Policy-based Authentication Framework in Ubiquitous Computing Environment

*Ji-In Lee, young bok cho, Sang Ho lee
Dept. of Computer Science, Chung Buk National University
Email : {allure, bogi0118, shlee} @netsec.chungbuk.ac.kr

Abstract: In this paper, we propose policy-based authentication framework which consists of policy server, CA and a policy language designed for ubiquitous environments.Using policies allows the security functionality to be modified without changing the implementation of the entities involved.

Policy- based authentication framework needs to be very expressive but lightweight and easily extensible. We propose the feasibility of our policy language and policy-based authentication framework in ubiquitous-environment through a prototype and solve the problem that traditional framework have a simple registration and authentication to provide dynamic service.

Keywords: Policy, authentication, ubiquitous.

1. Introduction

As computationally enabled devices (laptops, phones, PDAs, and even household appliances) become more commonplace and short range wireless connectivity improves, there is a increased need for more automated security in the resulting pervasive environments formed by mobile users accessing these resources and other services and information using handheld devices. These environments will be populated by a large number of wirelessly networked heterogeneous users, services and semi-automated entities of varied capabilities making it necessary to ensure that all these different entities behave appropriately. Policies guide the behavior of entities within the policy domain and have been used extensively in security, management and even network routing. Policy- based security is often used in systems where flexibility is required as users, services and access rights change frequently. Ubiquitous computing environ-ment require policy-based security authentication fame-work due to their extremely dynamic nature.

In this paper, we propose policy-based authentication framework which consists of policy server, CA and a policy language designed for ubiquitous environments that is based on deontic concepts and grounded in a semantic language. Policy-based authentication framework needs to be very expressive but lightweight and easily extensible. We propose the feasibility of our policy language and policy-based authentication framework in ubiquitous-environment through a prototype and solve the problem that traditional framework have a simple registration and authentication to provide dynamic service. The paper is structured as follows: The discussion about the related work in Section 2 includes the ubiquitous, policy and authentication of mist protocol, authentication protocol. Following this, in Section 3 we propose the prototype of policy-based authentication framework. In Section 4 we present our approach to authentication and discuss the types of delegation policy language. The contribution associated with our prototype are covered in Section 5. Finally in Section 6 we summarize our work and describe future research directions.

2. Related work

In this section, we present some of the existing research that relate to our design. Compared to the amount of research efforts directed towards ubiquitous computing, very little attention has been paid to the security aspects of ubiquitous computing so far. And we will give an outline ubiquitous, policy and describe authentication method.

1) Ubiquitous

In the ubiquitous computing paradigm, information and services are accessible virtually anywhere and at any time via any device - phones, PDAs, laptops or even watches[4, 6]. This has fueled the idea of ubiquitous computing and active information spaces where users can access services, run programs, utilize resources, and harvest computing power anytime and anywhere. This new generation of ubiquitous computing enables the delivery of integrated services and multimedia-enabled applications that are no longer bound by time or location barriers. Ubiquitous computing promotes the proliferation of embedded devices, smart gadgets, sensors and actuators. These devices will be everywhere, performing regular tasks, providing new functionality, extending the reach of traditional computing to physical spaces, and allowing users to interact seamlessly with the surrounding environment. The services will be integrated seamlessly into the environment that the user is familiar with, en-abling easy and automatic usage.

2) Policy

Policies are declarative rules governing choices in a system's behavior. They are increasingly popular in both academia and industry as a means for constraining system behavior. Network and system management tools have relied upon policy-based techniques for several years to add flexibility and adaptability to management infrastructures. Policies are declarative rules governing choices in a system's behavior. They are increasingly popular in both academia and industry as a means for constraining system behavior. Network and system management tools have relied upon policy-based techniques for several years to add flexibility and adaptability to management infrastructures.

