THREE-FACTOR AUTHENTICATION FOR MOBILE TRANSACTION

[1]Sharana Gowda, [2]Prof. Pundalik Ranjolkar
[1],M.TechStuden.,Computer Science & Engineering, VTU Belgaum
KLE Dr. M. S. Sheshgiri College of Engineering & Technology, Belgaum, Karnataka, India
[2]Assistant Professor, Computer Science & Engineering, VTU Belgaum
KLE Dr. M. S. Sheshgiri College of Engineering & Technology, Belgaum, Karnataka, India
Email: [1]sharangoudah@gmail.com, [2]pundalikr@rediffmail.com

Abstract-Nowadays important to secure user data in a distributed environment from a unauthorized person or a use. In a distributed system, various resources are distributed in the form of network services provided and managed by servers. Remote authentication is most commonly used method in a distributed environment using user name and password used in earlier days but it can easily be hacked by others by using some dictionary attacks. To overcome this problem two factor authentication was developed in this Approach both the password and smartcard being used again this is failed because if the smartcard get lost the attacker can easily guess the password. To overcome this problem authentication by using three-factor. In three factor authentication mainly involves first one is password, second one is OTP and Biometric characteristics such as finger print scan, face recognition etc.

Keywords- Authentication, Biometric, Encryption, Decryption, Local Element, Service Provider.

1. INTRODUCTION

In a distributed system, numerous resources are distributed within the form of network services provided and managed by servers. Remote authentication is that the most typically used methodology to work out the identity of a remote client. In general, there are three authentication factors:

1. Something the consumer or client knows: Password

2. Something the client has: Smart card

3. Something the consumer or client is: Biometric characteristics such as finger print, iris scan etc.

Most early mechanisms are supported username, password or positive identification and this type of authentication protocols are to straightforward to implements, and passwords have several vulnerabilities. This kind of human generated passwords are straightforward to come up with and bear in mind are sometimes are short string of characters poorly chosen. By exploiting these vulnerabilities, straightforward word book (Dictionary attacks) will crack passwords in a very short time [1].As a result of these considerations, hardware authentication

tokens are introduced to strengthen the protection in user authentication, and smart-card-based password or positive identification authentication has become one among the foremost common authentication mechanisms.

Smart-card-based password or positive identification authentication provides 2factorauthentication, namely a successful login needs the consumer to possess a legitimate charge account credit and an accurate positive identification. While it provides stronger security guarantees than password or positive identification authentication, it may also fail if both authentication factors are compromised (e.g., an attacker has successfully obtained the password and the data in the smart card).

Another authentication mechanism is biometric authentication [2], [3], [4], whenever users are known by their measurable human characteristics, like fingerprint, voiceprint, and iris scan. Biometric characteristics are believed to be a reliable authentication factor since they supply a possible supply of high-entropy data and can't be easily lost or forgotten. Despite these merits, biometric authentication has some imperfect features. Unlike password, biometric characteristics cannot be easily changed or revoked. Some biometric characteristics (e.g., fingerprint) can be easily obtained without the awareness of the owner. This motivates the three-factor authentication, which incorporates the advantages of the authentication based on password, biometrics and OTP or OTC.

We [5] in addition propose Location primarily based remote authentication protocol (LRAP), a secure location-based remote authentication protocol which could be accustomed proof the remote users in mobile environments. LRA Prelies on the employment of "classical" authentication ways (like the static passwords and therefore the just once passwords) combined with user location info at just once. To verify the integrity of the situation information, LRAP exploits a fervent part, named native part or local element (LE) that is a component of the stargazer 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.

2. LITERATURE SURVEY

Several authentication protocols have been proposed to integrate biometric authentication with password authentication and/or smart-card authentication. Lee et al. [6] designed an authentication system which does not need a password table to authenticate registered users. Instead, smart card and fingerprint are required in the authentication. However, due to the analysis given in [7], Lee et al.'s scheme is insecure under conspiring attack.

Instead of using smart card based authentication I am using LRAP (location based remote authentication protocol).
Here the *Location as authentication factor*. Two-factor authentication is considered not adequate for security problems encountered today, like phishing or identity theft [8]. And 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. Because of this we propose a scheme called fuzzy extractor here we are using fuzzy logic algorithm to our biometric and algorithm convert our biometric into a fuzzy generated random value.

