计算机应用　2008 28 (04): 910-911　ISSN: 1001-9081　CN: 51-1307/TP

信息安全

一种CA私钥的容侵保护机制

柴争义[1];白浩[1];张浩军[2]

河南工业大学[1]

收稿日期 2007-10-15　修回日期 2007-11-23　网络版发布日期 2008-4-28　接受日期

摘要　保护CA私钥的安全性是整个PKI安全的核心。基于RSA公钥算法和(t, n)门限密码技术，采用分阶段签名方案，确保私钥在任何时候都无需重构。同时，在私钥产生、分发及使用过程中,即使部分系统部件受到攻击,也不会泄漏CA的私钥，CA仍可以正常工作(即系统具有一定的容侵性)。通过VC和Openssl对系统进行了实现。

Abstract　Protecting the Certificate Authority (CA) private key is the key issue of the whole Public Key infrastructure (PKI). Based on Rivest　Shamir　Alleman (RSA) and (t, n) secret shared method, the two phrase signature scheme was used to ensure that the private key never be reconstructed at any time. At the same time, in the process of CA generation, delivery and usage, even if some part of the CA was broken, the CA private key was still safe, and CA still could work. At last, the system was realized by VC and Openssl.

关键词　容侵　认证中心　秘密共享　CA私钥

Key words　intrusion tolerant;Certificate Authority （CA）;secret sharing;CA private key

分类号

DOI:

扩展功能

本文信息

- Supporting info
- PDF(582KB)
- [HTML全文](0KB)
- 参考文献[PDF]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“容侵”的 相关文章
- 本文作者相关文章

· 柴争义
· 白浩
· 张浩军

通讯作者:
柴争义 super_chai@tom.com;chaizhengyi@haut.edu.cn

作者个人主页: 柴争义　白浩　张浩军