Middle-East Journal of Scientific Research 20 (11): 1578-1581, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.11.902

LRAP a Location-Based Remote Client Authentication Protocol for Mobile Environments

R. Vinusha

Department of Computer Science and Engineering,
Bharath University, India

Abstract: 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. Since the location information itself is subject to forging attacks, additional mechanisms must be used to certify its integrity. We propose LRAP, a novel protocol combining several authentication factors to securely authenticate a mobile user. In LRAP, 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 self-service gas stations, a widely available service vulnerable to several types of security attacks and we proposed an LRAP-based service exploiting one time codes and certified position for secure payment operations.

Key words: As use case · We considered the payment service · Services · The user's location might be used as authentication · Widely available service vulnerable to several.

INTRODUCTION

Authentication is considered the most important security service staying at the basis of many products and application services nowadays. To perform authentication, various meth- ods 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) and 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, even though both methods could be extended to achieve this protection too. 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 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 [1]. The ground navigation system LORAN (Long Range Aid to Navigation) for example is used in several military and navigation systems, but it cannot be used on wide range in any application scenario [2]. 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 II). We propose 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

Corresponding Author: R. Vinusha, Department Of Computer Science And Engineering, Bharath University, India

location data, LRAP 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 LRAP-based service involving payment with the mobile devices at the gas stations.

Literature Survey

Verifier-based Home Network Security Mechanism: The home network is expected to experience significant growth over next few years, as wireless and ubiquitous networking becomes more common and accessible. However, the broadcast nature of this technology creates new security issues. To ensure the effective deployment in home environments, network security must reach a certain level which is reasonably acceptable to the research community. The security mechanism for home networks must not require heavy computations, since usually consist of low CPUs capable, limited memory and storage and mobility concerns. This paper presents a secure authentication and session key establishment mechanism suitable for home networks [2]. The proposed scheme is based on the Secure Remote Password (SRP) protocol. The performance evaluation demonstrates that our proposed mechanism is more secure than previous ones while maintaining the similar level of security overhead including processing time.

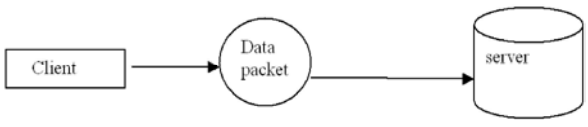
Two Factor Authentication Using Mobile Phones: This paper describes a method of implementing two factor authentication using mobile phones. The proposed method guarantees that authenticating to services, such as online banking or ATM machines, is done in a very secure manner [3]. The proposed system involves using a mobile phone as a software token for One Time Password generation[4]. The generated One Time Password is valid for only a short user defined period of time and is generated by factors that are unique to both, the user and the mobile device itself. Additionally [5], an SMS-based mechanism is implemented as both a backup mechanism for retrieving the password and as a possible mean of synchronization. The proposed method has been implemented and tested. Initial results show the success of the proposed method [6-15].

Secure Remote Client Authentication: This paper discusses an application of Secure Remote Client Authentication. It presents a Smart Cards and Digitally certification from third party vendors, Smart cards are based on algorithm to provide secure Remote client Authentication. These schemes vary significantly [16-20]. In relation to today's security challenges, which include phishing, man-in-the-middle attacks and malicious software. Secure Remote Client authentication plays a key role

Authentication in an Internet Banking Environment: On August 8, 2001, the FFIEC agencies1 (agencies) issued guidance entitled Authentication in an Electronic Banking Environment (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;2 increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies [21]. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services [22].

This guidance applies to both retail and commercial customers and does not endorse any particular technology [23]. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider [24]. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Data Flow Diagram



Module Description

Mobile Client: Client provides Login User Name and Password [25]. Then the card is swiped by the client. This starts one time encrypted code generation process in service provider, where the location of the user is identified using Local Element [26]. This code (encrypted key) is received by client mobile. The client enter key in credit institution to perform transaction [27].

Point of Sale: The Place of purchasing a product and make payment through our system. It receives Decrypted key of client from Service provider [28]. Here the key is typed by client. By which further transaction is carried out only when key is valid for secured transaction [29].

Service Provider: Service Provider gets card number from client, user terminal position and their information using local element. Then generates one time encrypted code for that information and send SMS this code to the client. In the same way it sends decrypted key to Point of sale.

Local Element: Local Element accesses to global navigation satellite system data, by dedicated connection to GPS Reference Stations and can exploit all the functions and data available in the mobile operator Network from the network database. This information is given to Service provider, since key generation in service provider needs Transaction time, location information.

Sending SMS: The client receives one time encrypted code in his/her mobile from service provider. This key is entered in point of sale. Only when this key is authenticated by Point of sale further transaction can be done.

