A Survey on Location Based Authentication Protocols For Mobile Devices

[1]Smruti. P. Patil, [2]S.U. Nimbhorkar

[1]Dept. of. Computer Science And Engineering
G. H. Raisoni College of Engineering, Nagpur, India

Abstract

As per the recent studies, the volatile growth has been seen in the use of mobile devices as the supporting technology for accessing Internet based services, as well as for personal communication needs in networking. Various studies indicate that it is impossible to utilize strong cryptographic functions for implementing security protocols on mobile devices. Our research negates this. Explicitly, a performance analysis focused on the most commonly used cryptographic protocols based on the location address (latitude & longitude) of the user for mobile applications and anticipated provably secure authentication protocol that is more efficient than any of the existing authentication protocol is being discussed in this paper. Understanding the use of public key cryptography which makes potential use of discrete logarithms problem. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm. To provide secure communication for mobile devices, authenticated protocol is an important primitive for establishing trusted connection. In this paper, it has been studied that the location based system provides a better security and acquires much less energy consumption than the existing authentication protocols.

Keywords: *Elliptic curve cryptography, location based cryptography, and authentication*

1. Introduction

The mobile devices (cell phone, tabs etc.) are being widely used by the people and mobile applications for accessing the wireless networks. In an increasingly interconnected world, the interaction among the devices and the people is increasing rapidly. Accessing the internet has become essential in many of the professions and also in the corporate sectors in today's competitive world.

Secure and fast transmission of sensitive digital information over wireless channels has become increasingly important. The use of public key cryptography consumes a significant portion of the overall system resource. The computation complexity of asymmetric key based system is complicated and is always subject to attacks by adversaries. Appreciating global roaming services became possible with the use of portable communication systems, and hence the system is available for the conversations over wireless networks. In wireless network, mobile users send and receive data packets wirelessly and therefore internet. Hence, portable communication is very much vulnerable to security than wired networks [1] - [7].

The security features needed to provide security to roaming services are authentication, integrity, user-privacy and non- repudiation. For achieving the goal of security, the cryptographic algorithms are being used such as pubic key and private key algorithms. Among the existing protocols, major parts of the protocols have been proposed on the secret key algorithms because mobile devices have limited memory. However secret-keys algorithms do not support non-repudiation. [6].

Privacy in location based services has become has become a topic of interest for research. There is an increasing number of devices with geo-positioning system and data communication capabilities. Many places have enabled a use of wireless LAN in recent years. Not only universities, colleges, homes but stations, airports, amusement parks and shopping malls have set up wireless LANs. For this type of networks location privacy issue is of great importance. [5]

2. Background and Related Work

This section discusses the results obtained from the previous researches. It is stated in [9] that this paper instigate the fast developing cryptographic researchers and to increase the security development in the field of information and security Elliptic Curve Cryptography (ECC) is a technique which uses smallest keys to provide high security and high speed in low bandwidth. Elliptic Curve Cryptography has become the cryptographic choice

for networks and communication devices due to its size and efficiency benefits.

S.Prasanna [9] has given the features of ECC as the security and efficiency. It has been examined that they also provides the basis for why the ECC is most suitable for constrained environments. This paper also explores its performance in wireless systems. ECC can be implemented in software and
in hardware . ECC can be implemented in different ways. ECC uses arithmetic algorithms as the main objective operations for high level security functions such as encryption for gaining confidentiality and digital signature for authentication. ECC can be implemented in software and in hardware. ECC follows generic procedure like parties agrees on publicly-known data items and each user generates their public and private keys [11]. Many devices are constrained devices that have small and restricted storage and can be applied. ECC can be functional. For wireless communication devices like PDA's, multimedia cellular phones .It can be used for security of Smart cards ,wireless sensor networks,
wireless mesh networks. Web servers that need to handle many encryption sessions.

S.Prasanna [10] also shows that the existing authentication protocols based on RSA asymmetric cryptography are not suitable for devices which consumes more computing power, memory capacity, key sizes and cryptographic support. For this reason only, an efficient protocol must be designed for resource constrained platforms to attain high level of security similar to the protocols which are being designed and implemented today. It has been studied that the performance of the Elliptic Curve Cryptography is good over the performance of RSA algorithm [10].

