{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 179
-
Number 46

Year of Publication: 2018

Authors:

Amar S. Gosavi, Nikhil B. Khandare

10.5120/ijca2018917168

{bibtex}2018917168.bib{/bibtex}

Abstract

This paper highlights the enhancement in security in VoIP by using ECC. The proposed protocol to enhance security comprises of two phases key generation, Secure transmission. Both phases included ECC which can be proved to be practically secure against most of the popular attacks. The security analysis of the proposed protocol is also given and protocol mathematically to be secure.

References

1. Ray, Sangram, G. P. Biswas, and Mou Dasgupta. "Secure multi-purpose mobile-banking using elliptic curve cryptography." Wireless Personal Communications 90.3 (2016): 1331-1354.
2. Ray, Sangram, Rachana Nandan, and G. P. Biswas. "ECC based IKE protocol design for internet applications." Procedia Technology 4 (2012): 522-529.
3. Butcher, David, Xiangyang Li, and Jinhua Guo. "Security challenge and defense in VoIP infrastructures." IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications

and Reviews) 37.6 (2007): 1152-1162.

4. Ray, Sangram, and G. P. Biswas. "Establishment of ECC-based initial secrecy usable for IKE implementation." Proc. of World Congress on Expert Systems (WCE). 2012.

5. Ray, Sangram, Urbi Chatterjee, and G. P. Biswas. "Efficient and Secure Communication Architecture for E-Health System."

6. Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

7. Hankerson, Darrel, Scott Vanstone, and Alfred Menezes. "Elliptic Curve Arithmetic." Guide to Elliptic Curve Cryptography (2004): 75-152.

8. Saxena, Neetesh, Bong Jun Choi, and Rongxing Lu. "Authentication and authorization scheme for various user roles and devices in smart grid." IEEE transactions on information forensics and security 11.5 (2016): 907-921.

9. Braga, A., et al. "Implementation Issues in the Construction of an Application Framework for Secure SMS Messages on Android Smartphones." The 9th Intl. Conf. on Emerging Security Information, Systems and Technologies. 2015.

10. Thomas, Minta, and V. Panchami. "An Encryption Protocol for end-to-end Secure Transmission of SMS." Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on. IEEE, 2015.

11. Saxena, Neetesh, and Narendra S. Chaudhari. "A secure approach for SMS in GSM network." Proceedings of the CUBE International Information Technology Conference. ACM, 2012.

12. Miller, Victor S. "Use of elliptic curves in cryptography." Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1985.

Index Terms

Computer Science Security

Keywords

Elliptic Curve Cryptography(ECC), Mobile Station International Subscriber Directory Number(MSISDN), Voice over Internet Protocol(VoIP), Session Initialization Protocol(SIP), Real-time Transport Protocol(RTP), Elliptic curve Diffie Hellman Problem(ECDHP), Diffie Hellman Problem(DHP).