计算机应用 2006 26 (08): 1813-1816 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于Java ME的点到点短信加密应用

杨建强[1,2]

襄樊学院电气信息工程系[1]

收稿日期 2006-2-15 修回日期 2006-4-4 网络版发布日期 2006-8-1 接受日期

摘要 针对短信传输的安全问题，给出了一种基于Java ME的短信加密应用解决方案。该方案用旧密钥加密新密钥来完成密钥的传递和更新，针对短信服务的特点，采用有效措施确保双方能够进行正常的短信通信：若对方未能收到新密钥或其确认短信，则允许重复发送新密钥及其确认短信；若双方在当前密钥生存期的1/3这段时间内未能及时更新密钥，则继续使用旧密钥通信。给出了密钥更新过程中特殊情况的处理方法。从安全性、可靠性方面对这些方法和措施进行了分析，说明了应用中需要注意的事项。

Abstract To keep SMS from interception in transmission, a solution of application of point-to-point SMS encryption based on Java ME was presented. This solution used encrypted SMS to deliver the new key. Considering the characteristics of SMS, effective measures were adopted to ensure that both sides could correctly communicate with each other through SMS.The new key SMS and its confirmation SMS were allowed to be sent again in case they were not received.Both sides would continue using the old key if the triplicate lifetime of the new key had elapsed and the new key was not updated. The means of solving special cases that occurred in the course of key updating were specified. Meanwhile, these measures were also analyzed in terms of security and reliability, and cases in need of attention were pointed out.

关键词 Java ME 短信服务 加密 密钥更新

Key words Java ME;Short Message Service(SMS);encryption;key update

分类号

DOI:

通讯作者:
杨建强 yjq@mail.whut.edu.cn

作者个人主页: 杨建强