3) Authentication

The proliferation of smart gadgets, appliances, mobile devices, PDAs and sensors has enabled the construction of ubiquitous computing environments, transforming regular physical spaces into "Active Information Spaces" services, and the surrounding physical spaces, yielding higher productivity and more seamless interaction between users and computing services. However, the deployment of this computing paradigm in real-life is hindered by poor security, particularly, the lack of proper authentication and access control techniques and privacy preserving protocols. Fig1. describe in active space authentication protocol [3]

1. Active space authentication protocol scenario

step1. Entrances to the Active Space can contain a base station for detecting entering badges
step2. the user moves sufficiently close to one of the available SAPs for authentication purposes. Some authentication devices may require the intervention of the user, e.g. inserting the iButton into its designated receptor.
Step3 : To achieve privacy, the SAP itself does not have sufficient information to authenticate users. However, it has a Lighthouse through which it can communicate with the Security Server. Mist communication is used hereto prevent the Security Server from pinpointing of the authenticated user. Through its Lighthouse, the SAP contacts the Security Server with a set of authentication requests, each representing a different authentication device
Step4 : Upon successful authentication, he AS, like Kerberos, issues a ticket granting ticket (TGT) for that user. Recall that in Mist, every user has a Lighthouse that stores his relevant information.

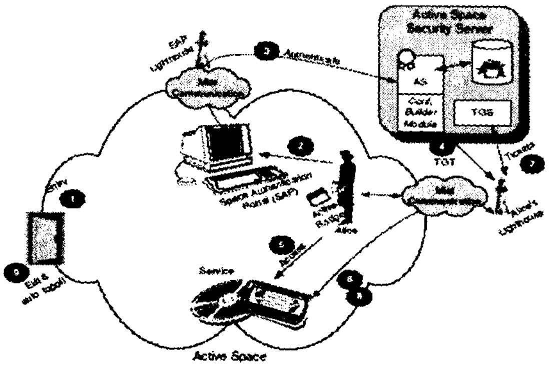

Fig.1 . Active Space Authentication Protocol

Step 5 : users can access services available in the space without the need to use a "fixed" workstation. Instead, they can interact with the services directly using any capable device
Step6 : This communication takes place using the Mist protocol to prevent the Lighthouse from deducing the user's location.
step7 : using the TGT stored at the Lighthouse for the target user, the Lighthouse can communicate with the TGS requesting tickets to access the required service
step8 : Using the information in these tickets along with the net confidence contained within, the service can make a decision whether to authorize the badge holder or not.

3. Policy-based authentication framework

Most traditional authentication methods either do not Scale well in massively distributed environments, with hundreds or thousands of embedded devices like Active Spaces, or they are inconvenient for users roaming around within Ubiquitous computing environments. Moreover, authentication in U- environments cannot use a "one-size-fits-all" approach, as authentication requirements differ greatly among different Active Spaces and different applications and contexts within the same Active Space. In this section, we propose an policy-based authentication framework that provides a flexible and convenient authentication and access control services and security managing, policy service for Ubiquitous computing environment. The framework's flexibility is demonstrated through its ability to support multiple authentication devices and methods, while allowing new authentication technologies to be incorporated dynamically. The framework enables the use of different wearable and embedded devices to authenticate entities with different levels of confidence.

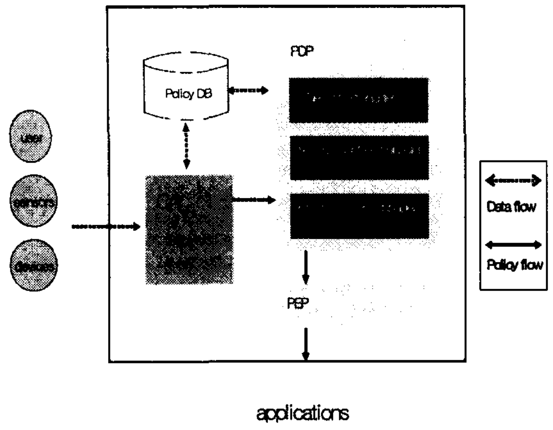

Fig.2 . Policy-based authentication framework

CA : certificate authentication
PDP : policy decision point
- Security manager
- Access control manager
- Policy context manager
PEP : policy enforcement point

We have designed and implemented a security framework, which provides access control to services in Smart-Spaces [1, 2]. This minimizes the resource consumption on the client and also avoids having the services installed on each client that wishes to use them, which is a blessing for most resource-poor mobile clients. Our system consists of six functional components:
(i) Certificate Authentication (ii) Security manager, (iii) Access control manager (iv) Policy context manager, and (v) Policy DB (vi) Policy Enforcement Point

