# Implementation of a Location Based Remote Client Authentication Protocol for Book Store

Dr. Vaibhav Jain
Physics Department, DAV (PG) College, Bulandshahr, UP, India.

*Mobile networks are driven by the need to provide more advanced services to mobile or nomadic computing devices, such as security services requiring remote client authentication. In such services, the user's location might be used as authentication factor, in addition to the typical authentication factors, like passwords, or one time tokens combined with the use of a physical device that a person owns, such as a card or a phone. To implement location based remote protocol which provides Secure Payment System from remote location and make the successful transaction from user account to Clients as well as authenticate user and location since the location information itself is subject to forging attacks, additional mechanisms must be used to certify its integrity. We implemented location based remote authentication protocol, a new protocol combining several authentication factors to securely authenticate a mobile user. In this protocol, the user's location can be determined and its correctness is certified by a third trusted party, called Local Element. As use case, we considered the payment service at the book stores, and we proposed a location-based service exploiting one time codes and certified position for secure payment operations.*

**Keywords:** Authentication, Global Positioning System (GPS), Spoofing.

## 1. INTRODUCTION

There is a need for stronger authentication methods, especially in 'remote" usage scenarios. The term "remote" is used here to refer to any infrastructure in which the clients and the service providers are connected via some potential insecure network, like the mobile network. With the appearance and advance of location sensing and social networking technologies, newer authentication classes, such as *where the user is, and when* or *somebody you know*, might be used in combination with the classical authentication factors. Determining and proving that a user is at a certain location is itself a challenging task as no single location sensing technology has emerged as a clear winner in all kinds of environments.

LBRAP, a secure location-based remote authentication protocol which can be used to authenticate the remote users in mobile environments. LBRAP is based on the use of "classical" authentication methods (like the static passwords and the one time passwords) combined with user location information at one time.

To verify the integrity of the location data, LBRAP exploits a dedicated component, named Local Element (LE), which is part of the European Galileo navigation satellite system. As a proof of concept, we designed and implemented an LBRAP-based service involving payment with the mobile devices at book stores.

## 2. RELATED WORK

*Location as authentication factor* : Two-factor authentication is considered not adequate for security problems encountered today, like phishing or identity theft [5]. Historically, biometric identification (such as fingerprints) have been used as the most authoritative method of authentication, but this technology cannot be always deployed on wide scale and requires collection and secure storage of such data.

To cope with the new attacks in banking services, new, cost-effective technology tools should be used in every bank's online security arsenal to protect their customers against security frauds [1]. Geolocation techology determining the true geographic position may prove beneficial in a multifactor authentication strategy, as noted also in the guidance document on the authentication in Internet banking environment [2]. The geo-location information has been used in the past in several location-based services, such as emergency and information services [3], tracking and monitoring systems [4], or even for establishing pairwise keys in the sensor networks [5]. In the security area, some location-authentication schemes have been proposed [6], but the location authentication is still considered a novel security service [7], mainly because the location data itself needs to be authenticated or certified by a trusted third party in order to be considered reliable.

*Location authentication problem and some solutions* : To obtain the location information, one possible and simple solution is to use the U.S. space-based GPS system. For anyone with a GPS receiver, the system provides accurate location and time information in all weather, day and night, anywhere in the world. However, from the security point of view, the authenticity of the GPS signal is not guaranteed because a false (or spoofed) GPS signal could be generated by a dedicated GPS signal simulator, and a typical GPS receiver would not be able to detect that. Some "advanced" GPS receivers are enhanced with antispoofing modules in order to detect whether the GPS signal comes from the satellite or from a fake GPS simulator. However, in the recent years, more and more advanced GPS simulators have become also readily available and can be hired relatively cheaply, thus it is not possible to guarantee that a GPS signal really comes from the "right" source or not.

To cope with the GPS signal authentication problem, Den-ning & Doran proposed a "location signature sensor" (LSS) tamper-proof device [6] whose role is to create (and verify) a location signature (LS) containing geodetic position and valid for a short time, e.g. for 5 ms. Thus, an LS acts more or less like an unpredictable one time password. Nevertheless, M.G. Kuhn notes some critical points of the LSS-based solution [8], such as "This system only provides symmetric authentication and anyone able to verify the output of a LSS in a geographical region will also be able to fake the output of such a sensor from anywhere within the same region". Other solutions [9] propose to exploit the location-positioning capabilities of a wireless network to check out the location information. Other solutions [7] proposed to guarantee the authenticity of location information against the most common location-related attacks are shortly presented.

*Galileo Local Elements*: The European Galileo programme aims to provide users with another satellite system (i.e. Galileo), independent but interoperable with the US GPS system. Galileo will be the first satellite navigation system specifically for civil purposes, generating new opportunities of market and pushing the advance in technology for Europe.

