计算机工程与应用 2008 44 (21): 69-71 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

Sun等两个完美前向安全E-mail协议分析与改进

苏仁旺

浙江工商大学 统计与数学学院，杭州 310035

收稿日期 2008-1-28 修回日期 2008-3-18 网络版发布日期 2008-7-17 接受日期

摘要 2005年，Sun等提出了两个完美前向安全的E-mail协议，尽管从短密钥保护的有效性来看这两个协议是安全的，但它们都不能提供密文的认证性，如果一个主动攻击者拦截或修改密文，则E-mail接受者会收到一个错误的明文。为了克服此缺点，对此两个协议作了改进，使得改进后的协议具有认证性，从而有更好的安全性和实用性。

关键词 完美前向安全 机密性 协议 认证性 E-mail

分类号

Cryptanalysis and improvements on Sun et al.’s e-mail protocols with perfect forward secrecy

SU Ren-wang

College of Statistics and Mathematics，Zhejiang Gongshang University，Hangzhou 310035，China

Abstract

In 2005，Sun et al have proposed two secure e-mail protocols with perfect forward secrecy.Although these two protocols seem to be secure from the protective efficiency of the short-term key，yet neither of them has considered the authentication of the delivering ciphertext.If an outside attacker intercepts and modifies a delivering ciphertext，the e-mail receiver will have to accept a false plaintext.To overcome this flaw，in this paper we will make improvements on Sun et al.’s protocols such that the improved protocols have authentication，better security and practicality.

Key words perfect forward secrecy confidentiality protocol authentication e-mail

DOI: 10.3778/j.issn.1002-8331.2008.21.018

通讯作者 苏仁旺 srwang123@sina.com