计算机工程 2012, 38(3) 124-125,129 DOI: 10.3969/j.issn.1000-3428.2012.03.042 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于二次剩余的增强型RFID认证协议

轩秀巍，滕建辅，白 煜

(天津大学电子信息工程学院，天津 300072)

摘要： 分析一种基于二次剩余的认证协议并对其进行改进，提出基于二次剩余的增强型无线射频识别(RFID)安全认证协议。改进协议中的阅读器和标签都产生随机数，并利用Hash函数和二次剩余理论对传输的数据进行加密，从而增强系统的安全性。分析结果表明，该协议可满足RFID系统对安全和隐私的要求，且计算量和存储量较少。

关键词： 无线射频识别 认证协议 Hash函数 二次剩余 假冒攻击 拒绝服务攻击

Enhanced RFID Authentication Protocol Based on Quadratic Residue

XUAN Xiu-wei, TENG Jian-fu, BAI Yu

(School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China)

Abstract: This paper analyzes the scheme proposed by Chen et al and presents an improved protocol based on quadratic residue and Hash function. In the improved protocol, random numbers are generated both by reader and tags. The transmitted information is encrypted by quadratic residue and Hash function. Analysis result demonstrates that the improved protocol not only can resist various attacks and ensure privacy, but also needs less computation and storage in the tags and server compared to other improved scheme.

Keywords: Radio Frequency Identification(RFID) authentication protocol Hash function quadratic residue impersonation attack Denial of Service(DoS) attack

收稿日期 2011-08-08 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.042

基金项目:

天津市自然科学基金资助项目(09JCYBJC00700)

通讯作者:

作者简介: 轩秀巍(1984－)，女，博士研究生，主研方向：无线网络安全，RFID系统；滕建辅，教授、博士生导师；白 煜，讲师、 博士

通讯作者E-mail: xiuweixuan@tju.edu.cn

参考文献：

[1] Miles S B.[J].Sarma S E, Williams J R. RFID Technology and Applications[M]. New York, USA: Cambridge University Press.2008,:-

[4] Chen Yalin, Chou Jue-Sam, Sun Hung-Min. A Novel Mutual- authentication Scheme Based on Quadratic Residues for RFID Systems[J].Computer Networks.2008, 52(12):2373-2380

[5] Yeh Tzu-Chang, Wu Chien-Hung, Tseng Yuh-Min. Improvement of the RFID Authentication Scheme Based on Quadratic Residues[J].Computer Communications.2011, 34(3):337-341

[6] Forouzan B A. 密码学与网络安全[M]. 马振晗, 贾军保, 译. 北京: 清华大学出版社, 2009.

本刊中的类似文章

1. 邹惠, 王建东, 宋超.加权门限多秘密共享方案[J]. 计算机工程, 2012,38(3): 148-149,165
2. 李全.基于改进后退策略的按位二进制防碰撞算法[J]. 计算机工程, 2012,38(3): 280-283
3. 马巧梅, 王尚平.一个超轻量级的RFID认证协议[J]. 计算机工程, 2012,38(2): 151-152
4. 邓宇乔.一种前向安全的代理重签名方案[J]. 计算机工程, 2012,38(2): 144-145
5. 倪霖, 钟辉, 段超.汽车制造生产线上RFID应用模式研究[J]. 计算机工程, 2012,38(04): 224-226
6. 张亚玲, 张超奇, 马巧梅.读写器可移动的RFID高效认证协议[J]. 计算机工程, 2012,38(01): 264-267
7. 方俊, 赵英良.基于RBF神经网络的一次性口令认证方案[J]. 计算机工程, 2011,37(9): 157-159
8. 韩秋君, 丁岳伟.SaaS模式下新型认证方案的设计与分析[J]. 计算机工程, 2011,37(7): 133-135
9. 钟翔, 沈为君.可信计算中基于属性的认证协议改进方案[J]. 计算机工程, 2011,37(6): 118-120
10. 周彦伟, 吴振强, 乔子芮.可信匿名认证协议的研究与设计?[J]. 计算机工程, 2011,37(5): 143-145

文章评论

反馈人		邮箱地址	
反馈标题		验证码	9350
	5		