Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 10, October 2013, pg.30 – 35

RESEARCH ARTICLE

An Improved Authentication Framework using Steganography along with Biometrics for Network Security

P. DHIVYA
Master of Engg, Dept of CSE
Sri Eshwar college of Engg,
Coimbatore, India

S. MOHANAGOWRI
Master of Engg, Dept of CSE
Sri Eshwar college of Engg,
Coimbatore, India

Dr. N. SARAVANASELVAM
Prof, Department of CSE,
Sri Eshwar college of Engg,
Coimbatore, India

Abstract- To protect the distributed system from unauthorized user, many technologies were proposed. But the security technology used in today's computer and Internet environment is the three-factor approach, the three factors are IP, smart-card, biometrics (fingerprint) along with steganography. This scheme is proposed to upgrade three-factor authentication in which password is used instead of IP. Our new framework provides strong protection against different kinds of attacks at a reasonable computational cost.
Keywords: Smart Card; Biometrics; Steganography; Computational Cost

I. INTRODUCTION

For thousands of years individuals have used passwords to authenticate their identity. The security system first implemented on computers 40 years ago was password. Authorities today agree that effective authentication of a person's identity requires a combination of at least two of the three independent means of authentication, or factors. The factors are IP, Smartcard, Biometrics(finger print) along with the steganography(concealing the message). Most early authentication mechanisms were purely based on passwords, which have much vulnerability [1]. To strength the security, two factor authentication mechanisms were used. The two factors are password and smart-card; it could also fail if both the authentication factors are compromised. In this case the three factor authentication mechanism was used to improve the security. The three factors are password, smart-card and biometrics [2],[3],[4]. But passwords have various attacks like password guessing attack and dictionary attack so in our scheme we are using IP instead of password. In order to provide more security we are using steganography along with biometric characteristics (finger print).

II. RELATED WORK

The main contribution of this paper could be a generic framework for three-factor authentication in distributed systems. The framework that planned has many deserves as follows: 1st, we have a tendency to demonstrate a way to incorporate statistics within the existing authentication supported open-end credit and information processing then with the steganography. Our framework is generic instead of instantiated within the sense that it doesn't have any extra needs on the underlying smart-card-based countersign authentication [5]. It's not solely modify the look and analysis of three-factor authentication protocols, however can also contribute a secure and generic up gradation from 2 issue authentication to three-factor authentication possessing the practice-friendly properties of the underlying two-factor authentication system. Second, authentication protocols in our framework will offer true three-factor authentication, namely IP, smart card, and biometric characteristics [6]. Additionally, our framework is often simply custom-made to permit the server to come to a decision the authentication factors in user authentication (instead of all 3 authentication factors). Last, within the planned framework clients biometric characteristics area unit unbroken secret from servers. This not solely protects user privacy however additionally prevents a single-point

failure (e.g., a broken server) from undermining the authentication level of different services. Moreover, the verification of all authentication factors is performed by the server. Above all, our framework doesn't think about any trusty devices to verify the authentication factors that additionally meet the imperfect feature of distributed systems wherever devices cannot be totally trusted.

III. EXISTING SYSTEM

Remote authentication is that the most typically used methodology to work out the identity of a foreign consumer. There was a lot of potential to get written document to active and passive aggressor in single and 2 issue authentication [7]. Passive aggressor: A passive attacker will get messages transmitted between the consumer and also the server. However, it cannot move with the consumer or the server. Active aggressor: the attacker will indiscriminately inject, modify, and delete messages within the communication between the consumer and also the server. Single issue authentication mechanisms area unit entirely supported secret, whereas such protocols area unit comparatively straightforward to implement, passwords (and human generated passwords in particular) have any vulnerabilities [9]. Two issue authentications give smart-card –based authentication particularly a triple-crown login needs the consumer to possess a legitimate smart-card and secret. It may conjointly fail if each authentication factors area unit compromised (e.g., AN aggressor has with success obtained the secret and also the knowledge within the good card).

