the consumer via the IdP. The Consumer’s mobile handset will display this request and the user needs to input the correct UIdN. This step is to insure that it is the actual account holder. A response message is generated and will be sent to the PEC. The PEP forwards the response to the VP, if the validation is successful. The CH will format a XACML request and send it to PDP for the policy evaluation. Since the consumer’s attributes are collected, these can be used for the further policy evaluation. The PDP will make the decision based on the policies in the policy repository. After this, the PDP sends the results to the PEP.

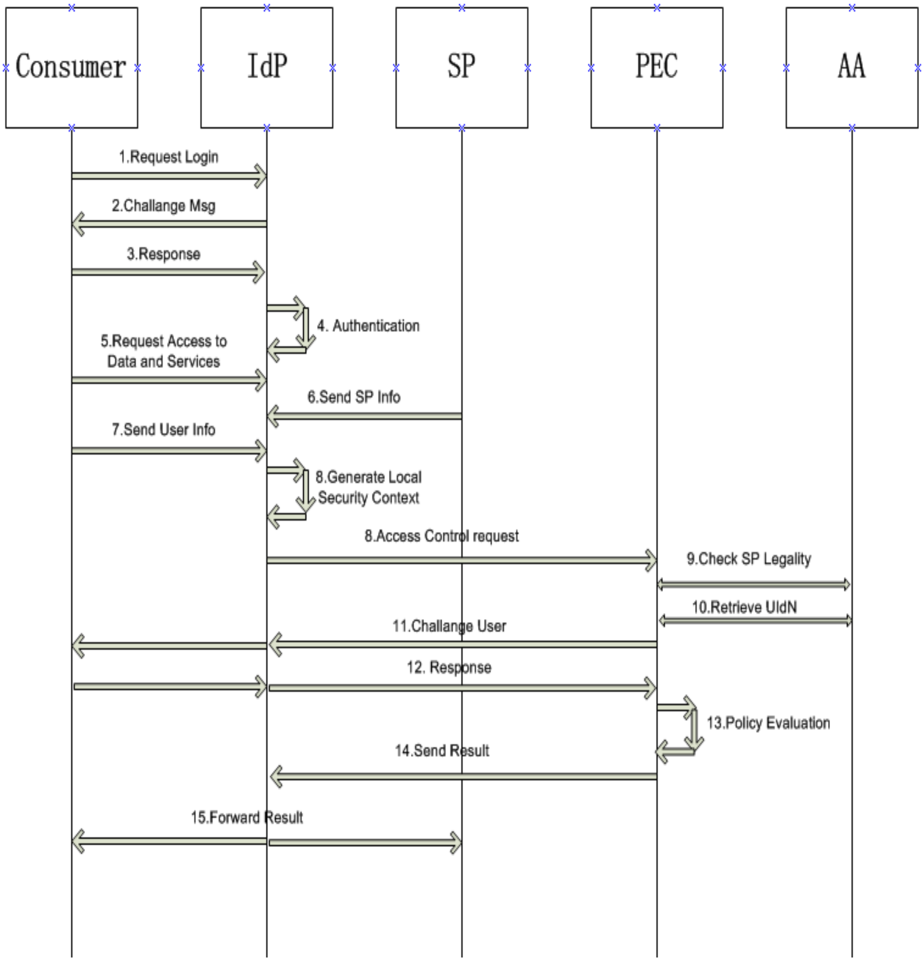

Fig. 2. Main Dataflow of MLive©

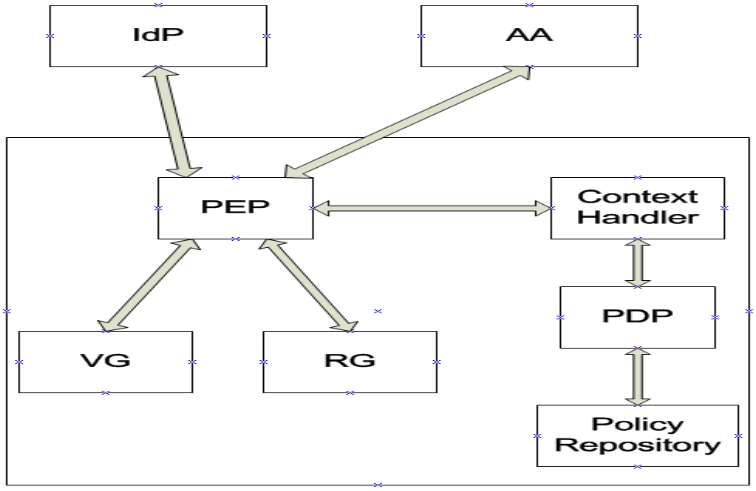

Fig. 3. Policy Evaluation Component (PEC)

5 Conclusion

Attributes based access control, which makes access decisions based on the attributes of requestors, resources, and environment can provide greater flexibility in today's mobile environment. This paper proposed the MLive© framework for access control based on attributes using XACML within a mobile environment domain. XACML defines the security definition and evaluation policies. By using specific attributes that are provided by the mobile users and the service providers in the future, a very secure mobile web services environment can be established and can help to grow the customer confidence and also provide seamless access to their mobile financial services from anywhere, anytime at the touch of a button.

References

1. Facebook Press Room (2010), `http://www.facebook.com/press/info.php?statistics`
2. Ardagna, C.A., De Capitani di Vimercati, S., Paraboschi, S., Pedrini, E., Samarati, P.: Ac XACML-based privacy-centered access control system. In: Proceedings of the First ACM Workshop on Information Security Governance, New York, NY, USA (2009)
3. Oh, S.: New role-based access control in ubiquitous e-business environment. Journal of Intelligent Manufacturing 21(5), 607–612 (2010)
4. Ahmed, A.S., Laud, P.: Formal Security analysis of OpenID with GBA protocol. In: Proceedings of the 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems, Aalborg, Denmark (May 2011)

5. Ahmed, A.S., Laud P.: ProVerif model files for the OpenID with GBA protocol (2011), `http://research.cyber.ee` (last accessed March 30, 2011)
6. Jrstad, I., Johansen, T.A., Bakken, E., Eliasson, C., Fiedler, M., Do van Thanh, M.: Releasing the potential of OpenID & SIM. In: Intelligence in Next Generation Networks. ICIN (October 2009)
7. Srirama, S.N., Jarke, M., Prinz, W.: A Performance Evaluation of Mobile Web Services Security. In: 3rd Internation. Conference on Web Information Systems and Technologies, March 3-6, pp. 386–392. INSTICC Press (2007)