计算机工程与应用 2008 44 (32): 126-128 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于Key值更新随机Hash锁的RFID隐私保护研究

张 伟, 陶志荣

江南计算技术研究所，江苏 无锡 214083

收稿日期 2007-12-11 修回日期 2008-3-25 网络版发布日期 2008-11-9 接受日期

摘要 在当前已有基于Hash函数增强RFID安全性的方法基础上，利用基于挑战-响应方式互相认证协议最小形式，针对已有的Key值更新随机Hash锁泄漏位置隐私的安全威胁，提出了一种改进的RFID互相认证方法。该方法弥补了已有研究的不足，对标签的响应增加了随机性，可以更好地应对位置隐私泄漏的威胁。

关键词 射频识别 认证协议 随机Hash锁 位置隐私

分类号

Research on Key Value Renewal Random Hash Lock-based RFID privacy enhancement

ZHANG Wei,TAO Zhi-rong

Jiangnan Institute of Computing Technology and Researching，Wuxi，Jiangsu 214083，China

Abstract

On the basis of the existed way of using Key Value Renewal Random Hash Lock to enhance the security of RFID system and by the use of the minimum form of authentication protocol using challenge-response，we proposed an improved RFID authentication protocol to give more protections for the location privacy.Through this approach，the tag’s response becomes random every time.Unauthorized location track will be impossible.

Key words Radio Frequency Identification（RFID） authentication random Hash lock location privacy

DOI: 10.3778/j.issn.1002-8331.2008.32.037

通讯作者 张 伟 prosche_1107@hotmail.com