International Journal of Computer Engineering Science (IJCES)
Volume 6 Issue 4 (2016) ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal http://www.ijces.com/

Invited Paper

NUMERICAL ANALYSIS ON CHEN'S AUTHENTICATION SCHEME FOR MULTI-SERVER ENVIRONMENT

Dhara Joshi[1], Krishna Dalsaniya[2], Chintan Patel[3]

Research Scholar, Department of Computer Engineering, MEFGI, India[1], Prof., Department of Information Technology, MEFGI, India[2], Prof., Department of Computer Engineering, MEFGI, India[3]

dhara.r.joshi@gmail.com[1], krishnadalasaniya10@gmail.com[2], chintan.p592@gmail.com[3]

ABSTRACT

With the fast advancement in the field of network security everything gets the chance to be possible on web. Remote user authentication is an imperative system in the networks framework to check the exactitude of remote user over the public channel. In this authentication procedure, server checks accreditation of the user that user is authentic and legal one or not. For that Server and user commonly confirm each other and make a same session key for encryption of upcoming conversations. There are two types of authentication: Single server and Multi server. To overcome the drawback of single server authentication (remembering id and pswd for accessing each of the server), the concept of Multi server comes, in which user first register with RC, and whatever servers are registerd under RC can be accessed by user by providing single id and pswd for all. Here We review US patent [US 9264425 B1] scheme which is based on Multi server authentication, we provide mathematical analysis of the same with some attacks found on it.

Index Terms— *Remote User Authentication, Multi Server authentication, Network Security, Smart Card, Numerical analysis*

INTRODUCTION

Advances in network communication improved the quality of online available services. Nowadays people prefer online services as it is easy to access without moving from your place and it provides faster accessibility. So the data transfer from user to server and server to user over the public channel and the possibilities of eavesdropping information is more in public channel compared to secure channel. In public channel there are chances of intercept, modify and delete the messages by an attacker. Authentication plans utilizing smart card have increased huge consideration due their appropriateness and ease of use in multi-server environment. So we can also say, by using smart card along with password is helped us to verify the legitimacy of the user.

Actually, an authentication procedure is for checking the correctness of both the user and the server. That simply means, authentication procedure involves mutual authentication between server and user and session key establishment for upcoming conversations. In Multi server environment there are mainly three entities involved: User, Server and RC (Registration Center). In Multi server authentication, user first have to register him/herself with RC, then after user can access any of the server associated with RC by providing same user id and password. So the benefit of this authentication is user doesn't have to remember all the password for accessing all the different service providing server and it is convenient for user.

There are many schemes available which are using smart card. It can be classified into two categories: Two factor and Three factor authentication. In two factor authentication [1-4], password and

smart card are used and in three factor authentication [5-7], password, smart card and biometrics are used. In three factor authentication Biometric properties (fingerprint, retina, face etc.) are involved. The benefit of using biometric properties are like it can't lost, not shared easily, contains unique feature, difficult to guess.

In 2005, Lee et al [1] proposed improved authentication scheme using smart card, which is of two factor authentication. In 2009, Xu et al [2] proposed a scheme in which they assumed that both password and smart card are not stolen at the same time, so they proposed a scheme in which either password or smart card is unknown to the attacker, so attacker does not impersonate the legal user. In 2014, He et al [5] proposed a scheme based on ECC, his scheme overcomes the drawbacks of Yoon et al [7]'s scheme and claimed that his scheme is actually the first correct three factor scheme. In 2015, Li et al [6] proposed a scheme with fuzzy extractor and make comparative study of Yoon et al [7] and Shen et al's scheme.

2. NUMERICAL ANALYSIS OF CHEN'S SCHEME

This Patent [US 9264425 B1] [8] is based on two factor authentication, that means it focuses on password and smart card in Multi Server Environment. This patent explains four various procedures like 1) Registration Procedure, 2) Login Procedure, 3)Verification Procedure and 4) Password Changing Procedure. All the procedures are explains here with numerical calculations. Instead of original hash value, we have assumed hash value for simplicity.

