山东大学学报(工学版) 2013, 43(2) 11-17 DOI: ISSN: 0412-1961 CN: 21-1139

机器学习与数据挖掘

标准模型下基于无证书密钥封装的口令认证密钥交换协议

杨珺涵1,曹天杰1,2

1. 中国矿业大学计算机学院, 江苏 徐州 221116; 2. 中科院研究生院信息安全国家重点实验室, 北京 100039

摘要：

为确保协议的安全性,提出了一种标准模型下可证安全的口令认证密钥交换协议。利用无证书密钥封装机制来传递口令等用户身份验证信息;基于DDH(decision Diffie-Hellman)假设,在标准模型下证明了新协议的安全性。结果显示,该协议是前向安全的,可实现用户间的双向认证,能够有效地抵抗多种攻击。

关键词： 无证书密钥封装 标准模型 交换协议 双向认证 口令认证

Password authenticated key exchange protocol based on certificateless key encapsulation in the standard model

YANG Jun-han1, CAO Tian-jie1,2

1. School of Computer, China University of Mining and Technology, Xuzhou 221116, China;
2. State Key Laboratory of Information Security, Graduate School of the Chinese Academy of Sciences, Beijing 100039, China

Abstract:

To guarantee the security of exchange protocol, a novel password authenticated key exchange protocol without random oracle model was introduced. Clients' identity information was delivered by the certificateless key encapsulation mechanism. The security of the proposed protocol was proved in the standard model based on decision Diffie Hellman (DDH) assumption. Security analysis showed that the provided protocol was forward security and achieved mutual authentication, which could resist multiple attacks.

Keywords: certificateless key encapsulation standard model exchange protocol mutual authentication password authentication

收稿日期 2012-12-20 修回日期 网络版发布日期

DOI:

基金项目:

信息安全国家重点实验室开放基金资助项目;江苏省2011年度普通高校研究生科研创新计划资助项目(CXZZ11-0295)

通讯作者:

作者简介: 杨珺涵(1985-),女,河南开封人,博士研究生,主要研究方向为安全协议与可证明安全.E-mail:yang-junhan@163.com 曹天杰(1967-), 男, 江苏徐州人, 工学博士, 教授, 博导, 主要研究方向为密码学与信息安全.E-mail:cjcao@cumt.edu.cn

作者Email:

PDF Preview

参考文献：

本刊中的类似文章