西安电子科技大学学报 2007 34 (6): 926-929+934 ISSN: 1001-2400 CN: 61-1076/TN

扩展功能

本文信息

Supporting info

PDF(507KB)

[HTML全文](0KB)

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

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“匿名通信”的相关文章

本文作者相关文章

- 李龙海
-
- 付少锋
- 肖国镇

对一种(t, N-2)弹性Mix Net的密码学分析

李龙海1，2, 付少锋1, 肖国镇2

(1. 西安电子科技大学 计算机学院，陕西 西安 710071；2. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

收稿日期 修回日期 网络版发布日期 2007-11-19 接受日期

摘要 分析了Gao等人提出的(t, N-2)弹性Mix Net方案，发现存在严重安全漏洞. 主动攻击者利用Elgamal算法的可展性构造具有相关性的密文组，然后通过观察对应明文组的相关性获得输入与输出的对应关系，最终破坏Mix Net的秘密性. 两个不同服务器组中的恶意服务器可以相互勾结利用共谋攻击使Mix Net输出错误结果，并以不可忽略的概率逃过验证协议的检验. 分析结果说明Gao的方案不满足(t， N-2)弹性，且基于该Mix Net的电子投票应用也是不安全的.

关键词 匿名通信 Mix Net 共谋攻击

分类号 TN918

Cryptanalysis of a (t, N-2)-resilient Mix Net

LI Long-hai1,2,FU Shao-feng1,XIAO Guo-zhen2

(1. School of Computer Science and Technology, Xidian Univ., Xi′an 710071， China;2. State Key Lab. of Integrated Service Networks, Xidian Univ., Xi′an 710071， China)

Abstract

We analysed Gao et al.’s (t, N-2)-resilient Mix Net scheme and found some serious security flaws in their design. In order to break Mix Net’s privacy, an active attacker can construct a list of ciphertexts with some relativity by utilizing the malleability of the ElGamal encryption scheme, and then observe the corresponding relativity of plaintexts to get the relationship between input and output elements. The malicious servers from two different groups can initiate collusion attacks proposed by this paper to make the Mix Net system output wrong and cheat the verifying protocol with non-negligible probability of success. The result of analysis shows that Gao et al.’s scheme does not satisfy (t, N-2)-resilience and that the electronic voting application based on their Mix Net is also insecure. <BR>

Key words anonymous communication Mix Net collusion attacks

DOI:

通讯作者