计算机工程与应用 2007 43 (22): 120-121 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

一种针对TPM的抗重放攻击方案

周雅洁，陈 萍，张晶伟，关焕梅

武汉大学 计算中心，武汉 430072

收稿日期 修回日期 网络版发布日期 2007-7-20 接受日期

摘要 可信平台模块（Trusted Platform Module，TPM）是可信计算技术的核心。可信计算平台需要TPM的可信测量能力、可信存储能力和可信报告能力，向用户证实平台是可信的。然而当前人们主要关心TPM的实现以及其上的应用开发，却很少讨论TPM本身的安全性。这样一方面很难使人们相信TPM本身是安全的，另一方面也不能很好的将TPM应用到安全领域中。对用户和TPM交互时所遵循的重要协议——对象无关授权协议OIAP进行分析，证明了该协议会受到重放攻击并提出了相应的解决方案。

关键词 可信平台模块 对象无关授权协议 重放攻击

分类号

Solution of anti-replay attack in TPM

ZHOU Ya-jie，CHEN Ping，ZHANG Jing-wei，GUAN Huan-mei

Computer Center，Wuhan University，Wuhan 430072，China

Abstract

The Trusted Platform Module（TPM） is the core of the the trusted computing technology.The trusted computing platforms need to be verified trustful by functionality of identity，measurement，protected storage of the TPM.However，the people take more care of the realization and exploitation of the TPM than the security of the TPM itself and this hampers the application of the TPM in the security technology.We prove that the object-independent authorization protocol is exposed to replay attack and propose a countermeasure to avoid this attack.

Key words Trusted Platform Module（TPM） object-independent authorization protocol replay attack

DOI:

通讯作者 周雅洁 E-mail：yjzhou@whu.edu.cn