西安电子科技大学学报 2009, 36(4) 714-720 DOI: ISSN: ISSN 1001-2400 CN: 61-1076/TN

本期目录 | 下期目录 | 过刊浏览 | 高级检索 [打印本页] [关闭]

论文

通用可组合安全的Internet密钥交换协议

彭清泉;裴庆祺;杨超;马建峰

(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

摘要：

通过对新一代Internet密钥交换协议(IKEv2)进行分析，指出了其初始交换过程中存在发起者身份暴露和认证失败问题．而在无线接入网络环境下，对发起者身份等敏感信息进行主动保护是十分必要的．提出了一种适用于无线网络环境下的Internet密钥交换协议，该协议让响应者显式地证明自己的真实身份，实现了对发起者主动身份保护．并通过重新构造认证载荷，有效防止了认证失败问题．在通用可组合安全模型下，证明了该协议达到了通用可组合安全．性能分析和仿真实验表明，该协议具有较少的计算量和通信量．

关键词： Internet协议安全 密钥交换 Internet密钥交换协议 可证安全 通用可组合

Universally composable secure Internet key exchange protocol

(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071， China)

(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi'an 710071， China)

Abstract:

The new Internet key exchange protocol (IKEv2) is analyzed, and it is found that the protocol can not achieve active identity protection to the initiator and has the security flaw of authentication failure in its initial exchange. However, it is necessary to protect the identity information to the initiator under the environment of a wireless access network. In this paper, a novel key exchange protocol for the wireless network based on IKEv2 initial exchange is proposed, which realizes active identity protection to the initiator by the responder explicitly proving his true identity, and achieves successful authentication by reconstructing the authentication payload. With the Universally Composable (UC) security model, this new protocol is analyzed in detail, with the analytical results showing that it affords provably UC security. Performance analysis and simulation results show that the proposed protocol has less computation and communication overhead.

Keywords: Internet protocol security key exchange Internet key exchange protocol provably secure universally composable

收稿日期 2008-11-21 修回日期 网络版发布日期 2009-07-01

DOI:

基金项目:

国家自然科学基金资助(60633020,60573036,60803150)

通讯作者: 彭清泉

作者简介:

参考文献：

［1］Harkins D, Carrel D. Internet Key Exchange［EB/OL］.［1998-11-11］. http://tools.ietf.org/rfc/rfc2409.txt.
［2］Kaufman C. Internet Key Exchange (IKEv2) Protocol［EB/OL］.［2005-12-25］. http://tools.ietf.org/rfc/rfc4306.txt.
［3］Krawczyk H. SIGMA: the ‘SIGn-and-Mac' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols［C］//Advances in Cryptology-CRYPTO'2003 LNCS 2729. Berlin: Springer-Verlag,

扩展功能
本文信息
Supporting info
PDF(636KB)
[HTML全文](1KB)
参考文献[PDF]
参考文献
服务与反馈
把本文推荐给朋友
加入我的书架
加入引用管理器
引用本文
Email Alert
文章反馈
浏览反馈信息
本文关键词相关文章
Internet协议安全
密钥交换
Internet密钥交换协议
可证安全
通用可组合
本文作者相关文章
彭清泉
裴庆祺
庞辽军
马建峰
PubMed
Article by Peng,Q.Q
Article by Fei,Q.Q
Article by Pang,L.J
Article by Ma,J.F

2003: 400-425.

［4］Boyd C, Mao W, Paterson K. Deniable Authentication for Internet Protocols［C］//Proceedings of IWSP'03 LNCS 3364. Berlin: Springer-Verlag, 2003: 137-150.

［5］Tschofenig H, Kroeselberg D, Pashalidis A, et al. EAP IKEv2 Method［EB/OL］.［2007-09-27］. http://tools. ietf. org/id/draft-tschofenig-eap-ikev2-15.txt.

［6］Bellare M, Rogaway P. Entity Authentication and Key Distribution［C］//Advances in Cryptology-Crypto'93 LNCS 773. Berlin: Springer-Verlag, 1994: 232-249.

［7］Canetti R, Krawczyk H. Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels［C］//Advances in Cryptology-Eurocrypt'01 LNCS 2045. Berlin: Springer-Verlag, 2001: 453-474.

［8］Canetti R. Universally Composable Security: a New Paradigm for Cryptographic Protocols［EB/OL］.［2005-12-14］. http://eprint.iacr.org/2000/067.ps.

［9］Canetti R, Dodis Y, Pass R, et al. Universally Composable Security with Pre-Existing Setup［C］//Proceedings of the 4th Theory of Cryptology Conference (TCC) LNCS 4392. Berlin: Springer-Verlag, 2007: 61-85.

［10］杨超, 曹春杰, 马建峰. 通用可组合安全的Mesh网络认证协议［J］. 西安电子科技大学学报, 2007, 34 (5): 814-817.

Yang Chao, Cao Chunjie, Ma Jianfeng. Universally Composable Secure Authentication Protocol for Wireless Mesh Networks［J］. Journal of Xidian University, 2007, 34(5):814-817.

［11］Meadows C. Analysis of the Internet Key Exchange Protocol Using the URL Protocol Analyzer［C］//Proceedings of IEEE Symposium on Security and Privacy'99. Los Alamitos: IEEE, 1999: 216-231.

［12］Canetti R, Krawczyk H. Universally Composable Notions of Key Exchange and Secure Channels［C］//Advances in Cryptology-Eurocrypt'02 LNCS 2332. Berlin: Springer-Verlag, 2002: 337-351.

本刊中的类似文章

1. 杨超;曹春杰;马建峰 .通用可组合安全的Mesh网络认证协议[J]. 西安电子科技大学学报, 2007,34(5): 814-817

2. 白国强;蔡勉;肖国镇.一种关于GH-PKD的密码分析方法[J]. 西安电子科技大学学报, 2000,27(6): 740-745

3. 丁勇 .一种用椭圆曲线密码构建的传感网络密钥管理方案[J]. 西安电子科技大学学报, 2008,35(4): 739-742

文章评论

序号	时间	反馈人	邮箱	标题	内容
1	2009-10-21	caragon	caragon@googlemail.com		????????????????????????????????₤????????????????f???ugg ukugg saleugg bootsUGG Bailey Buttonsupra shoesnike dunkMBT Shoes Cheap UGG Cardy UGG Shoes Sale