P.O.Box 8718, Beijing 100080, China	Journal of Software, Sept. 2006,17(9):1980-1988
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2006 by *Journal of Software*

移动IPv6网络基于身份签名的快速认证方法

田 野, 张玉军, 刘 莹, 李忠诚

田 野1,2, 张玉军1, 刘 莹1,2, 李忠诚1
1(中国科学院 计算技术研究所,北京 100080)
2(中国科学院 研究生院,北京 100049)
作者简介: 田野(1979－),男,重庆涪陵人,博士,主要研究领域为下一代互联网,无线移动网络安全.张玉军(1976－),男,博士,副研究员,主要研究领域为下一代互联网,移动计算.刘莹(1978－),女,博士生,主要研究领域为计算机系统的性能评测,网络性能评测,数据密集性大规模系统的性能评测.李忠诚(1962－),男,博士,研究员,博士生导师,CCF高级会员,主要研究领域为计算机网络,可信计算.
联系人: 田 野 Phn: +86-10-62565533 ext 9228, E-mail: jack_ty@ict.ac.cn, http://www.ict.ac.cn

Received 2005-05-25; Accepted 2005-12-31

Abstract
Access authentication is important to the deployment and application of mobile IPv6 network, and Authentication in handover procedure will reduce handover performance in mobile IPv6 network. However, many studies for the access authentication in mobile IPv6 network ignore the effect of authentication in handover procedure. Furthermore, many certificate-based authentication schemes are not fit for the wireless mobile environment. To solve these drawbacks, a fast mutual authentication mechanism using Identity-based signature in mobile IPv6 network is proposed. The identity-based signature scheme uses NAI (network access identifier) as public key and simplifies the key management in wireless mobile environment, so it can resolve the deficiency in PKI-based authentication mechanism. An effective combination of the fast handover and authentication can minimize the additional load resulting from authentication in mobile procedure. Performance analysis results show that the proposed mechanism is more efficient than other schemes.

Tian Y, Zhang YJ, Liu Y, Li ZC. A fast authentication mechanism using identity based signature in mobile IPv6 network. *Journal of Software*, 2006,17(9):1980-1988.
DOI: 10.1360/jos171980
http://www.jos.org.cn/1000-9825/17/1980.htm

摘要
接入认证对移动IPv6网络的部署和应用至关重要,在切换过程中加入认证过程会影响移动IPv6网络的切换性能.当前,对移动IP网络中接入认证的研究大多没有考虑对切换性能的影响.另外,目前许多双向认证机制都是基于证书的方式来实现,无线移动环境的特殊性使得这种方式并不适合无线移动网络.一种适用于移动IPv6网络的基于身份签名的快速双向认证方法被提了出来.该方法使用NAI(network access identifier)作为公钥,简化了无线移动环境中的密钥管理问题,有效地解决了基于PKI(private key infrastructure)的认证机制的不足.同时,该方法有效结合了快速切换和接入认证过程,降低了移动过程中由于引入接入认证带来的额外开销.最后,通过性能分析证明该方法比其他方法更有效.

基金项目：Supported by the National Natural Science Foundation of China under Grant No.90604014 (国家自然科学基金); the Innovation Funding from the Institute of Computing Technology, the Chinese Academy of Sciences under Grant No.20056350 (中国科学院计算技术研究所创新课题)

References:

[1] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. IETF RFC 3775, 2004.

[2] Koodli R. Fast handovers for mobile IPv6. IETF RFC 4068, 2005.

[3] Le F, Patil B, Perkins CE, Faccin S. Diameter mobile IPv6 application. Internet IETF Draft, draft-le-aaa-diameter-mobileipv6-04, 2004.

[4] Pack S, Choi Y. Pre-Authenticated fast handoff in a public wireless LAN based on IEEE 802.1x model. In: Proc. of the IFIP TC6/WG6.8 Working Conf. on Personal Wireless Communications 2002.

[5] Kim C, Kim YS, Huh EN, Mun Y. Performance improvement in mobile IPv6 using AAA and fast handoff. In: Proc. of the ICCSA 2004. LNCS 3043, Springer-Verlag, 2004. 738?745.

[6] Eronen P, Hiller T, Zorn G. Diameter extensible authentication protocol (EAP) application. IETF RFC 4072, 2005.

[7] Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H. Extensible authentication protocol (EAP). RFC 3748, 2004.

[8] Aboba B, Simon D. PPP EAP TLS authentication protocol. RFC 2716, 1999.

[9] Palekar A, Simon D, Salowey J, Zhou H, Zorn G, Josefsson S. Protected EAP protocol (PEAP) version 2. Internet IETF Draft draft-josefsson-pppext-eap-tls-eap-10, 2004.

[10] Lee BG, Kim HG, Sohn SW, Park KH. Concatenated wireless roaming security association and authentication protocol using ID-based cryptography. In: Proc. of the IEEE VTC 2003-Spring, the 57th IEEE Semiannual, Vol 3. 2003. 1507?1511.

[11] Shamir A. Identity-Base cryptosystems and signature schemes. In: Advances in Cryptology—Crypto'84. LNCS 196, Springer-Verlag, 1984. 47?53.

[12] Boneh D, Franklin M. Identity based encryption from the Weil pairings. In: Advances in Cryptology—Crypto 2001. LNCS 2139, Springer-Verlag, 2001. 213?229.

[13] Hess F. Efficient identity based signature scheme based on pairings. In: Select Areas in Cryptography—SAC 2002. LNCS 2595, Springer-Verlag, 2003. 310?324.

[14] Cha JC, Cheon JH. An identity-based signature from gap Diffie-Hellman groups. In: Proc. of the Public Key Cryptography—PKC 2003. LNCS 2567, Springer-Verlag, 2003. 18?30.

[15] Yi X. An identity-based signature scheme from the Weil pairing. IEEE Communications Letters, 2003,7(2):76?78.

[16] Dupont F, Bretagne E, Bournelle J. AAA for mobile IPv6. Internet IETF Draft draft-dupont-mipv6-aaa-01, 2001.

[17] Barreto PSL, Kim HY, Lynn B, Scott M. Efficient algorithms for pairing-based cryptosystems. In: Advances in Cryptology—Crypto 2002. LNCS 2442, Springer-Verlag, 2002. 354?368.

[18] Scott M. Multiprecision integer and rational arithmetic C/C++ library (MIRACL). 2005. http://indigo.ie/~mscott/

[19] Galbraith SD, Harrison K, Soldera D. Implementing the Tate pairing. In: Proc. of the Algorithm Number Theory Symp.—ANTS V. LNCS 2369, Springer-Verlag, 2002. 324?337.

[20] Libert B, Quisquater JJ. A new identity based signcryption scheme from pairings. In: Proc. of the IEEE Information Theory Workshop (ITW 2003). 2003. 155?158.

[21] Gemmell PS. An introduction to threshold cryptography. CryptoBytes, 1997,2(3):7?12.