An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments

S.K. hafizul Islam, Ruhul Amin, G.P. Biswas, Mohammad Sabzinejad Farash, Xiong Li, Saru Kumari

PII: S1319-1578(15)00082-8
DOI: http://dx.doi.org/10.1016/j.jksuci.2015.08.002
Reference: JKSUCI 188

To appear in: *Journal of King Saud University - Computer and Information Sciences*

Received Date: 12 January 2015
Revised Date: 22 April 2015
Accepted Date: 27 August 2015

Please cite this article as: hafizul Islam, S.K., Amin, R., Biswas, G.P., Farash, M.S., Li, X., Kumari, S., An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments, *Journal of King Saud University - Computer and Information Sciences* (2015), doi: http://dx.doi.org/10.1016/j.jksuci.2015.08.002

An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments

SK hafizul Islam[a,*], Ruhul Amin[b], G. P. Biswas[b], Mohammad Sabzinejad Farash[c], Xiong Li[d], Saru Kumari[e]

[a,*]*Department of Computer Science and Information Systems, Birla Institute of Technology and Science, Pilani Campus, Rajasthan 333031, India*

[b]*Department of Computer Science and Engineering, Indian School of Mines, Dhanbad-826004, Jharkhand, India*

[c]*Department of Mathematical Sciences and Computer, University of Kharazmi, Tehran,Iran*

[d]*School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China*

[e]*Department of Mathematics, Agra College, Agra, Dr. B. R. A. University, Agra, 282002, Uttar Pradesh, India*

hafi786@gmail.com, amin_ruhul@live.com, gpbiswas@gmail.com, sabzinejad@khu.ac.ir, lixiongzhq@163.com, saryusiirohi@gmail.com

Abstract

In the literature, many three-party authenticated key exchange *(3PAKE)* protocols are put forwarded to established a secure session key between two users with the help of trusted server. The computed session key will ensure secure message exchange between the users over any insecure communication networks. In this paper, we identified some deficiencies in Tan's *3PAKE* protocol and then devised an improved *3PAKE* protocol without symmetric key en/decryption technique for mobile-commerce environments. The proposed scheme is based on the elliptic curve cryptography and one-way cryptographic hash function. In order to proof security validation of the proposed *3PAKE* scheme, we have primarily used widely accepted *AVISPA* software whose results confirm that the same scheme is secure against active and passive attacks including replay and man-in-the-middle attacks. The proposed scheme is not only secure in the *AVISPA* software, but it also secure against relevant numerous security attacks such as man-in-the-middle attack, impersonation attack, parallel attack, key-compromise impersonation attack, etc. In addition, our protocol is designed with low computation cost than other relevant protocols. Therefore, the proposed protocol is more efficient and suitable for practical use than other protocols in mobile-commerce environments.

Keywords: Elliptic curve cryptography, authenticated key exchange protocol, man-in-the-middle attack, mobile-commerce environments.

1. Introduction

The authentication of the communicating clients and the confidentiality of the transmitted message are the primary objectives of network security, when the communication media is a public network. Thus, to achieve these two security goals simultaneously, many *3PAKE* protocols have been introduced. *3PAKE* protocol allows two clients to authenticate each other with the assistance of a trusted server and then computes a secret session key via any public network. The session key can subsequently be used to establish a secure channel between the clients. *3PAKE* protocol is divided into following categories: password-based *3PAKE* [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11] and *3PAKE* protocol using server's public key [12, 13, 14, 15]. In password-based *3PAKE* protocol, two clients share an easy-memorable password with the trusted serve and then generate the session key securely between them with the help of the server. However, most of these protocols are susceptible to undetectable off-line password guessing attack [1, 2], on-line password guessing attack [6, 7, 8, 16, 17], impersonation attack [18], unknown key-share attack [17, 19], etc. In addition, the computation cost and communication load of these protocols are heavy because they have employed the modular exponentiation [2, 3, 4, 6, 8], public/symmetric key encryption/decryption [1, 2, 4, 7, 8] and the transmitted message size is large in each round [1, 3, 4, 8]. Due to the limitations of bandwidth, computation ability and storage space of the low-power mobile devices, the above mentioned protocols are not suitable for mobile-commerce environments. Another type of *3PAKE* protocol used the server's public key and public/symmetric key