计算机工程 2007 33 (09): 182-183 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期 下一期

安全技术

银证系统中数据安全传输的综合防御措施

周克江

(湖南省第一师范学校信息技术系，长沙 410002)

收稿日期 修回日期 网络版发布日期 2007-4-28 接受日期

摘要 2004年8月，在美国召开的国际密码学会议上，来自中国山东的王小云教授宣布成功破译了MD5、HAVAL-128、MD4和RIPEMD算法，并在任何初始值下用2^40次Hash运算给出了SHA-0的碰撞。这意味着目前广泛应用于电子商务、银行系统、证卷系统的安全认证算法——Hash函数分析领域堡垒的轰然倒塌。面对严峻而残酷的现实，依赖于Hash算法的银证系统数据安全传输问题，也就成为人们不得不及时解决的实际问题。该文给出了一种银证系统数据安全传输的综合防御措施。

关键词 SHA-1 MD5 WAP AES WTLS

分类号 TP393.08

DOI:

通讯作者:

作者个人主页: 周克江