计算机工程 2011, 37(24) 109-111 DOI: 10.3969/j.issn.1000-3428.2011.24.036 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

改进的Kerberos单点登录协议

邵叶秦 [a]，陈建平 [b]，顾 翔 [b]

(南通大学 a. 现代教育技术中心；b. 计算机科学与技术学院，江苏 南通 226019)

摘要： 现有Kerberos协议易受密码猜测字典攻击和报文重放攻击。为此，提出一个改进的Kerberos单点登录协议。在认证报文中添加随机数并使用动态密钥，防止密码猜测字典攻击，为每个报文添加一个唯一的序列号，防止报文重放攻击。实验结果证明了改进协议的有 效性。

关键词： 单点登录 Kerberos协议 字典攻击 重放攻击

Improved Kerberos Single Sign-on Protocol

SHAO Ye-qin [a], CHEN Jian-ping [b], GU Xiang [b]

(a. Center of Modern Educational Technology; b. School of Computer Science and Technology, Nantong University, Nantong 226019, China)

Abstract: This paper analyzes the problems of the password guessing dictionary attacks and message replay attacks in current Kerberos protocol. An improved single sign-on protocol is proposed. The prevention of password guessing dictionary attacks is achieved by adding a random number and employing a dynamic key in authentication messages. The resistance of replay attacks is realized by marking the message between a client and its corresponding server with a unique serial number. Experimental results show that the improved protocol is valid.

Keywords: single sign-on Kerberos protocol dictionary attack replay attack

收稿日期 2011-07-01 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.036

基金项目:

江苏省高校自然科学基金资助项目(08KJB520009)；江苏省现代教育技术研究“十一五”规划立项课题基金资助项目(2010-R- 16939, 2010-R-16884)

通讯作者:

作者简介: 邵叶秦(1978－)，男，实验师，主研方向：网络安全； 陈建平，教授；顾 翔，副教授

通讯作者E-mail: hnsyk@163.com

参考文献：

[1] Bellovin S, Merritt M. Limitations of the Kerberos Authentication System[J].Computer Communications Review.1990, 20(5):119-

[2] Marin-Lopez R, Pereniguez-Garcia F, Ohba Y, et al. A Kerberized Architecture for Fast Re-authentication in Heterogeneous Wireless Networks[J].Moblile Networks &

Applications.2010, 15(3):392-412
[3] 张小红, 樊中奎. 基于认证协议的Web单点登录优化设计[J].计算机工程.2010, 36(13):146-148 浏览
[4] Dif?e W, Hellman M E. New Directions in Cryptography[J].IEEE Trans. on Information Theory.1976, 22(6):644-654
[6] Neuman C, Yu T, Hartman S, et al. The Kerberos Network Authen- tication Service(V5) [EB/OL]. (2005-07-01). http://www.ietf.org/ rfc/rfc4120.

本刊中的类似文章

1. 王明辉, 王建东.基于口令的三方认证密钥交换协议[J]. 计算机工程, 2012,38(2): 146-147
2. 胡红宇, 李军义.改进的基于口令的群密钥协商协议[J]. 计算机工程, 2011,37(3): 132-133,136
3. 韩崇砚, 张红旗, 张斌, 杨艳.一种抗重放攻击的Web服务认证协议[J]. 计算机工程, 2011,37(21): 91-93
4. 张秋余, 蔡志鹏, 袁占亭.一种安全的单点登录系统口令同步方案[J]. 计算机工程, 2011,37(17): 122-123,142
5. 万灿军;李长云.开放网络环境中面向信任的单点登录[J]. 计算机工程, 2010,36(3): 148-151
6. 陈家琪, 冯俊, 郝妍.无证书密钥协商协议对跨域Kerberos的改进[J]. 计算机工程, 2010,36(20): 150-152
7. 张小红, 樊中奎.基于认证协议的Web单点登录优化设计[J]. 计算机工程, 2010,36(13): 146-148
8. 金伟祖;李平新.基于CAS集群的单点失效问题解决方案[J]. 计算机工程, 2010,36(1): 51-54
9. 胡志刚;曾巧平.基于视觉密码的Kerberos改进协议[J]. 计算机工程, 2009,35(18): 159-160
10. 邱司川;潘 进;刘丽明.IKEv2协议的分析与改进[J]. 计算机工程, 2009,35(15): 126-128

文章评论

反馈人		邮箱地址	
反馈标题		验证码	8412