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 [9]. Geo location technology 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 [10]. The geo-location information has been used in the past in several

location-based services, such as emergency and information services [11], tracking and monitoring systems [12], or even for establishing pairwise keys in the sensor networks [13]. In the security area, some location-authentication schemes have been proposed [14], but the location authentication is still considered a novel security service [15], 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 anti spoofing 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 (e.g. can be hired relatively cheaply), and 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, Denning & Doran proposed a "location signature sensor" (LSS) tamper-proof device [13] whose role is to create (and verify) allocation signature (LS) containing geodetic position and valid for a short time, e.g. for 5ms. Thus, an LS acts more or less like an unpredictable one time password. Nevertheless, Kuhn notes some critical points of the LSS-based solution [16], 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, like [17], propose to exploit the location-positioning capabilities of a wireless network to check out the location information. Other solutions proposed to guarantee the authenticity of location information against the most common location-related attacks are shortly presented in [15].

Galileo Local Elements. The European Galileo programmer 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, avail-ability 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 [15]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 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 OTChas 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 or fund transfers to non-registered third party accounts. In some security products, like in the

Clavister SMS One-Time Password service 3, 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.

3. PRELIMINARIES AND DEFINITIONS

In this section, we first describe the system model and give the definition of LRAP protocol. Then, we define.

A. Definition of a System Model

Mobile Client: Client provides Login User Name and password, then location of the user is identified by local element after this we have to do transaction at this time it will ask for biometric here we have to give the biometric(like finger print). After that service provider generates the token and send to mobile client.

Service Provider: Service Provider gets account details 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.

B. Goals

The aim of this project is to investigate a systematic approach for developing a secure three-factor authentication with the protection of user privacy. Three-factor authentication mainly involves three levels of security, first one is password, second one is One-Time-Password (OTP) or One-Time-Code (OTC), and Biometric characteristics such as finger print scan, face recognition etc. In this project, we are using finger print scan as biometric authentication.

C. Problem Statement/Existing System

Remote authentication is most commonly used method in a distributed environment using user name and password used in earlier days but it can easily be hacked by others by using some dictionary attacks. To overcome this problem two factor authentication was developed in this Approach both the password and smartcard being used again this is failed because if the smartcard get lost the attacker can easily guess the password.And again to overcome this problem three factor authentication includes user name, password Smart card and biometric embedded in smart card again this approach is failed.Because if the smartcard get lost shown below in
figure 1

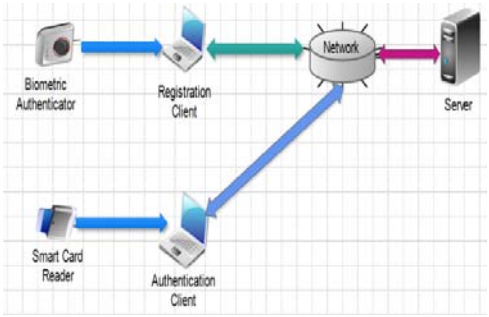

Figure.1: A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Sy

4. PROPOSED SYSTEM

Approach both the password and smartcard being used again this is failed because if the smartcard get lost the attacker can easily guess the password.To overcome this problem authentication by using three-factor. In three factor authentication mainly involves first one is password, second one is OTP and Biometric characteristics such as finger print scan, face recognition etc.

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 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 (location based remote authentication protocol) -based service involving payment with the mobile devices at the gas stations.

1. Our approach demonstrates how to obtain secure three-factor authentication from two-factor authentication.
2. The framework satisfies all security requirements on three-factor authentication and has several other practice-friendly properties (e.g., key agreement, forward security, and mutual authentication).

3. The user of OTP provides secure authentication for discovering user interaction

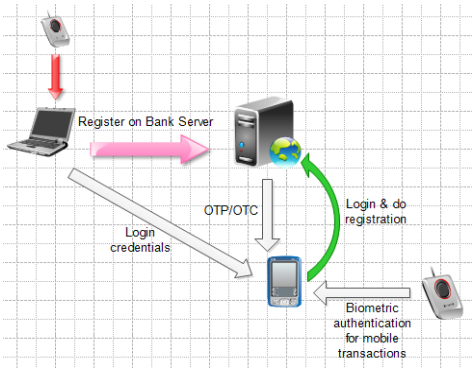

Figure.2: Three-Factor Authentication for Mobile Transaction.

5. SOLUTION

- **LDEA ALGORITHM**

In LRAP, we derive the location-dependent data encryption (LDEA) algorithm-key. But we use the symmetric key encryption with a shared key (named KSe) to generate the Final-key. To ensure the integrity of the OTC, the SP calculates a keyed digest on the OTC and the symmetric key KSa. The TOKEN obtained by encrypting the OTC with a symmetric algorithm (like 3DES) and the Final- key is different at each session. Since the position determined by the GPS receiver of the UT terminal could be inaccurate and inconsistent depending on how many satellite signals are received.