Managers handle communication between various entities in the system. The our framework is flexible and allows any medium to be used for communication. Users and services are treated equally as Clients. The entities in the our system enjoy non-repudiation, authentication, and protection from replay attacks vis-'a-vis the simplified PKI. The Certificate Authentication is responsible for generating x.509 version 3 digital certificates for each entity in the Our system and for responding to certificate validation queries from PDP. PDP is responsible for security and access control, context aware managing. The Security manager provide protection for security. Finally, users and services are treated equally as *Clients*. Our infrastructure is designed to minimize the load on portable devices and provide a media independent infrastructure and communication protocol for the provision of services. In addition to solving the issue of controlling access to services in a *Smart Space*, also accommodates users that are foreign entities, that is entities that are not known to the system in advance. In many conventional systems, access rights are static; agents are not able to request permission to access a Service to which they are not preauthorized. The our architecture allows agents to ask for permission and other agents to actually delegate rights that they have. This extends the security policy in a secure manner, as only agents that have the permission to delegate, can actually delegate.
Figure 2 illustrates the working of the our system. CA on receiving a request for a service asks the PDP whether the request is valid. The PDP replies with a positive or negative response depending on the security policy. Based on this response, the PDP allows or denies the CA request. When a user needs to access a service that it does not have the right to access, it requests another user, who has the right for the permission to access the Service. If the entity requested has the permission to delegate the access to the Service, the entity sends a delegation message to the Security Manager and the requester.

4. Policy language for Ubiquitous computing environment

Security policies in system are written as rules in first order logic. One set of policies is used by the authentication server at the time of logon or authentication. These policies determine the confidence level of authentication. The other set contains access control policies, which determine whether a principal is allowed access to a particular resource.
To illustrate, we present a simplified example of such policies. The various authentication devices are assigned confidence values, using the following rules:

```
- Authenticated(P, PDA)

- requestAct(Sender, Receiver, Action)

- delegateWhen (mark, matthew,right(Action,
 Condition)) ,

- CanAccess (P, ColorPrinter ) :
  (NetConfidenceValue
  (P, V) ϶ V>60%)
```

5. Contribution

Our system is a flexible and dynamic policy-based authentication framework and language that is based on deontic concepts and which can be used to describe several kinds of policies. For example, consider security policies. Security policies restrict access to certain resources in an organization. Our system can be used to create actions on the resources and to describe role based rights and prohibitions for the users in the organization. Conversation policies are very important in semi autonomous environment [5] like ubiquitous computing environments. The order in which speech acts occur is called a conversation. By specifying what speech acts an agent can use under certain conditions (rights), and by specifying what speech acts an agent should use (obligation)under certain conditions (could include the speech acts just received), a policy for conversations can be specified in our system. Other policies can similarly be described in terms of deontic principles making our system.

6. Conclusions

We have presented an authentication framework that builds over policy and introduces new enhancements that allow it to blend nicely into ubiquitous computing environments. The authentication framework enables single sign-on using any devices the user may be carrying or wearing at any time. It allows the decoupling of users from devices and captures some of the dynamism and programmability of Active Spaces by assigning confidence levels to different authentication methods and incorporating context sensitive information. We propose the feasibility of our policy language and policy-based authentication framework in ubiquitous-environment through a prototype and solve the problem that traditional framework have a simple registration and authentication to provide dynamic service.

Our future work will include developing policy language like DAML+OIL and/or OWL ontologies and implement our architecture.

References

[1] J. Undercoffer, F. Perich, A. Cedilnik, L. Kagal, A. Joshi,and T. Finin. A Secure Infrastructure for Service Discovery and Management in Pervasive Computing. *To be published in ACM MONET : The Journal of Special Issues on Mobility of Systems, Users, Data and Computing*, 2003.

[2] L. Kagal, J. Undercoffer, F. Perich, A. Joshi, and T. Finin. A Security Architecture Based on Trust Management for Pervasive Computing Systems. In *Proceedings of Grace Hopper Celebration of Women in Computing 2002*, 2002.

[3] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas, "A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments," presented at International Workshop on Smart Appliances and Wearable Computing (Proceedings of the 22nd International Conference on Distributed Computing Systems Workshops 2002), Vienna, Austria, 2002.

[4] M. Satyanarayanan. Pervasive Computing: Vision and Challenges. *IEEE Communications*, 2001.

[5] L. R. Phillips and H. E. Link. The role of conversation policy in carrying out agent conversations. *Issues in Agent Communication 2000: 132-143*, 2000.

[6]M.Weiser. The Computer for the Twenty-First Century. *Scientific American, pp. 94-10, September 1991*, 1991.