计算机工程与应用 2008 44 (9): 109-112 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

关于RFID标签的安全策略研究

宋合营, 赵会群

北方工业大学 信息工程学院，北京 100041

收稿日期 2007-7-10 修回日期 2007-9-10 网络版发布日期 2008-3-11 接受日期

摘要 在比较分析现有的RFID标签安全策略基础上，提出一种新型的基于随机更新过程的安全策略。该策略能有效解决RFID标签信息的安全问题，并且不需要高强度运算和加密技术。该策略在每次标签激活时由标签内电路随机改变其数据并向应用系统发出通知。应用系统接收到通知后更新已注册的标签数据。经过多次激活之后，标签新数据与旧数据完全不同，从而防止了标签非法跟踪。介绍不可链接性的定义，并在相关理论的基础上给出详细的分析。

关键词 RFID标签 更新过程 不可链接性

分类号

Study on strategy of security about RFID tags

SONG He-ying,ZHAO Hui-qun

School of Information and Engineering，North China University of Technology，Beijing 100041，China

Abstract

Based on the analysis of previous security strategy about RFID tags，this paper proposes a kind of new security strategy built on random update process which can solve the security problems effectively occurred in the RFID tags，and does not required much computational power and cryptographic techniques.The strategy can change the tag data at random driven by the internal circuitry during each activation and informs the change to the system.Then the system may modify the appropriate entry in its database.After a certain number of activations the new tag data cannot be linked with the original one so as to avoid illegal tracing.Besides，the definition of unlinkability is given，and the detail analysis is provided based on relative theories.

Key words RFID tags update process unlinkability

DOI:

通讯作者 宋合营 songheying@gmail.com