- **FUZZY EXTRACTOR**

A fuzzy extractor extracts a nearly random string R from its biometric input w in an error-tolerant way. If the input changes but remains close, the extracted R remains the same [18]. To assist in recovering R from a biometric input w0, a fuzzy extractor outputs an auxiliary string P. However, R remains uniformly random even given P. The fuzzy extractor is formally defined in two steps that is shown below.

Definition (Fuzzy Extractor): An (M, m, l, t, belongs to) fuzzy extractor is given by two procedures (Gen, Rep).

$$\xrightarrow{BioData:w} \boxed{\text{Gen}} \rightarrow \begin{cases} R: & \text{Random String;} \\ P: & \text{Auxiliary String.} \end{cases}$$

Gen is a probabilistic generation procedure, which on(biometric) input w2M outputs an "extracted" string R belongs to {0, 1} power (l) and an auxiliary string P. For any distribution 'W' on M of min-entropy m, if <R; P><-Gen (W) then we have SD (<R, P>, <Ul, P>) <=e Here, Ul denotes the uniform distribution on l-bit binary strings.

$$\xrightarrow[P]{BioData:w'} \boxed{\text{Rep}} \rightarrow R \text{ if } \mathsf{dis}(w, w') \leq t.$$

Rep is a deterministic reproduction procedure allowing to recover R from the corresponding auxiliary string P and any vector w0 close to w: for all (w,w')belongs to M satisfying dis(w,w')<=t, if <R; P><-Gen(w) then we have Rep(w',P)=R.

A. *Advantages*

1. Our approach demonstrates how to obtain secure three-factor authentication from two-factor authentication.
2. The framework satisfies all security requirements on three-factor authentication and has several other practice-friendly properties (e.g., key agreement, forward security, and mutual authentication).
3. The user of OTP provides secure authentication for discovering user interaction

6. CONCLUSION

Preserving security and privacy is a challenging issue in distributed systems. Three- factor authentication to protect services and resources from unauthorized use. The authentication is based on password, One-Time-Password (OTP) or One-Time-Code (OTC), and biometrics**.** 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. 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] D.V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," Proc. Second USENIX Workshop Security, 1990.

[2] Biometrics: Personal Identification in Networked Society, A.K. Jain, R. Bolle, and S. Pankanti, eds. Kluwer, 1999.

[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003.

[4] Ed. Dawson, J. Lopez, J.A. Montenegro, and E. Okamoto, "BAAI: Biometric Authentication and Authorization infrastructure," Proc. IEEE Int'l Conf. Information Technology: Research and Education (ITRE '03), pp. 274-278, 2004.

[5]REF1:www.idosi.org/mejsr/mejsr20(11)14/46.pdf

[6] J.K. Lee, S.R. Ryu, and K.Y. Yoo, "Fingerprint-Based Remote User Authentication Scheme Using Smart Cards," Electronics Letters,vol. 38, no. 12, pp. 554-555, June 2002.

[7] C.C. Chang and I.C. Lin, "Remarks on Fingerprint-Based Remote User Authentication Scheme Using Smart Cards,"ACM SIGOPS Operating Systems Rev., vol. 38, no. 4, pp. 91-96,Oct. 2004.

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

[9] 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.

[10] Federal Financial Institutions Examination Council, "Authentication inInternet Banking Environment", http://www.ffiec.gov/press/pr101205.htm,Oct. 2005.

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

[12] M. Gruteser and X. Liu, "Protecting Privacy in Continuous Location- Tracking Applications", *IEEE Security & Privacy Magazine*, Vol. 2, Issue 2, pp. 28–34, 2004.

[13] D. Liu and P. Ning, "Location-based pairwise key establishments for static sensor networks", *Proc. of the 1st ACM workshop on Security of adhoc and sensor networks*, Fairfax, Virginia, pp. 72-82, 2003.

[14] 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.

[15] 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.

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

[17] R.A. Malaney, "A location enabled wireless security system", *Proc. OfGLOBECOM 2004*, 4, pp. 2196 2200.

[18] Xinyi Huang, Yang Xiang, Member, IEEE, Ashley Chonka, Jianying Zhou, and Robert H. Deng, Senior Member, IEEE "A Generic Framework for Three-Factor Authentication: Preserving Securityand Privacy in Distributed Systems"