Weaknesses of SIP Authentication Scheme for Converged VoIP Networks

Q. Pu

***Abstract*—The Session Initiation Protocol (SIP) is commonly used to establish Voice over IP (VoIP) calls. Mostly recently, Yoon et al. proposed an efficient SIP authentication scheme in a converged VoIP network based on elliptic curve cryptosystem (ECC). In this letter, we first demonstrate that it is insecure against off-line password guessing attacks.**

***Index Terms*—Voice over Internet Protocol; Session Initial Protocol; elliptic curve; authentication.**

Voice over Internet Protocol (VoIP) is a fast growing technology believed to be the future replacement for traditional Public Switched Telephone Network (PSTN). There are many protocols used in VoIP signaling, but Session Initiation Protocol (SIP)[1] is one of the widely used ones. It has been chosen by the Third-Generation Partnership Project (3GPP) as the protocol for multimedia application in 3G mobile networks. SIP is an application-layer protocol that is capable of handling all the signalling requirements of a VoIP session, i.e. initiating, managing and terminating voice and video sessions across packet networks. It is analogous to the SS7 protocol[2] in traditional telephony. Security and privacy requirements in a VoIP environment are expected to be equivalent to those in PSTN.

SIP is a text-based client-server protocol. When a user requests to use an SIP service, he needs to be authenticated first before getting the service from the server. In SIP specification [1], the authentication mechanism proposed is HTTP digest based authentication[3]. However, it was found vulnerable to the off-line password guessing attacks and the server spoofing attacks[4]. Yang et al. [4] proposed a SIP authentication scheme but it is not suitable for devices with a low computational power because it works only for Discrete Logarithm (DL) settings and involves in costly exponential computation. Unlike many legacy Time Division Multiplex (TDM) voice networks that are physically separated from data-centric networks, the new VoIP networks allow the convergence of networks. Therefore, the services that are enabled by SIP should be equally applicable to mobile and ubiquitous computing [5]. To meet this goal, based on Yang et al.'s scheme, Yoon et al.[5] quite recently proposed a new SIP authentication scheme in a converged VoIP network using elliptic curve cryptosystem (ECC), which has the well-known advantages with regard to processing and size constraints[6]. In this letter, we demonstrate Yoon et al.'s scheme[5] is still vulnerable to off-line password guessing attacks.

E-mail: monkey_joan@sina.com.cn.

Manuscript completed on April 15, 2010.

The full version is submitted to a journal, which does not allow me to post it here.

REFERENCES

[1] J. Rosenberg et al., SIP: Session Initiation Protocol, IETF RFC 3261, June2002.

[2] International Telecommunications Union. ITU-T Recommendation Q.700: Introduction to CCITT Signalling System 7. Recommendation Q.700, International Telecommunications Union, March 1993.

[3] J. Franks et al., HTTP authentication: basic and digest access authentication, IETF RFC 2617, June (1999).

[4] C. C. Yang et al., Secure authentication scheme for session initiation protocol, Computer & Security (24) (2005) 381-386.

[5] E-J. Yoon, K-Y. Yoo, C. Kim, Y-S. Hong, M. Jo, H-H. Chen, A Secure and Efficient SIP Authentication Scheme for Converged VoIP Networks, Computer Communications (2010), doi: 10.1016/j.comcom. 2010.03.026.

[6] D. Hankerson, A. Menezes, S. Vanstone. Guide to elliptic curve cryptography. Springer-Verlag, New York, USA, 2004.

[7] Y-P. Liao, S-S. Wang, A New Secure Password Authenticated Key Agreement Scheme for SIP using Self-Certified Public Keys on Elliptic curves, Computer Communications (2009), doi: 10.1016/ j.comcom.2009.10.005.

[8] F. Wang and Y. Zhang , A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography, Computer Communication, 31.(2008) 2142-2149.

[9] M. Bellare, D. Pointcheval, P. Rogaway. Authenticated key exchange secure against dictionary attacks. Proc. of EUROCRYPT'2000. Berlin, Germany:Springer-Verlag, 2000: 139-155.

[10] A. Durlanik, I. Sogukpinar, SIP authentication scheme using ECDH, World Enformatika socity Transaction on Engineering computing and technology 8 (2005) 350-353.

[11] L. Wu et al., A new provably secure authentication and key agreement protocol for SIP using ECC, Computer Standard & Interfaces, 31 (2) (2009) 286-291.