IV. PROPOSED SYSTEM

This theme is to analyze a scientific approach for the look of secure three-factor authentication with the protection of user privacy. The method for registration, initial one is science, then provide their fingerprint of the user and a cryptography key is generated to the users email id. When user login with success, user wish to convey their fingerprint if each are match it will raise to produce the key code. Using revolving credit based mostly secret authentication protocol and cryptologic rule. But additionally it will contribute a secure and generic upgrade from two-factor authentication to three-factor authentication. A second authentication issue known as biometric identification will alleviate the matter and any improve the system's assurance.

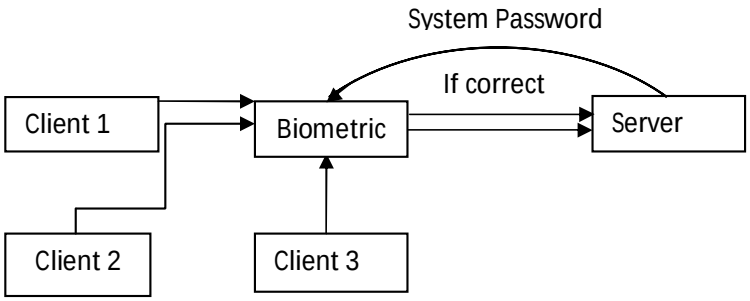
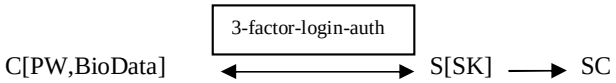


Figure 1. Client Server Communication through biometric

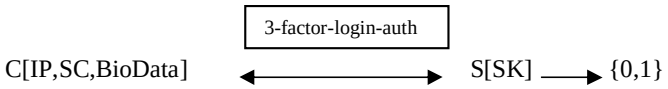
A. Three-Factor Authentication: Three-factor authentication is extremely kind of like smart-card primarily based positive identification authentication; with the distinction that it needs are biometric characteristics as an extra authentication issue. A three-factor protocol involves a consumer C and a server S, and consists of five phases.

3-Factor-Initialization**:** S generates 2 system parameters PK and SK. PK is revealed within the system, and SK is unbroken secret by S, associate degree execution of this formula is denoted by 3-Factor-Initialization (k) ⟶ (PK,SK) where k is system security parameter.

3-Factor-Reg: A consumer C, with associate degree initial positive identification PW and biometric characteristics such as BioData can be registered on the system by running this type of interactive protocol with the server S. The output of this protocol may be a open-end credit SC, that is given to C. associate degree execution of this protocol is denoted by



3-Factor-Login-Auth: This is often another interactive protocol between the consumer C and also the server S, that allows the consumer to login with success victimization PW, SC, and BioData. AN execution of this protocol is denoted by,



3-Factor-Password-Changing: This protocol allows a consumer to alter his/her secret when a winning authentication. The information within the positive identification is going to be updated accordingly.

3-Factor-Biometrics-Changing2: Associate degree analogue of password- dynamical is biometrics-changing, particularly the consumer will amendment his/her statistics utilized in the authentication e.g., employing a completely different finger or victimization iris rather than finger. Whereas biometrics-changing isn't supported by previous three-factor authentication protocols, we tend to believe it provides the consumer with additional flexibility within the authentication.

B. Cost effectiveness: In general, three-factor authentication is a smaller amount computationally economical than smart-card-based arcanum authentication, since the previous needs extra machine resources for biometric identification. to create three-factor authentication sensible, biometric-related operations should be performed quick and accurately. As indicated in, the performance of extracting and authenticating sure sorts of bioscience (e.g., face and keystroke) is not satisfactory; however others (e.g., fingerprint and iris) will satisfy sensible needs.

C. Security requirements: A three-factor authentication protocol may also face passive attackers and active attackers as outlined in SCPAP. A passive (an active) assaulter is often any classified into the subsequent three varieties. Attacker has the charge account credit and therefore the biometric characteristics of the consumer. It's not given the security code of that customer. Assailant has the secret code and therefore the biometric characteristics. It's not allowed to get the information within the charge account credit. Assailant has the open-end credit and therefore the secret code of the consumer. It's not given the biometric characteristics of that consumer. Notice that such associate assailant is unengaged to mount any attacks on the (unknown) life science, as well as life science faking and attacks on the data (related to the biometrics) hold on within the charge account credit.

