PRIVACY ENHANCED ARCHITECTURE FOR LOCATION BASED SERVICES IN THE NEXT GENERATION WIRELESS NETWORK

Alberto Escudero-Pascual
IMIT, Royal Institute of Technology
Isafjorsgatan 39, Stockholm, Sweden, aep@kth.se

Abstract - Location-based services (LBS) can be described as applications that exploit knowledge about where an information device (user) is located. For example, location information can be used to provide automobile drivers with optimal routes to a geographical destination or a group of friends with the names and coordinates of Spanish's restaurants in the neighborhood open on a Saturday night.

We propose a privacy enhanced location based service (PE-LBS) architecture which allows a mobile node to request location based services via a proxy server hiding the network location of the mobile device while providing service accountability.

The architecture is composed of six modules: location acquisition hardware, XML data record parser [1], XML service request, transport module, LBS proxy and service modules. Privacy Enhanced Technologies has been carefully integrated to enhance the privacy of our architecture by protection of personal identifiable information.

One of the components of our architecture is the LBS Proxy Server, responsible of processing SOAP [2] (message envelope) requests and generate responses. When the SOAP request is recieved by a server, it gets bound to the class specified in the request. The proxy server works as a SOAP Dispatcher, by determining which class should handle a given request, and loading that class, if necessary. The SOAP server acts as an intermediary between a SOAP client and the requested service provider.

Keywords - privacy, location based services, privacy enhanced technologies.

I. Location Based Services Architecture

The proposed privacy enhanced location based service (PE-LBS) architecture is composed of six functional modules as follows:

A. Location Acquisition Hardware

The location acquisition hardware is responsible for calculating the position of the mobile device based on a set of data inputs that can vary from GPS radio signals or infrared beacons to an enhanced tape measure. The output is a set of coordinates based on a reference system. For example, most GPS receivers use a global reference system named WGS 84 (World Geodetic System 1984).

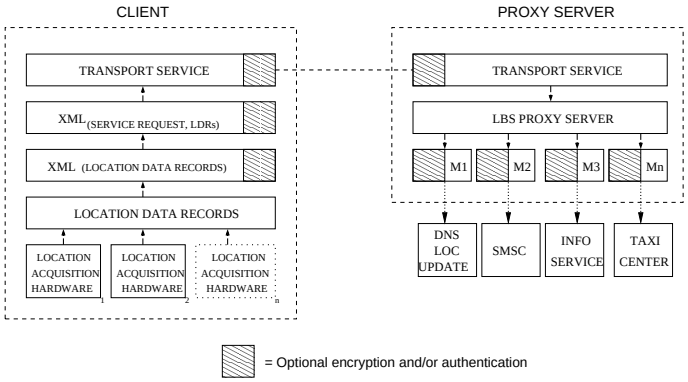

Fig. 1. PE-LBS Architecture

Location information records obtained from the hardware can include: latitude, longitude, altitude, velocity, horizontal error, vertical error, global error, orientation, etc.

B. XML Location Data Record

The format of the location records provided by the hardware or multiple pieces of hardware can be of very different nature. The XML Location Data Record module is responsible for creating XML output based on location information provided by the location acquisition hardware.

C. XML Service Request

The XML service request module will take the location information from the XML location data record and build a service request. In our architecture the service request uses Simple Object Access Protocol (SOAP) [2] to encapsulate and exchange RPC calls using the extensibility and flexibility of XML. SOAP can potentially be used in combination with a variety of other protocols; however, the most common use of SOAP is in combination with HTTP, the experimental HTTP Extension Framework, or SNMP.

D. Transport Service

This module implements the equivalent of OSI layer 4 by providing reliable transparent data transfer between end points, along with error recovery, and flow control. It is responsible for the transport of the remote procedure call to the location based service proxy server.

