INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 3327 – 3332
RECEIVED : 15.03.2018 PUBLISHED : 19.04.2018

Access Control Establishment Using Geo-Wall

R. Keerthivasan[1], K.S. Srivastavan Iyer[2], Vyshnav A.K[3], M. Vishal[4], G. Karthikeyan[5], A. Shiny[6]

[1*]Computer Science And Engineering, SRMIST, Chennai, India
[2]Computer Science And Engineering, SRMIST, Chennai, India
[3]Computer Science And Engineering, SRMIST, Chennai, India
[4]Computer Science And Engineering, SRMIST, Chennai, India
[5] Computer Science And Engineering, SRMIST, Chennai, India
[6] Assistant Professor, Computer Science And Engineering, SRMIST , Chennai, India

Abstract

Recent enhancements in location technologies, reliability and precision are fostering the development of a new wave of applications that make use of the location information of users. Such applications introduces new aspects of access control which should be addressed. On the one side, precise location information may play an important role and can be used to develop Location-based Access Control (LBAC) systems that integrate traditional access control mechanisms with conditions based on the physical position of users. On the other side, location information of users can be considered sensitive and access control solutions should be developed to protect it against unauthorized accesses and disclosures. In this chapter, we address these two aspects related to the use and protection of location information, discussing existing solutions, open issues, and some research directions.

I. EXISTING SYSTEM

In the last decade, the diffusion and reliability achieved by mobile technologies have revolutionized the way users interact with the external world. Today, most people always carry a mobile device and can stay on- line and connected from everywhere. Location information is then available as a new class of users' information that can be exploited to develop innovative and valuable services (e.g., customer-oriented applications, social networks, and monitoring services). Several commercial and enterprise-oriented location-based services are already available and have gained popularity. These services can be partitioned in different categories. For instance, there are services that provide information on the position of the users or on the environment surrounding the location of a user (e.g., point of interest, traffic alerts), or services which can help in protecting human lives or highly sensitive information/resources. As an example, the enhanced 911 in North America can exploit location information of users to immediately dispatch emergency services (e.g., emergency medical services, police, or firefighters) where they are needed, reducing the margin of error. In an environment offering location-based services (LBSs), users send a request for using such services to a LBS provider. The provider collects the user personal information, possibly interacting with a location server (LS), to decide whether the service can be granted and how it can be possibly personalized. The location server works as the positioning system that measures the locationinformation of users carrying mobile devices, and provides such information at different levels of granularity and with different Quality of Service (QoS). The types of location requests that a Location Server can satisfy depend on the specific mobile technology, the methods applied for measuring users position, and the environmental conditions.

Among the different issues that need to be addressed in the development of location-based services, access control is becoming increasingly important. Access control represents a key aspect to the success of location-based services, and can be radically changed by the availability of location information, which includes position and mobility of the users. In this chapter, access control issues are analyzed from two different perspectives:

1) we analyze how current access control systems can integrate and exploit location information in evaluating and enforcing access requests, thus introducing Location- Based Access Control (LBAC) systems;

2) we analyze how access control mechanisms should change for evaluating and enforcing access to location information, which might be highly sensitive. integrate and exploit location information in evaluating and enforcing access requests, thus introducing Location- Based Access Control (LBAC) systems; 3) we analyze how access control mechanisms should change for evaluating and enforcing access to location information, which might be highlysensitive.

II. EXISTING SYSTEM

Access control systems are based on policies that define authorizations concerning access to data/services. Authorizations establish who can (positive authorizations), or cannot (negative authorizations), execute which actions on which resources [8]. Recent advancements allow the specifications of policies with reference to generic attributes/properties of the parties (e.g., name, citizenship, occupation) and the resources (e.g., owner, creation date) involved [9]. A common assumption is that these properties characterizing users and resources are stored in profiles that define the name and the value of the properties. Users may also support requests for certified data (i.e., credentials), issued and signed by authorities trusted for making statements on the properties, and uncertified data, signed by the owner itself. For instance, an authorization can state that “a user of age greater than 18 and with a valid credit card number (requester) can read (action) a specific set of data (resource)”. When an access request is submitted to the access control system, it is evaluated against the authorizations applicable to it.

