Indian Journal of Communications Technology and Electronics (IJCTE)
Vol.2.No.1 2014pp 40-44
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

ENHANCING SECURITY AND PRIVACY FOR CREDIT CARDS VIA LOCATION SENSING

PREETHI. B, LATHA RAJESH
Dept.ofCSE
VELS University
Pallavaram, Chennai
preethimam@gmail.com, lathasrec@gmail.com

ABSTRACT

In Mobile networks the user's location, passwords might be used as authentication factor to provide security services for remote client authentication. In addition there are many typical authentication factors. In Location based Remote client Authentication Protocol for mobile environment (LRAP), combines several authentication factors to securely authenticate a mobile user. In LRAP, the user's location can be determined by a third party used by user's mobile for secure payment operations. This paper is to investigate a systematic approach to generate an encrypted data to real user mobile number along with decrypting key as SMS only when the location of credit card matches with the location of user's mobile in order to avoid unauthorized access of credit card.

Keywords— Encryption, Decryption, Local Element, Service Provider

1. INTRODUCTION

Authentication is considered as the most important security service staying at the basis of many products and application services now a day. To perform authentication, various methods with a variable degree of reliability are typically employed. These methods are classified into three main classes or factors:

What the user is (e.g. a fingerprint, retinal, voice recognition pattern or other biometric data)
What the user has (e.g. an ID card, security token, mobile device or cell phone)
What the user knows (e.g. a static passwords or a one-time code).

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. Thus, there is a need for stronger authentication methods, especially in 'remote" usage scenarios. 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. 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. In LRAP, a secure location-based remote authentication protocol which can be used to authenticate the remote users in mobile environments. LRAP 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, LRAP exploits a dedicated component, named Local Element (LE). They implemented an LRAP-based service involving payment with the mobile devices at the gas stations. We proposed to design and implement the identification of Credit card forgery by the location based tracking using the mobile with GPS. In this System the encryption and decryption key will be generated for authentication purpose.

1.1 Related Work

Location as an authentication factor. Two-factor authentication is considered not adequate for security problems encountered today, like phishing or identity theft [5].. In the security area, some location-

authentication schemes have been proposed [11], Network-Based Processing considered a novel security service [12], mainly because the location data itself needs to be authenticated or certified by a trusted third party in order to be considered reliable. 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, However, fromthe 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. [14], propose to exploit the location-positioning capabilities of a wireless network to check out the location information. 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. Further details on LE design and implementation are given in [16]. 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. Typically, the OTC has a limited validity lifetime (e.g. 60 s) because time itself is used at the OTC generation. In some security products, like in the Clavister SMS One-Time Password service 3, the OTC is generatedby 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. In [1] LRAP the verification scheme is implemented by comparing the User's credit card location with the User's mobile location.

2. PRELIMINARIES

This section reviews the definitions of Encryption, Decryption, GPS tracking and Service Provider.

2.1 Encryption

Encryption is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people. In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that does the work of the encryption algorithm.

2.2 Types of Encryption algorithms

1. Symmetric Encryption Algorithm
2. Asymmetric Encryption Algorithm

2.2.1 Symmetric Encryption Algorithm

When the same secret, password or key is used to encrypt and to decrypt then it is said to be symmetric encrypting key algorithm.

2.2.2Asymmetric Encryption Algorithm

This type of algorithm uses a different key for decryption and encryption and has some functional advantages over symmetric encryption which if fast, and can be secured by on-the-fly key generation and frequent key changes. Asymmetric encryption on the other hand employs a different key for decryption and encryptions by so called public key encryption in which anyone can get the public key of the recipient to encrypt files or messages so that only the holder of the private key of the public-private key pair can open the item.

2.3 Decryption

Decryption is the process of converting encrypted data back into its original form, so that it can be understood by the user.

2.4 GPS tracking

A GPS tracking unit is a device that uses the Global Positioning System to determine the precise location of a vehicle, person, or other asset to which it is attached and to record the position of the asset at regular intervals. The recorded location data can be stored within the tracking unit, or it may be transmitted to a central location data base, orinternet-connected computer, using a cellular(GPRS or SMS), radio, or satellite modem embedded in the unit. This allows the asset's location to be displayed against a map backdrop either in real time or when analyzing the track later, using GPS tracking software.

2.5 Mobile Tracking via GPS

Mobile phone tracking refers to the attaining of the current position of a mobile phone, stationary or moving. Localization may occur either via multilateration of radio signals between (several) radio towers of the network and the phone, or simply via GPS. Mobile positioning, which includes location based service that discloses the actual coordinates of a mobile phone bearer, is a technology used telecommunication companies to approximate where a mobile phone, and thereby also its user (bearer), temporarily resides. The more properly applied term locating refers to the purposerather than a positioning process. Such service is offered as an option of the class of location-based services

2.5.1 Hybrid Systems

Hybrid positioning systems use a combination of network-based and handset-based technologies for location determination. One example would be some modes of Assisted GPS, which can both use GPS and network information to compute the location. Both types of data are thus used by the telephone to make the location more accurate (i.e. A-GPS). Alternatively tracking with both systems can also occur by having the phone attain his GPS- location directly from the satellites, and then having the information sent via the network to the person that is trying to locate the telephone.