- **Assumed Parameters**

User iDi =1 Password PWi =2 Random No r = 3
Master Key x = 4 Secret no. y = 5 User Nonce Ni = 6
Remote server Identity SIDj = 7 Remote server Nonce Nj = 8 New Password PWinew = 9
New Random No rnew = 10

- **Assumed Hash Values**

h(1) = 21 h(21)=22 h(4||5)=23 h(22||23)=24
h(1||4)=25 h(1||21)=36 h(25)=27 h(5)=8
h(28||6||7)=29 h(25||24||6)=37 h(24||6||7)=38 h(13||24||6)=32
h(13||6||24||7)=33 h(3)=36 h(1||36)=39 h(13||8||24||7)=34
h(13||8||6||24||7)=35

Registration Procedure:

h(r XOR PWi) = h(3 XOR 2)= h(1) = 21

Ri = h(h(r XOR PWi)) = h(h(1)) = h(21) = 22

Mi = h(Ri||h(x||y)) = h(22||h(4||5)) = h(22||23) = 24

Ei = Mi XOR h(r XOR PWi) = 24 XOR 21 = 13

Li = h(IDi||x) = h(1||4) = 25

Wi = Li XOR h(IDi ||h(r XOR PWi)) = 25 XOR h(1||21) = 25 XOR 36 = 61

Fi = h(Li) = h(25) = 27

Login Procedure:

Li = Wi XOR h(IDi ||h(r XOR PWi)) = 61 XOR h(1||21) = 61 XOR 36 = 25

Fi* = h(Li) = h(25) = 27 and Fi*=Fi → 27=27 → Yes User is authenticated

Mi = Ei XOR h(r XOR PWi) = 13 XOR 21 = 24

Ri = h(h(r XOR PWi)) = h(21) = 22

Gij = Ri XOR h(h(y)||Ni||SIDj) = 22 XOR h(28||6||7) = 22 XOR 29 = 11

CIDi = h(r XOR PWi) XOR h(Li||Mi||Ni) = 21 XOR h(25||24||6) = 21 XOR 37 = 48

Hij = Li XOR h(Mi||Ni||SIDj) = 25 XOR h(24||6||7) = 25 XOR 38 = 63

Zi = h(Ei||Mi||Ni) = h(13||24||6) = 32

First Parameter Set m1 = {CIDi,Gij,Hij,Zi,Ni}

Verification Procedure:

Ri = Gij XOR h(h(y)||Ni||SIDj) = 11 XOR h(28||6||7) = 11 XOR 29 = 22

Mi = h(Ri||h(x||y)) = h(22||23) = 24

Li = Hij XOR h(Mi||Ni||SIDj) = 63 XOR h(24||6||7) = 63 XOR 38 = 25

h(r XOR PWi) = CIDi XOR h(Li||Mi||Ni) → 21=48 XOR h(25||24||6) = 48 XOR 37 = 21

Ei = Mi XOR h(r XOR PWi) = 24 XOR 21 = 13

h(Ei||Mi||Ni) ?= Zi → h(13||24||6) = 32 → 32 = 32 → Yes

Generates Nj = 8

Vij = h(Ei||Ni||Mi ||SIDj) = h(13||6||24||7) = 33

Second parameter Set m2 = {Vij,Nj}

h(Ei||Ni||Mi ||SIDj)?= Vij →h(13||6||24||7) = 33 → 33 = 33 → Yes

Vij' = h(Ei ||Nj||Mi||SIDj) = h(13||8||24||7) = 34

Third Parameter Set m3 = {Vij'}

h(Ei ||Nj||Mi||SIDj) ?= Vij' → h(13||8||24||7) =34 → 34=34 →Yes

SK = h(Ei||Ni||Nj||Mi||SIDj) = h(13||6||8||24||7) = 35

Password Change Procedure:

Li = Wi XOR h(IDi ||h(r XOR PWi)) = 61 XOR h(1||21) = 61 XOR 36 = 25

Fi* = h(Li) = h(25) = 27

Fi* ?= Fi → 27 = 27 → Yes

Select PWinew=9 , rnew=10

Winew = Li XOR h(IDi || h(rnew XOR PWinew)) = 25 XOR h(1|| h(10 XOR 9)) = 25 XOR h(1||h(3)) = 25 XOR h(1||36) = 25 XOR 39 = 62

Einew = Ei XOR h(r XOR PWi) XOR h(rnew XOR PWinew) = 13 XOR 21 XOR 36 = 60.