II. PROPOSED SYSTEM

The proposed system architecture is composed of three main entities:

i) A location server, that manages positioning systems (e.g., GPS, cellular technologies) and answers to requests for location information

ii) Several validators, that are responsible for evaluating the requests and determining whether the location informa- tion can be released, based on preferences of the users

iii) Client applica- tions, that submit requests for location information. The authors assume trust relationships between users, validators, and location servers. Users are registered with at least one location server and store their require- ments within it. These requirements are implemented by the validators. When a client application needs to access the location of a user, it first selects the relevant location server, and then submits the request.

.

III. LOCATION BASED ACCESS CONTROL

The diffusion and reliability reached by mobile technologies provide a means to use location information for improving access control systems in a novel way. Although, research on LBAC is a recent topic, the notion of LBAC is in itself not new. Some early mobile networking protocols already relied on linking the physical position of a terminal device with its capability of accessing network resources . Extensive adoption of wireless local networks has triggered new interests in this topic. Some studies focused on location-based information for monitoring users movements on Wireless Lan and 802.11 Networks . Myllymaki and Edlund describe a methodology for aggregating location data from multiple sources to improve location tracking features. Other researchers have investigated a line closer to LBAC by describing the architecture and operation of an access server module for access control in wireless local networks[1].

Controlling access to wireless networks, complying with IEEE 802.11 family protocols, is principally aimed at strengthening the well-known security weaknesses of wireless network protocol rather than at defining a general, protocol-independent model for LBAC.

The need for a protocol-independent location technique has been high- lighted by a study exploiting heterogeneous positioning sources like GPS, Bluetooth, and WaveLAN for designing location-aware applications. Cho et al. present a location-based protocol (Location-Based network Access Control) for authentication and authorization, in infrastructure- based WLAN systems based on IEEE 802.11. The protocol is used to securely authenticate the location claims released by wireless users, and exchange the keys shared for data encryption. The infrastructure is com- posed of three parties: the key server responsible for authentication, location claim verification, and key distribution, the access points, and the mobile stations. The solution is based on the fact that a mobile station is in a given location if and only if it receives all the relevant information from the corresponding access points. The protocol uses a Diffie-Helmann algorithm to authenticate location claims, authorize network access, and generate the shared keys for communications between mobile stations and access points. Location- based information and its management have been also the subject of a study by Varshney

[1] in the area of mobile commerce applications. This is a related research area that has strong connection with location systems and is a promising source of requirements for LBAC models.

IV. MODULE DESCRIPTION

An Access Control System for LBAC Policies Ardagnaetal. define a LBAC system that supports location-based policies. Intuitively, a location- based policy exploits the physical location of users to define when they can access a service or a resource. The authors identify three main steps towards the development of a LBAC system: i) the design of a reference LBAC architecture that can support the evaluation and enforcement of location- based policies; ii) the definition of location-based conditions; and iii) the definition of a mechanism for the evaluation and enforcement of location- based conditions.

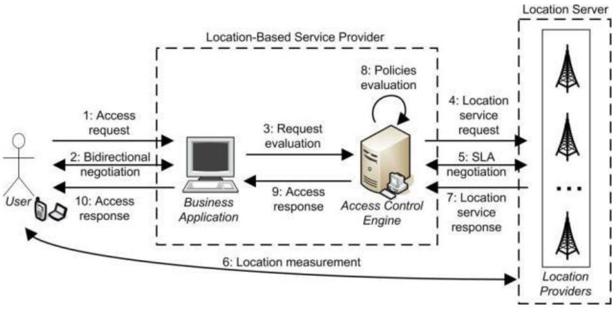

Fig. 1. *LBAC architecture*

LBAC definition changes the conventional access control architecture, since there are more parties involved. Figure 1 presents a LBAC architecture that involves four logical components.

User: The entity whose access request to a location server must be authorized by a LBAC system. Users carry terminals enabling authentication and some form of location verification.

Business application: Customer-oriented application that offers services whose release is regulated by location-based policies.

Access Control Engine (ACE). The entity that is responsible for evaluating access requests according to some location-based policies. The ACE communicates with one or more Location Providers for acquiring location information. The ACE does not have direct access to the location information; rather, it sends requests to external services and waits for the corresponding answers.