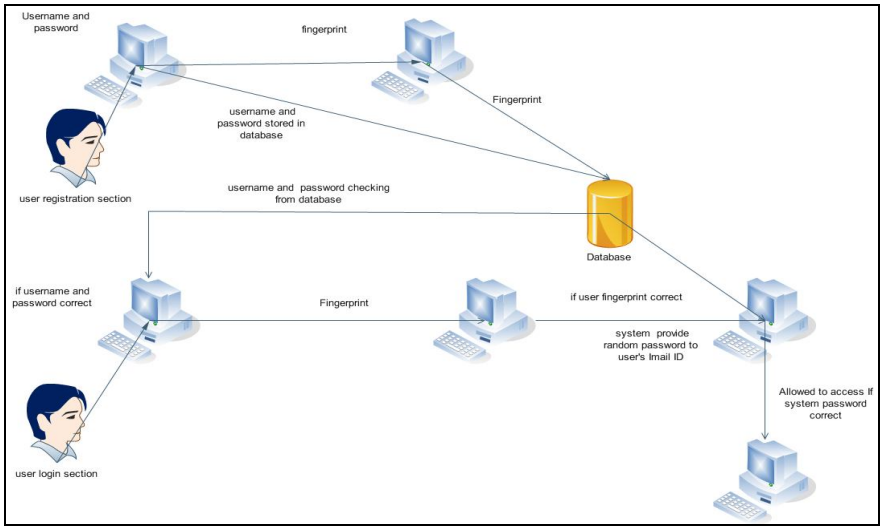


Figure 2. System Architecture

A. Fuzzy Extractor

Fuzzy extractors [8] convert biometric information into random strings that makes it doable to use cryptographical techniques for biometric security. There accustomed encipher and attest users records, with biometric inputs as a key. Codeword is evaluated by polynomial and therefore the secret message is inserted because the coefficients of the polynomial. The polynomial is evaluated for various values of a collection of options of the biometric information. therefore Fuzzy commitment and Fuzzy Vault were per-cursor to Fuzzy extractors. Fuzzy extractor could be a biometric tool to attest a user victimisation its own biometric guide as a key [10]. As fuzzy extractors modify a way to generate robust keys from life science and alternative clangorous information, it applies cryptography paradigms to biometric information which means that (1) build very little assumptions concerning the biometric information (these information comes from form of unwanted soundurces and do not need individual to take advantage of that so it is best to assume the input is unpredictable) (2) Apply cryptographical application techniques to the input. (for that fuzzy extractor translates biometric details into secret code, uniformly random and dependably consistent random string).

B. Metric Space

A topological space may be a set M with a distance perform dis : M×M IR+ =[0,∞] that obeys varied natural properties. One example of topological space is playing metric:M=Fn Fn is over some alphabet F (e.g.,F=) and

distance(W,W') is that the variety of positions during which they take issue. The entrophy calculation can be defined by, the min-entropy $H_\infty(A)$ of a random variable A is $-\log(\max_a \Pr[A=a])$]

Comparison with Previous Protocols

The purpose of this paper is to investigate a systematic approach for the design of secure three-factor authentication. Thus, like almost all generic constructions, our framework does not have advantages from the computational point of view. Nevertheless, it is still affordable for smart-card applications, due to the efficient designs of SCPAP and fuzzy extractor: There are a number of efficient SCPAPs in the literature, and fuzzy extractors can be constructed from error-correcting code and standard pair wise- independent hashing, both of which require only lightweight operations. In addition, the proposed framework enjoys several desirable properties of SCPAP. This saves the time and effort on the design of three-factor authentication with those properties, and more importantly avoids the confusing "broken and improved" process in the existing research on three-factor authentication.

V. SYSTEM IMPLEMENTATION

A. Passive Attacker:

A passive attacker can obtain messages transmitted between the client and the server. However, it cannot interact with the client or the server. Passive attacker with smart card and a passive attacker with passwords it is certainly more desirable that SCPAP is secure against an active attacker with smart card and an active attacker with password.

Type I attacker has the smart card and the biometric characteristics of the client. It is not given the password of that client.

Type II attacker has the password and the biometric characteristics. It is not allowed to obtain the data in the smart card.

Type III attacker has the smart card and the password of the client. It is not given the biometric characteristics of that client. Notice that such an attacker is free to mount any attacks on the (unknown) biometrics, including biometrics faking and attacks on the metadata (related to the biometrics) stored in the smart card.