The Local Element (LE) is an important element of the ground infrastructure of Galileo, and is in charge with certifying the position and time information. LE will deliver enhanced performance in terms of accuracy, integrity, availability and continuity by combining Galileo/GPS satellite-only services with information coming from external sources. In particular, the LE developed in the GAL-PMI project [10] provides augmentation and certification features using data acquired from Global Navigation Satellite System (GNSS) and Telecom Italia (GSM) cellular networks. Further details on LE design and implementation are given [11].

*One Time Codes*: In remote client authentication based on one-time codes, both the prover (the entity whose identity is verified) and the verifier share a secret: the prover presents the secret to the server as is, that is the shared secret is the One Time Code (OTC), or in a derived form, e.g. as generated with the RSA Secure ID authenticator [12]. Typically, the OTC has a limited validity lifetime (e.g. 60 s) because time itself is used at the OTC generation, and the prover can use an OTC to authenticate to the verifier only once.

The OTC can be either generated independently by the user, or it can be generated by the verifier and sent to the user (provided that the user established a relationship with the verifier). The latter method is used by several banks to offer advanced services, such as mobile banking [13] or fund transfers to non-registered third party accounts. In some security products, like in the Clavister SMS One-Time Password service [14], the OTC is generated by a Gateway controlling the access to the network resources, applications and files of a corporate network, and is distributed to the user's mobile phone as a flash SMS. Subsequently, the clients can get access to the protected resources by using any standard Web browser and the OTC received via SMS. We used a somehow similar approach in our protocol, as described in Section 4.

## 3. EXISTING SYSTEM

No single authentication method can fully protect against all types of security attacks. For example, the challenge-response one-time codes or the application-level PKI-based authentication render phishing and malicious software attacks useless, but they do not protect against man-in-the-middle attacks, even though both methods could be extended to achieve this protection too [15]. Thus, there is a need for stronger authentication methods, especially in 'remote" usage scenarios. The term "remote" is used here to refer to any infrastructure in which the clients and the service providers are connected via some potential insecure network, like the mobile network. With the appearance and advance of location sensing and social networking technologies, newer authentication classes, such as *where the user is, and when* [13] or *somebody you know* [14], might be used in combination with the classical authentication factors [13,15]. The Global Positioning System (GPS) is the de facto location technology for wide outdoor area, but it does not work in covered areas or indoors and it can be easily spoofed (see Section 2).

## 4. LOCATION-BASED REMOTE AUTHENTICATION

### 4.1. PROTOCOL

The protocol is composed of two phases: a registration phase and an operational phase. In LBRAP, the SP (acting as verifier) generates an OTC encrypted with a key derived from UT location (called TOKEN) and sends it to the UT to be used for authentication, provided that the user has registered first with the SP as shown in Figure 1.

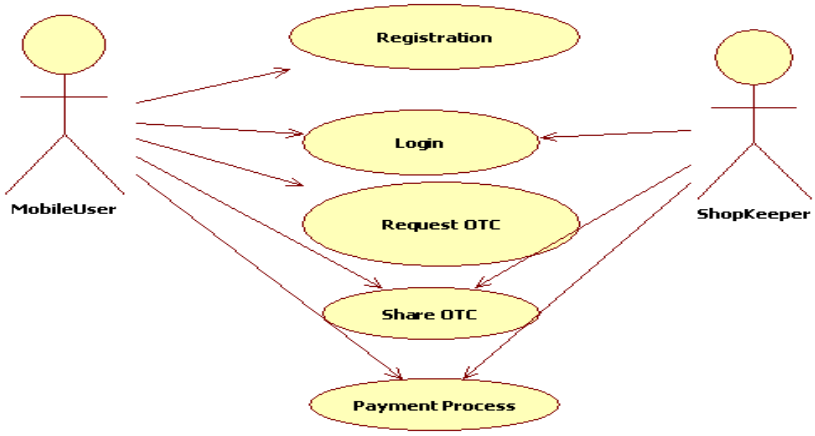


**Fig 1.** USE-CASE Diagram.

In the registration phase, the client provides several data to the SP, such as: (1) Person identification data, like name, surname, birthplace, fiscal code; (2) UT identification data, such as the phone number and the IMEI (International Mobile Equipment Identity) code uniquely identifying the UT device in the cellular network; (3) Authentication data, that is data required by the authenticated key agreement protocol; (4) Other data, such as a bank account number (if a payment operation need to be performed in the service), or service subscription type (silver, gold).

LBRAP is based on three factors:

(a) Where a person is.

(b) When - that is the location of the user associated with the time information, something the user has - such as a GPS and GSM/UMTS aware terminal.

(c) Something the user knows, that is a static PIN (Personal Identity Number) used to access the device and an OTC. LBRAP architecture involves several factors, i.e. the user and the User Terminal (UT), the Service Provider (SP) and the Galileo LE.

## 5. LBRAP-BASED PAYMENT SERVICE AT BOOK STORE

This section describes the design and implementation of a LBRAP-based payment service at book stores. It is having 3 modules.

### 5.1. Mobile User module

This module is an implementation of end user application for using the shopping services in secured way using the LBRAP protocol.

