计算机应用 2006 26 (05): 1055-1057 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

Ku-Chien远程身份认证方案的安全性分析

张利华

北京航空航天大学电子信息学院

收稿日期 2005-11-7 修回日期 2005-12-14 网络版发布日期 接受日期

摘要 Ku－Chien远程身份认证方案是一种使用智能卡、低开销、实用的口令认证方案。本文分析了Ku－Chien方案的安全性，指出了Ku－Chien方案的安全缺陷：不能抵御并行会话攻击和伪造主机攻击。分析了产生安全缺陷的原因：登陆阶段用户计算出的秘密信息和认证阶段远程主机计算出的秘密信息具有类似的结构。最后，利用口令更改计数器，给出了一种改进的口令认证方案。该方案允许用户自主选择并更改口令，实现了双向认证；能够抵御重放攻击、内部攻击，具备强安全修复性；能够抵御并行会话攻击和伪造远程主机攻击。

Abstract Ku-Chien proposed a low cost and practical solution to password authentication using smart cards. the security of Ku-Chien's scheme is analyzed in this paper. it still has some weaknesses: it cannot resist parallel session attack; it also cannot withstand masquerading remote system attack. The reason of faults is due to the similar structure of secure information of login phase and authentication phase. Based on password changing counter, an enhanced password authentication scheme with better security strength is presented. This scheme has many merits: freely choosing and changing passwords; providing mutual authentication; resisting message replaying attack and insider attack; having strong security reparability; withstanding parallel session attack and remote system attack.

关键词 身份认证,口令,智能卡,安全分析

Key words authentication,password,smart cards,security analysis

分类号

DOI:

通讯作者:
张利华 lh_zhang@ee.buaa.edu.cn

作者个人主页: 张利华