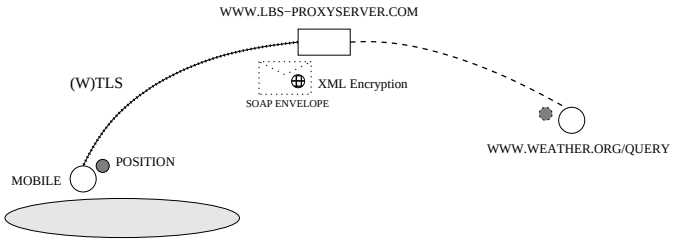

Fig. 2. SOAP Request via PE-LBS proxy

E. Location Based Service Proxy Server

The functionality of the LBS Proxy Server is to process SOAP (message envelope) requests and generate responses. When the SOAP request is recieved by a server, it gets bound to the class specified in the request. The proxy server works as a *SOAP Dispatcher*, by determining which class should handle a given request, and loading that class, if necessary. The SOAP server acts as an intermediary between a SOAP client and the requested service provider.

F. Service Modules

A service module acts as a SOAP interface, a frontend that requests information or the execution of a procedure, parses and formats the response and returns it according to the request (if necessary). The procedure can run in the same server (e.g. return a prime number of *n* bits) or be the result of a call in a remote server (e.g. send an e-mail message to a certain address).

Let us consider the scenario where a mobile device with a unique identifier *mobileID* requests the temperature information for a certain position and time. In this case, the SOAP server (LBS-proxy) works as a proxy of the SOAP client (mobile device) and the temperature service provider. In fact, the proxy can conceal from the temperature server the mobile device's *mobileID* and protect its identity as this information is not required to obtain the requested service. But, must the proxy know about the location of the mobile device to proxy the temperature request service? No, we can hide the position information from the proxy and still get the temperature in that position. To do this we use a privacy enhanced proxy.

II. MIXES AND PE-LBS PROXIES

David Chaum described in [3] a technique based on public key cryptography that allows an electronic mail system to hide who a participant communicates with as well as the content of the communication.

More generaly, messages are exchanged through a chain of one or more intermediaries called "mixes". The purpose of a mix is to hide the correspondences between the items in its input and those in its output. The main function of a mix is to: receive and decrypt messages, buffer messages until a defined number of messages has been received, change the sequence of the received messages in a random manner and encrypt and forward the messages to the next mix or to the receiver.

Three of the benefits of our arquitecture are: the possibility of a PE-LBS proxy to act as a "mix" by buffering and changing the sequence of the service requests, a mobile device can use a chain of PE-LBS proxies configured as a "mixing network" to forward a location based service requests and that these functionalities can be done independently of the specific transport network.

III. A PROOF OF CONCEPT

A proof of concept was implemented using Fastrax's iTrax02 GPS receiver. The iTrax02 is an ultra-low power consumption receiver, roughly the size of a stamp and specifically designed for small portable devices. In one of the scenarios, the location information is encrypted using a public key encryption scheme (with multiple private keys), embedded in a XML message and transmited to a proxy that runs a secure DNS update module [5]. This location privacy solution allows a mobile terminal to publish its location as an encrypted DNS location record via the proxy, while concealing from eavesdroppers and third parties the relation between the location information and the identity of the mobile terminal and its user.

IV. CONCLUSIONS

By using a proxy server between the mobile node and the location based service we have shown that we can hide the network location of the mobile device and in some cases even provide misleading physical location(s) for the mobile device [4].

Combining XML Encryption with XML Signature in Simple Object Access Protocol service requests provide both message digest and message authentication functionality. Taking advantage of the extensibility and flexibility of XML it is easy to implement and extend the set of privacy enhanced location based services while still hiding the mobile node's network and physical location as desired[1].

V. REFERENCES

[1] W3C "XML Encryption Syntax and Processing", Working Draft, 18 October 2001.

[2] W3C "Simple Object Access Protocol (SOAP) 1.1", Technical Report. May 2000.

[3] D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms". Communications of the ACM (24)2, 1981 pp. 84-88

[4] A. Escudero. "Privacy and Identity in the Information Society - Protection of personal identifiable information in mobile internet". IPSC-IPTS (EU). Brussels. October 2001.

[5] C. Davis, et al. "RFC 1876: A Means for Expressing Location Information in the Domain Name System", January 1996.

- - -

[1] This work would not be possible without the support and advice of Gerald Q. Maguire Jr.