### 5.2. Service Provider

This is a third party server for providing the service in secured way by providing the encrypted OTC to the mobile user for doing the online shopping. This module uses the LBRAP protocol for generating the OTC and encryption of OTC.

### 5.3. Book Store module

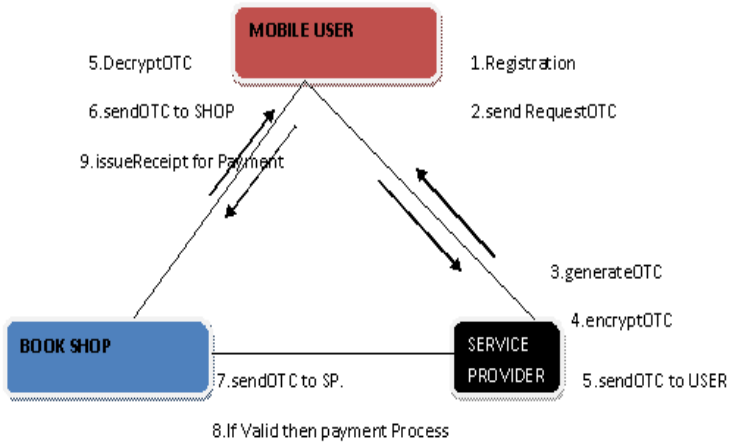


**Fig. 2:** Collaboration diagram.

## 6. CONCLUSIONS

The LBRAP protocol exploited both traditional and contextual (i.e. location) authentication factors for client authentication in mobile environments. Furthermore, we designed and implemented a proof of concept for the LBRAP protocol, in the form of a real case scenario allowing user to perform payments at the Book stores. Future work is to improve privacy issues, tamper resistant security module.

## 6. REFERENCES

[1] M. Alexander; “Keeping Online Banking Safe: Why Banks Need Geolocation and Other New Techniques Right Now”. http://www.bankersonline.com/security/ safebanking.html, May 2005.

[2] Federal Financial Institutions Examination Council; “Authentication in Internet Banking Environment”, http://www.ffiec.gov/press/pr101205.htm, Oct. 2005.

[3] E. Toye, R. Sharp, A. Madhayapeddy and D. Scott; “Using Smart Phones to Access Site-Specific Services”, IEEE Pervasive Computing, Springer-Verlag, Vol. 4(2), pp. 60-66, 2005.

[4] M. Gruteser and X. Liu; “Protecting Privacy in Continuous Location-Tracking Applications”, IEEE Security & Privacy Magazine, Vol. 2(2), pp. 28–34, 2004.

[5] D. Liu and P. Ning; “Location-based pairwise key establishments for static sensor networks”, Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, Fairfax, Virginia, pp. 72-82, 2003.

[6] D.E. Denning and P.F. MacDoran; “Location-based authentication: grounding cyberspace for better security”, Computer Fraud & Security, pp. 12-16, Feb. 1996.

[7] A.I. Gonz´alez-Tablas Ferreres, B. Ramos Alvarez and A.R. Garnacho; “Guaranteeing the Authenticity of Location Information”, IEEE Pervasive Computing, Vol. 7(3), pp. 72-80, July-Sept. 2008.

[8] M.G. Kuhn; “An Asymmetric Security Mechanism for Navigation Signals”, Proc. of the 6th Information Hiding Workshop, pp. 239-252, 2004.

[9] R.A. Malaney; “A location enabled wireless security system”, Proc. of IEEE GLOBECOM, pp. 2196-2200, 2004.

[10] M. Spelat and F. Margary, “GAL-PMI Project: Global Navigation Satellite Systems to Support Mobility and Security”, Proc. of Space Applications Days 2008, Toulouse (France), pp. 608-612, 22-25 April 2008.

[11] J. Ringert, E. Wasle, J. Hanley and S. Scarda; “Bringing Galileo into LBS Market – the Agile Project”, Proc. of IEEE 17th Int. Symp. on Personal, Indoor and Mobile Radio Communications, pp. 1-5, 11-14 Sept. 2006.

[12] T. Weigold, T. Kramp and M. Baentsch; “Remote Client Authentication”, IEEE Security and Privacy, Vol. 6(4), pp. 36-43, 2008.

[13] R.J. Hulsebosch, M.S. Bargh, G. Lenzini, P.W.G Ebben and S.M. Iacob; “Context Sensitive Adaptive Authentication”, Smart Sensing and Context, Vol. 4793, pp. 93-109, 2007.

[14] J. Brainard, A. Juels, R.L. Rivest, M. Szydlo and M. Yung; “Fourth Factor Authentication: Somebody You Know”, Proc. of ACM CCS 2006, pp. 168-178, 2006.

[15] H. Zheng, J. Kwak, K. Son, W. Lee, S. Kim and D. Won; “Confidence Value Based Multi Levels of Authentication for Ubiquitous Computing Environments”, Proc. of ICCSA 2006, LNCS 3981, pp. 954-963, 2006.