P.O.Box 8718, Beijing 100080, China	Journal of Software，Sept. 2005,16(9):1617-1624
E-mail: jos@iscas.ac.cn	ISSN 1000-9825，CODEN RUXUEW，CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2005 by The Editorial Department of *Journal of Software*

一种用于移动IPv6的混合认证方法

陈 炜, 龙 翔, 高小鹏

Full-Text PDF Submission Back

陈 炜, 龙 翔, 高小鹏
(北京航空航天大学 计算机学院,北京 100083)
作者简介: 陈炜(1977－),男,四川自贡人,博士生,主要研究领域为计算机网络安全;龙翔(1963－),男,博士,教授,博士生导师,主要研究领域为计算机体系结构,计算机网络安全;高小鹏(1970－),男,博士,讲师,主要研究领域为计算机体系结构,计算机网络安全.
联系人: 陈 炜 Phn: +86-10-82338059, E-mail: buaa_chen@yahoo.com.cn, http://www.buaa.edu.cn

Received 2004-04-09; Accepted 2004-07-06

Abstract

In the rapidly expanding mobile environment, authenticity of communicating parties is one of the big research challenges and is receiving increasing attention. In the Mobile IPv6 defined by IETF (Internet engineering task force), IPSec (IP security) protocols and RR (return routability) mechanism are used to protect signaling between related communicating nodes, however, how to realize identity authentication has not been efficiently solved. In this paper, the advantages and disadvantages of two authentication techniques?certificate-based authentication and identity-based authentication are analyzed. The scalability of certificate-based means is excellent, but the deployment of PKI (public key infrastructure) and the distribution of certificates make this method costly. On the contrary, identity-based method hurdles the deficiency of certificate-based means, nevertheless the scalability suffers from the share of parameters among related nodes. Then an approach of integrating the two methods mentioned above is proposed to realize a secure and fast authentication with low cost and high scalability. Finally, this hybrid technique is applied in Mobile IPv6 to improve the negotiation of SA (security association), and the security issues are discussed.

Chen W, Long X, Gao XP. A hybrid authentication method used for mobile IPv6. *Journal of Software*, 2005,16(9):1617-1624.
DOI: 10.1360/jos161617
http://www.jos.org.cn/1000-9825/16/1617.htm

摘要

随着移动通信的快速发展,通信实体的身份认证日益成为研究人员面临的巨大挑战.在IETF(Internet engineering task force)的移动IPv6草案中,IPSec(IP security)协议和RR(return routability)机制被用于保护相关通信节点之间的通信信令,但解决通信实体身份认证问题的方法存在一定的不足.首先分析了基于证书和基于身份的认证技术的优点和不足.基于证书的认证方法有很好的可扩展性,但PKI(public key infrastructure)的部署和证书的分发代价较高.反之,由于相关节点需要共享一组系统参数,基于身份的认证方法可扩展性差,但克服了基于证书的认证方法的不足.然后,提出一种同时使用上述两种认证方法的混合认证方法.该混合认证方法为实现安全、快速、低成本和可扩展性好的身份认证提供了一种新的思路.最后,将这种混合技术用于改进移动IPv6安全关联的协商过程,并讨论了该技术的安全性.

基金项目：陈炜(1977－),男,四川自贡人,博士生,主要研究领域为计算机网络安全;龙翔(1963－),男,博士,教授,博士生导师,主要研究领域为计算机体系结构,计算机网络安全;高小鹏(1970－),男,博士,讲师,主要研究领域为计算机体系结构,计算机网络安全.

References:

[1] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. draft-ietf-mobileip-ipv6-24.txt, 2003.

[2] Arkko J, Devarapalli V, Dupont F. Using IPSec to protect mobile IPv6 signaling between mobile nodes and home Agents. draft-ietf-mobileip-mipv6-ha-IPSec-06.txt, 2003.

[3] Nikander P, Aura T, Arkko J, Montenegro G. Mobile IP version 6 route optimization security design background. draft-nikander- mobileip-v6-ro-sec-00, 2003.

[4] Stallings W. Cryptography and Network Security: Principles And Practice. 3rd ed., Upper Saddle River: Prentice Hall, 2003.

[5] Kent S, Atkinson R. Security architecture for the Internet protocol. RFC2401, 1998.

[6] Kent S, Atkinson R. IP encapsulating security payload (ESP). RFC2406, 1998.

[7] Kent S, Atkinson R. IP authentication header. RFC2402, 1998.

[8] Cheng PC. An architecture for the Internet key exchange protocol. IBM Systems Journal, 2001,40(3):721-746.

[9] Kaufman C. Internet key exchange (IKEv2) protocol. draft-ietf-IPSec-ikev2-11.txt, 2003.

[10] Piper D. The Internet IP security domain of interpretation for ISAKMP. RFC2407, 1998.

[11] Maughan D, Schertler M, Schneider M, Turner J. Internet security association and key management protocol (ISAKMP). RFC2408, 1998.

[12] Harkins D, Carrel D. The Internet key exchange (IKE). RFC2409, 1998.

[13] Boneh D, Franklin M. Identity based encryption from the Weil pairing. In: Proc. of the Crypto 2001. LNCS 2139, Springer-Verlag, 2001. 213-229. http://crypto.stanford.edu/~dabo/pubs.html

[14] Cha J, Cheon J. An identity-based signature from gap Diffie-Hellman groups. In: Proc. of the PKC 2003. LNCS 2567. 2003. 18(30. http://www.math.snu.ac.kr/~jhcheon/publication.html

[15] Aboba B, Beadles M. The network access identifier. RFC2486, 1999.