The existing authentication protocol highlighted in [10], which have the basis of RSA algorithm are not feasible for such devices having low battery power, key sizes and cryptographic support. Due to these reasons it was possible to implement Hyper elliptic Curve Cryptography (HECC) in resource constrained mobile devices with improved performance as compared to RSA. Protocols related to HECC systems can be directly used in mobile devices. The performance of this algorithm is better than RSA and somewhat low than Rabin Cryptosystem.
The paper [12] deals with the performance of various encryption techniques that have been measured for the betterment of the security services. Active server pages (ASP) has been selected and five different encryption algorithm have been studied. The different algorithms are Blowfish, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Tiny Encryption Algorithm and Towfish. These algorithms are known to be able to support 132-bit size.

There are quite a number of Web browsers that are available in the market, but these four are known to be among the top and most popular. They are Internet Explorer, Mozilla Firefox, Opera and Netscape Navigator. From analysis, we hope to find out the most impeccable Web browsers that can match in the best possible way with the encryption algorithms for ASP scripts. There are different numbers of Web browsers available in the market, but these four are known to be among the top and most popular. They are Internet Explorer, Mozilla Firefox, Opera and Netscape Navigator. From analysis, we hope to find out the most impeccable Web browsers that can match in the best possible way with the encryption algorithms for ASP scripts.

The study made in paper [13] deals with security measures considered for the performance of the encryption process at different scripts languages used for the web browsing. In this paper performance analysis is followed by the conduction if the simulation tests in order to obtain the best Encryption Performance Evaluation of Symmetric Encryption Algorithm.

The [13] paper deals with the conclusion of an efficient algorithm scheme suitable for the mobile devices. For mobile station authentication it uses Elliptic Curve Cryptosystem; this scheme provides both the communication efficiency and computational efficiency as compared to other authentication schemes. The scheme requires one scalar point multiplication operation and two short messages on mobile stations for each session establishment after the initial one-time delegation key verification. It is well suited for low-power mobile devices in wireless networks.

3. Privacy and Preserving Techniques for location-based services

In a general scenario to use a location based service, a user first retrieves his/her location information with the GPS system and then issues a query to a location- based service with his/her location information as a parameter. After processing the location-based service returns the results to the client. To protect location privacy in location-based systems is of utmost importance. Different approaches have been suggested for providing the security to such systems.[14]

The Query Enlargement Technique – The key idea in this technique is to lower the spatial resolution of location data sent to the location-based service. This technique hides the user's exact location and fails to hide the user's region location.

The spatial clocking technique [14]. In this, k user's locations are collected to form a corresponding clocking region which is sent to location-based service. The location-based service then returns all candidate results corresponding to any location in the cloaking region. This technique is somewhat inefficient to process the queries properly.

In obfuscation techniques, user locations are concealed within dummies (faked or fixed locations). Dummies can be randomly generated faked locations or fixed locations such as road intersections. In most of the existing obfuscation systems, dummies are generated at client side in the context of one client - one server.
Mixes and Binomial Mixes are commonly used in anonymous and privacy preserving systems. [14] Message collection, message selection, message transformation and message delivery are the parameters used in Mixes and Binomial-Mixes. Location- Hiding Property and User's Location Privacy Map is also used in Binomial-Mix-Based Location Anonymizer System With Global Dummy Generation [14].

For external location-based system, GPS is mostly used. GPS is mostly depended system on receiving satellite transmission, it does not function effectively in built-up areas and is especially not accessible indoors. [15]. GPS uses satellites for location determination and its receiver needs to communicate with at least four satellites to find the location, hence this approach can be unreliable and time consuming. Due to the limitation of this system another technology was developed at Olliveti Research Laboratory which used infrared technology for indoor location identification. This method also had some limitations and then came Radio Frequency Identification Technology (RFID) which has been used in many organizations and agencies such as U.S Department of Defence, the food and Drug Administration and Wal Mart Stores. RFID has two main components: RFID tag or transponder and RFID reader. RFID tags are categorized as either active (with a battery) or passive (powered by the signal strength emitted by the reader.