All the phases are mentioned above with the numerical analysis, it shows how the user enters his credential, how it will verify, the overall scenario of scheme cleared with the numerical analysis.

3. REVIEW OF CHEN'S SCHME

Table 1 - Computation Cost Analysis

Phases / Schemes	Registration phase	Login phase	Authentication phase	Password Change phase	Total
Chen's Scheme	10Th + 6Tx + 4TC	11Th + 9Tx + 9TC	14Th + 5Tx + 30TC	7Th + 6Tx + 2TC	42Th + 26Tx + 45Tc

Table 2- Entity Wise Analysis

Entities / Schemes	User	Server	Registration Center	Total
Chen's Scheme	23Th + 16Tx + 21TC	12Th + 5Tx + 20TC	8Th + 5Tx + 4TC	42Th + 26Tx + 45Tc

Where,

Th = Time for one way hash function

Tx = Time for XOR function

Tc = Time for Concat function

4. CONCLUSION

This paper analyzes the Chen's Scheme in mathematical terms. Chen's Scheme is based on two factor Remote user authentication scheme. We analyzed the functions performed in each and every phase of authentication scheme and also analyzed functions performed by every participating entity. In future, we will try to make our proposed scheme which is more robust compared to Chen's scheme.

REFERENCES

[1] N. Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card," *Comput. Stand. Interfaces*, vol. 27, no. 2, pp. 177–180, 2005.

[2] J. Xu, W. T. Zhu, and D. G. Feng, "An improved smart card based password authentication scheme with provable security," *Comput. Stand. Interfaces*, vol. 31, no. 4, pp. 723–728, 2009.

[3] D. Mishra, "Design and Analysis of a Provably Secure Multi-server Authentication Scheme," *Wirel. Pers. Commun.*, vol. 86, no. 3, pp. 1095–1119, 2016.

[4] G. R. Alavalapati, A. K. Das, E.-J. Yoon, and K.-Y. Yoo, "A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography," *IEEE Access*, vol. 4, no. c, pp. 1–1, 2016.

[5] D. He and D. Wang, "Robust Biometrics-Based Authentication Scheme for Multiserver Environment", *IEEE Syst. J.*, pp.1–8, 2014.

[6] X. Li, K. Wang, J.Shen, S. Kumari, F. Wu and Y. Hu, "An enhanced biometrics-based user authentication scheme for multi-server environments in critical system", *J. Ambient Intell. Humaniz. Comput.*, Vol. 7, no. 3, pp.427–443, 2016.

[7] E. J. Yoon and K. Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235–255, 2013

[8] C. T. Chen, "Anonymity authentication method in multi-server environments," U.S. Patent 9264425 B1, Feb 16, 2016

Miss. Dhara R. Joshi received Bachelor of Engineering in Computer Engineering from V.V.P. Engineering College, Rajkot under Gujarat Technological University (GTU), Ahmedabad, India in 2015. She is currently pursing Master of Computer Engineering in Computer Engineering from Marwadi Education Foundation Group of Institution (MEFGI), Rajkot, India under GTU. She is interested in Research on Cryptography, Network Security, Smart card, Three factor Authentication.

Prof. **Krishna Dalsaniya** is a faculty in the Department of Information Technology at Marwadi Education Foundation, Rajkot. Her main area of interest includes MANETs and cluster based protocols for adhoc networks. She has completed M.E. from Marwadi Education Foundation Group of Institutions (MEFGI), Rajkot in 2015.She is professional member of IEEE, IAENG, IACSIT.

Prof. **Chintan Patel** is a faculty in the Department of Computer Engineering at Marwadi Education Foundation, Rajkot. His main area of interest includes Delay Tolerant Network, IOT. He is professional Member of IEEE , CSI , IAENG , IACSIT.