The technology of locating is based on measuring power levels and antenna patterns and uses the concept that a mobile phone always communicates wirelessly with one of the closest base stations, so knowledge of the location of the base station implies the cell phone is nearby.

2.6 Service provider

Service provider (SP) offers merchants online services for accepting electronic payments by a variety of payment methods including credit card and bank-based payments. Some SPs provide unique services to process other next generation methods (Payment systems) including cash payments, wallets such as PayPal, Web Money and prepaid cards.

Typically, a SP can connect to multiple acquiring banks, card, and payment networks. In many cases, the SP will fully manage these technical connections, relationships with the external network, and bank accounts. This makes the merchant less dependent on financial institutions and free from the task of establishing these connections directly - especially when operating internationally. Furthermore, a full service SP can offer risk management services for card and bank based payments, transaction payment matching, reporting, fund remittance and fraud protection.

3. RSA ALGORITHM FOR ENCRYPTION AND DECRYPTION

The RSA Algorithm for encryption and decryption will be explained along with simple example as follows

Input: Recipient's RSA public key, (n, e) of length k = |n| bytes; data D (typically a session key) of length |D| bytes with |D|<=k-11.

Output: Encrypted data block of length k bytes

Form the k-byte encoded message block, EB,

1. EB = 00 || 02 || PS || 00 || D

Where || denotes concatenation and PS is a string of k-|D|-3 non-zero randomly- generated bytes (i.e. at least eight random bytes).Convert the byte string, EB, to an integer, m, and most significant byte first,

2. m = StringToInteger(EB)
3. Encrypt with the RSA algorithm
4. c = m^e mod n
5. Convert the resulting cipher text, c, to a k-byte output block, OB
6. OB = IntegerToString(m, k)
7. Output OB.

Suppose we wish to encrypt the 3-byte/24-bit key bit string "8002EA" using the RSA public key

1. The message block is the byte string "8002EA".
2. Compute the message representative
3. m = StringToInteger("8002EA") = 8389354
4. Encrypt with the RSA algorithm
5. c = 8389354^5 mod 25009997 = 2242555
6. Encode the result as a byte string
7. OB =IntegerToString(2242555, 4) = 002237FB

Note that the maximum length of the output block is 4 bytes, because the largest possible integer result is 0x017D9F4C (= n-1), which requires 4 bytes to store in encoded form.

4. CREDIT CARD FORGERY IDENTIFICATION

4.1 Registration

Every user must have to register in the bank in order to become an authorized user to use his/her own Credit Card. The registration procedure is as follows:

1.The customer must have to provide their basic information like username, address, contact information, email id, photo proofs and other required information.

2.The user must also have to register to get an credit card usage application in his/hermobile to login in that application whenever he uses his/her Credit Card.

3. Once the Registration process gets overthe bank administration must have to verify whether all the information provided is true to their knowledge.

4.The information provided are then stored in the database of the server after all verification. Once the information registered is true then the Server generates a Credit card which contains all the information related to the user. The client is given the login information

like Username and Password to login to the Credit card usage application.

As in the existing authentication protocols, we assume the registration phase is performed in a secure and reliable environment, and particularly the device is trusted for its purpose.

4.2 Login-Authentication

The client first swaps his/her Credit card into a card reader for shopping which will extract the data, and then the following process will be done.