With the rapid rise in GSM and smart phones, location services in China achieved a rapid growth in the year 2009. At present, networks of domestic telecom operators are upgraded to Cell-ID, and it allows any mobile phone user to locate with a mobile base station, and as of now, most mobile phone users take this method to locate. A new approach of location service system- Mobile New Concept which applies LL-TOA method based on base station for positioning the mobile phone, thus combine mobile positioning and mobile instant messaging organically providing a brand new experience of location services and communication with friends.[16]

4. Conclusion

In this survey paper, we have seen the different authentication protocols and the location-based techniques too. All the techniques have some or more advantages and disadvantages and therefore the new techniques have been evolved. This paper exposed the importance location-based system to provide the secure and fast transmission of data through the wireless medium.

References

[1] K.Saravana selvi\ T.Vaishnavi2 I.Assistant Professor ,Bharath Niketan Enginering college, Tamil Nadu "Rabin PublicKey Cryptosystem for Mobile Authentication" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012.

[2] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system, " IEEE J. Set. Areas Commun. ,vol. 11, pp. 821-829, 1993.

[3] C. C. Lo and Y. J. Chen, "Secure communication mechanisms for GSM networks," IEEE Trans. Consum . Electron. , vol. 45, pp. 1074-1080, 1999.

[4] T.-F. Lee, c.-c. Chang, and T. Hwang, "Private authentication techniques for the global mobility network," Wireless Personal Commun. , vol. 35, no. 4, pp. 329-336, 2005.

[5] T.-F. Lee, S.-H. Chang, T. Hwang, and S.-K. Chong,"Enhanced Delegation-Based Authentication Protocol for PCSs, " IEEE Trans. Wireless Commun. , vol. 8, no.5, pp. 2166-2171, 2009.

[6] H.-Y. Lin and L. Harn, "Authentication protocols with non-repudiation services in personnel communication systems, " IEEE Commun. Lett. , vol. 3, no. 8, pp. 236-238, 1999.

[7] H.-Y. Lin, "Security and authentication in PCS, "Comput. Elect. Eng. , vol. 25, no. 4, pp. 225-248, 1999.

[8] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems, " IEEE Trans. Wireless Commun. , vol. 4, no. 1, pp. 57-64, 2005.

[9] S. Prasanna Ganesan, Dr. GRD College of Science, "An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography "978-1-4244-5848-6/10/$26.00 © 2010 IEEE.

[10] S. Prasanna Ganesan, Dr. GRD College of Science, "An Authentication Protocol For Mobile Devices Using Hyperelliptic Curve Cryptography "International Journal of Recent Trends in Engineering and Technology, Vol. 3, No. 2, May 2010.

[11] S. U. Nimbhorkar, L.G.Mallik, "A Survey On Elliptic Curve Cryptography" International Journal Of Advanced Studies In Computers Science And Engineering, survey ECC_June12.

[12] Syed Zulkarnain Syed Idrus1, Syed Alwee Aljunid2, Salina Mohd Asi3, Suhizaz Sudin4, and R. Badlishah Performance Analysis of Encryption Algorithms' Text Length Size on Web Browsers. Ahmad5 IJCSNS International Journal of Computer Science 20 and Network Security, VOL.8 No.1, January 2008Manuscript received January 5, 2008. Manuscript revised January 20, 2008.

[13] Caimu Tang, Member, IEEE, and Dapeng Oliver Wu, Senior Member, IEE" -An Efficient Mobile Authentication Scheme for wireless networks " IEEE transactions on wireless communications, vol. 7, NO. 4, APRIL 2008.

[14] Binomial-Mix-based Location Anonymizer System with Global Dummy Generation to Preserve User Location Privacy in Location-Based Services. 2010 International Conference on Availability, Reliability and Security.

[15] Seyed Hossein Siadat, Ali Selamat" Location-Based System for Mobile Devices Using RFID" Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, 2008 IEEE DOI 10.1109/AMS.2008.44.

[16] Panigrahi, Sunil Kumar, Soubhik Chakraborty, and Jibitesh Mishra. "A Statistical Analysis of Bubble Sort in terms of Serial and Parallel Computation." (2012).

[17] Xiufeng Liu1, Longguang Zhang2, Xiuju Zhan1, Pingping Chen1." Location-based Mobile Instant Messaging System" Information Technology College, Guangzhou University of Chinese Medicine, Guangzhou, China .©2012 IEEE.