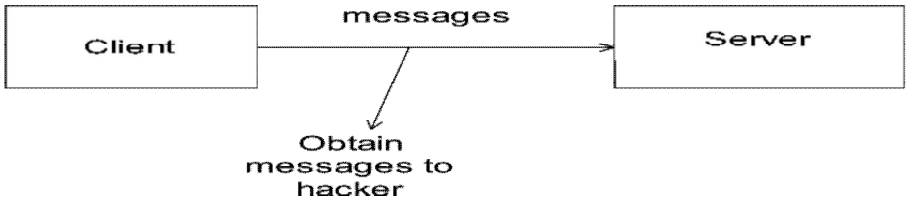
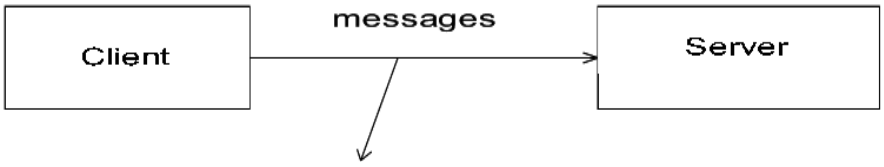


Figure 3. Passive Attack

B. Active Attacker:

An active attacker has the full control of the communication channel. In addition to message eaves-dropping, the attacker can arbitrarily inject, modify, and delete messages in the communication between the client and the server.



Obtain Messages and Editing

Figure 4. Active Attack

C. Forward Security:

Users are identified by their measurable human characteristics, such as fingerprint, voiceprint, and iris scan. Biometric characteristics are believed to be a reliable authentication factor since they provide a potential source of high-entropy information and cannot be easily lost or forgotten.

D. Key Agreement:

When user password and his/her fingerprint correct. The server (denoted by S) generates one system password to user after enter this password system allowed to access and these password kept secret by S.

E. Mutual Authentication:

Mutual Authentication is a security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection.

VI. CONCLUSION

Preserving security and privacy is a challenging issue in distributed systems. This paper makes a step forward in solving this issue by proposing a generic framework for three-factor authentication to protect services and resources from unauthorized use. The authentication is based on IP, smart card, and biometrics. Our framework not only demonstrates how to obtain secure three-factor authentication from two-factor authentication, but also addresses several prominent issues of biometric authentication in distributed systems (e.g., client privacy and error tolerance). The analysis shows that 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). The future work is to fully identify the practical threats on three-factor authentication and develop concrete three-factor authentication protocols with better performances.

REFERENCE

[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] 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
[6] 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.
[7] C.H. Lin and Y.Y. Lai, "A Flexible Biometrics Remote User Authentication Scheme," Computer Standards Interfaces, vol. 27, no. 1, pp. 19-23, Nov. 2004.
[8] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 523-540, 2004.
[9] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," IBM Systems J., vol. 40, no. 3, pp. 614-634, 2001
[10] C.-I. Fan and Y.-H. Lin, "Provably Secure Remote Truly Three- Factor Authentication Scheme with Privacy Protection on Biometrics," IEEE Trans. Information Forensics and Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.

BIOGRAPHY

P.DHIVYA received her B.Tech(IT) Degree from P.A College of Engineering, Pollachi, Tamilnadu, India and pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her fields of Interest are Network Security, Operating systems and Datastructures.

S.MOHANA GOWRI received her B.Tech(IT) Degree from Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India and pursuing M.E Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her fields of Interest are Principles of Compiler Design, Operating systems and Software Engineering.

Dr. N. Saravana Selvam has obtained his Ph.D. in Computer Science and Engineering from Anna University, Chennai in the year 2013. He has obtained both of his Post Graduate degree, M.E.(Computer Science and Engineering) and Graduate degree B.E., (Electronics and Communication Engineering) from Madurai Kamaraj University (Tamilnadu, India). He is currently serving as Professor & Head of Department of Computer Science and Engineering at Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu. During his fifteen years of teaching profession, he shouldered a member of teaching, administrative and societal based assignments. He is a Life Member of ISTE, IAEng and IACSIT. Currently, he is specializing in the area of Network Engineering.