Location Providers (LPs). The trusted entities that provide the location information (e.g., context data about location and timing, location-based predicate evaluation) by implementing Location Server interfaces.

Interactions among the User, the Business Application, the Access Control Engine, and the Location Providers are carried out via re- quest/response messages . The process is initiated by a user that submits an access request to a Business Application . A negotiation process between the two parties is then used to exchange those data that are relevant to the policy evaluation . The request is further forwarded to the ACE that interacts (if needed) with the Location Providers , evaluates policies , and returns an access decision. Communications between the ACE and the Location Providers may be driven by a service level agreement (SLA) negotiation phase. This negotiation is used to agree upon and set quality of services attributes and the corresponding service cost.

V. FUTURE SCOPE

We briefly describe some open issues that need to be taken into consideration in the future development of access control systems for location-based services. Reliable enforcement based on fine-grained context information. As discussed, a key aspect to the success of location-based access control systems is the definition of a reliable enforcement solution, able to verify information which is approximate and time-variant. In the near future, location servers will provide a wealth of additional environment- related knowledge (e.g., is the user sitting at her desk or walking to- ward the door? Is she alone or together with others?), that may give the opportunity of defining and evaluating new classes of location- based conditions in the context of LBAC systems. LBAC systems however may be flawed by the intrinsic errors of location measure- ments, in calculating such fine-grained knowledge. Future access con- trol mechanisms should then try to enhance current approaches to the management of uncertain information, thus providing policy evalua- tion mechanisms able to support fine-grained location information.

Privacy-aware LBAC. An important aspect to consider in today access control systems is the protection of the user privacy. Some solutions have been presented in the past (e.g., [9]) which provide, on the one side, access control functionality and, on the other side, privacy pro- tection. However, LBAC systems introduce new threats that should be carefully considered. In particular, a fundamental issue to be ad- dressed considers the conflicting requirements of preserving users privacy and of providing high quality LBAC. A suitable protocol should in fact balance the tradeoff between the level of location accuracy requested by LBAC providers and the protection of the location in- formation requested by the users. A possible approach in develop- ing a privacy-aware LBAC may integrate access control with location privacy solutions (e.g., obfuscation and anonymity techniques).

Integration of different location sources. An important issue in the development of LBAC systems is represented by the availability of several location servers, which support different positioning systems for measuring location of the users.

In this context, a solution which implements communication and negotiation protocols between the LBAC system and multiple, functionally equivalent, location servers is needed. These protocols should provide an approach based on service level agreement attributes which maximize the QoS and/or cost/benefit functions.

REFERENCES

[1] Varshney, U.: Location management for mobile commerce applications in wireless internet environment. ACM Transactions on Internet Technology (TOIT) 3(3) (December 2003) 236–255

[2] Ardagna, C., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Privacy-enhanced location services information. In Acquisti, De Capitani di Vimercati, Gritzalis, Lambrinoudakis, eds.: Digital Privacy: Theory, Technologies and Practices. Auerbach Publications (2007)

[3] Enhanced 911: http://www.fcc.gov/911/enhanced/.

[4] Chicago Tribune: Rental firm uses GPS in speeding fine. July 2nd, p.9. Associated Press: Chicago, IL, 2001.

[5] Duckham, M., Kulik, L.: Location privacy and location- aware computing. In Drummond, J., Billen, R., Forrest, D., Joao, D., eds.: Dynamic & Mobile GIS: Investigating Change in Space and Time. CRC Press (2006) 34–51

[6] Ardagna, C., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Location privacy protection through obfuscation-based techniques. In: Proc. of the 21st Annual IFIP WG

11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, USA (July 2007)

[7] Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: Proc. of the 3rd International Conference on Pervasive Computing (PERVASIVE 2005), Munich, Germany (May 2005)

[8] Samarati, P., De Capitani di Vimercati, S.: Access control: Policies, models, and mechanisms. In Focardi, R., Gorrieri, R., eds.: Foundations of Security Analysis and Design. LNCS 2171. Springer-Verlag (2001)

[9] Ardagna, C., Cremonini, M., De Capitani di Vimercati, S., Samarati, P.: A privacy- aware access control system. Journal of Computer Security 16(4) (2008) 369–39