CONCLUSION

In our work, we proposed the LRAP 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 LRAP protocol, in the form of a real case scenario allowing user to perform payments at the self service gas stations [30]. Future work is foreseen on other aspects of our scheme (e.g. privacy issues, tamper resistant security module, sufficient key space or computation and energy costs)

REFERENCES

1. Kumaravel. 2013. A Routing Algorithm over Semi-regular Tessellations, Xplore, pp(s): 1180-1184.
2. Kumaravel,. 2013. A Algorithm for Automaton Specification for Exploring Dynamic Labyrinths, Indian Journal of Science and Technology, pp: 6-5.
3. Kumaravel, 2013. A Introducing an Efficient Programming Paradigm for Object-oriented Distributed Systems, Indian Journal of Science and Technology, 6(5S): 4597-4603.
4. Weigold, T., T. Kramp and M. Baentsch, 2008. Remote Client Authentication, IEEE Security and Privacy, 6(4): 36-43.
5. Hulsebosch, R.J., M.S. Bargh, G. Lenzini, P.W.G Ebben and S.M. Iacob, 2007. Context Sensitive Adaptive Authentication, Proc. of EuroSSC, LNCS 4793, pp: 93-109.
6. Brainard, J., A. Juels, R. Rivest, M. Szydlo and M. Yung. 2006. Fourth Factor Authentication: Somebody You Know, Proc. of ACM CCS, pp: 168-178. [4] H. Zheng, J. [4].
7. Schneier, B., 2005. Two-Factor Authentication: Too Little, Too Late, Communications of ACM, 48(4): 136.
8. Alexander, M., 2005. Keeping Online Banking Safe: Why BanksvNeed Geolocation and Other New Techniques Right Now. http://www. bankersonline. com/security/safebanking.html.
9. Federal Financial Institutions Examination Council, Authentication in Internet Banking Environment, http://www.ffiec.gov/press/pr101205.htm.
10. Toye, E., R. Sharp, A. Madhayapeddy and D. Scott. Using Smart Phones to Access Site-Specific Services, IEEE Pervasive Computing, Springer-Verlag, 4(2): 60-66.
11. Gruteser, M. and X. Liu, 2004. Protecting Privacy in Continuous Location- Tracking Applications, IEEE Security & Privacy Magazine, 2(2): 28-34.
12. Liu, D. and P. Ning, 2003. 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.
13. Denning, D.E. and P.F. MacDoran, 1996. Location-based authentication: grounding cyberspace for better security, Computer Fraud & Security, 2: 12-16.
14. Ferreres, A.I. Gonz´alez-Tablas, B. Ramos Alvarez and A.R. Garnacho, 2008. Guaranteeing the Authenticity of Location Information, IEEE Pervasive Computing, 7(3): 72-80.
15. Kuhn, M.G., 2004. An Asymmetric Security Mechanism for Navigation Sig- nals, Proc. of Sixth Int'l Workshop Information Hiding (IH), LNCS 3200, pp: 239-252.
16. Malaney, R.A., 2004. A location enabled wireless security system, Proc. Of GLOBECOM 4: 2196-2200.
17. Spelat, M. and F. Margary, 2008. GAL-PMI Project: Global Navigation Satellite Systems to Support Mobility and Security, Proc. of Space Applications Days 2008, Toulouse (France), 22-25, pp: 608- 612.

18. Ringert, J., E. Wasle, J. Hanley and S. Scarda, 2006. Bringing Galileo Into LBS Market - the Agile Project Proc. of IEEE 17th Int. Symp. On Personal, Indoor and Mobile Radio Communications, 11-14 : 1-5.
19. Lackey, K., 2008. Thieves skim credit card data at fuel pumps, USA TODAY, 5 August, http://www. usatoday. com/money/industries/energy/2008- 08-04-gaspumpskimming N.htm.
20. TruckFLIX LLC. 2007. Fuel fraud: Thieves use pay-at-pump technology to steal millions, https://secure.truckflix.com/news article. php?newsid =5298,
21. Bergstrom, C. and J. Chuprun, Optimal hybrid frequency hop com- munication system using nonlinear adaptive jammer countermeasures and active fading mitigation, Proc of IEEE GLOBECOM 98(6): 3426-3431.
22. Leemon, C., Baird III, William L. Bahn, Michael and D. Collins, Jam resistant communications without shared secrets, Proc. of ICIW08, Omaha, Nebraska, April 24-25, http://leemon.com/papers/2008bbc.pdf.
23. Liao, H.C., Y.H. Chao, C.Y. Hsu, 2006. A Novel Approach for Data Encryption Depending on User Location, Proc. of PACIS 2006, 5-9, http://www.pacis-net.org/file/2006/1117.pdf.
24. Qiu, D., 2007. Security Analysis of Geoencryption: A Case Study Using Loran, Proc. of ION GNSS 2007, Texas, USA, pp: 1146- 1154.
25. Dominici, F., D. Mazzocchi, P. Mulassano, M. Spelat, G. Boiero and P. Lovisolo, 2009. NAV/COM Hybrid Architecture for Innovative Location Based Payment Systems, Proc of CCNC pp: 1-5.
26. Gonz´alez-Tablas, A.I., K. Kursawe, B. Ramos and A. Ribagorda, 2005. Sur-vey on Location Authentication Protocols an1d Spatial-Temporal Attestation Services, Proc of EUC Workshops 2005, LNCS 3823, pp: 797-806.
27. Randall, K. Nichols, Panos C. Lekkas. Wireless security: models, threats and solutions. 2006. Tata Mgraw Hill,.
28. Kumaravel. 2013. A an Application of Non-uniform Cellular Automata for Efficient Cryptography, Xplore, pp(s): 1200 -1205.
29. Kumaravel. 2013. A Application of Non-uniform Cellular Efficient Cryptography Automata, Indian Journal of Science and Technology, 6(5S): 4561-4566.
30. Kwak, K., Son, W. Lee, S. Kim and D. Won, 2006. Confidence Value Based Multi Levels of Authentication for Ubiquitous Computing Environments, Proc. of ICCSA, LNCS 3981, pp: 954-963.