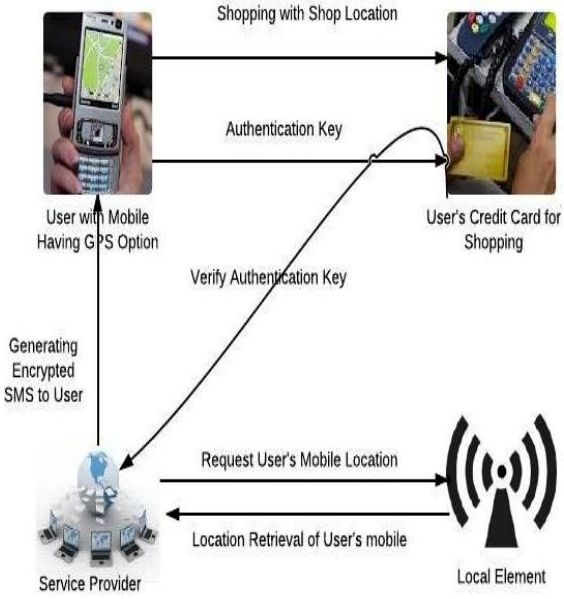

Fig.4.1 Login-Authentication Overview

1. Whenever the user wishes to use his/her credit card for shopping then he/she must have to login to the application usage of credit card in his/her mobile using the provided username and password by the bank.
2. If the username and password does not match with already existing username and password in the database then the user will not be allowed to login to the application and also for further process.
3. Whenever the user uses his/her credit card for shopping then the information will be passed to the service provider, which also perform the functions of the database.
4. The Service Provider in turn generates an encrypted SMS to original user's mobilenumber which was registered in the database.
5. The Service Provider also requests theLocal Element to retrieve the location of the user's mobile number who is using his/her Credit Card for shopping.
6. If the User's Credit Card location and the mobile location are same then the ServiceProvider generates decrypted form of the encrypted message to the user's mobilenumber.
7. If the Service Provider found that the User's Credit Card location and the mobile location are different then the user will not receive the decrypted message and will not be allowed for transaction.
8. Once the user received both the encrypted and decrypted message to his/her mobile number the user must have to upload boththe encrypted and decrypted message tothe application.
9. The Service Provider cross checks the user's encrypted and decrypted message matches with the encrypted and decrypted message in the database of the Service Provider. If it matches then the user will be allowed to pay money using his/her Credit Card otherwise the user will not be allowed for transaction.

Thus, this is how the Credit Card Forgery Identification system with location based tracking using mobiles with GPS works and avoid the unauthorized access of Credit Cards even if the user lost his/her Credit card. So, we can say that our work is highly secure and reliable.

4.3 Password-Change

After a successful login, the client can change his/her password. The server allows the client tochange the old password with new password and updates the data in the Credit card and database accordingly.

5. CONCLUSION

In our work, we proposed the Credit Card Forgery Identification protocol exploiting 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 Credit Card Forgery Identification protocol, in the form of a real case scenario allowing user to perform payments of any kind.

Even if the user lost his/her credit card and mobile the unauthorized users cannot perform the transaction. The analysis shows that the work satisfies all security requirements and has several other practice-friendly features. The future work is to fully identify the practical threats on Credit Card Forgery Identification protocol and develop concrete five- factor authentication protocols with better performances.

REFERENCES

[1] Diana BerbecaruPolitecnico di Torino, Dip. DiAutomatica e InformaticaCorsoDucadegliAbruzzi "19th International Euro micro Conference on Parallel, Distributed and Network-BasedProcessing" , 2011, DOI 10.1109/PDP.2011.32,pp. 141-145

[2] R.J. Hulsebosch, M.S. Bargh, G. Lenzini, P.W.G Ebben, and S.M. Iacob, "Context Sensitive Adaptive Authentication", Proc. of EuroSSC 2007, LNCS 4793, pp. 93-109.

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

[4] 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.

[5] B. Schneier, "Two-Factor Authentication: TooLittle, Too Late", Communications of ACM, Vol.48, No. 4, Apr. 2005, 136.

[6] M. Alexander, "Keeping Online Banking Safe: Why Banks Need Geolocation and Other New Techniques RightNow". http://www.bankersonline.com/security/safebanking.html, May 2005.

[7] Federal Financial Institutions Examination Council, "Authentication in Internet Banking Environment", ttp://www.ffiec.gov/press/pr101205.htm, Oct.2005.

[8] E. Toye, R. Sharp, A. Madhayapeddy, and D. Scott, "Using Smart Phones to Access Site-Specific Services", IEEE Pervasive Computing, Springer-Verlag, Vol. 4, Issue 2, pp. 60-66, 2005.

[9] K. Nichols Randall and Panos C. Lekkas, "Wireless security: models, threats, and solutions", Tata McGraw Hill, 2006.

[10] F. Dominici, D. Mazzocchi, P. Mulassano, M. Spelat, G. Boiero, P. Lovisolo, "NAV/COM Hybrid Architecture for Innovative Location Based Payment Systems", Proc of CCNC 2009, pp. 1-5.

[11] D.E. Denning and P.F. MacDoran, "Location-based authentication: grounding cyberspace for better security", Computer Fraud & Security, Vol.1996, Issue 2, Feb. 1996, pp. 12-16.

[12] A.I. Gonz´alez-TablasFerreres, B. Ramos Alvarez, and A.R. Garnacho, "Guaranteeing the Authenticity of Location Information", IEEE Pervasive Computing, Vol. 7, Issue 3, July-Sept.2008, pp. 72-80.

[13] M.G. Kuhn, "An Asymmetric Security Mechanism for Navigation Signals", Proc. of Sixth Int'l Workshop Information Hiding (IH) 2004, LNCS 3200, pp. 239-252.