计算机工程　2009 35 (22): 150-152　ISSN: 1000-3428　CN: 31-1289/TP　首页　当期目录　上一期

安全技术

PMAC模式的消息伪造攻击

刘彦宾1，韦永壮2,3

(1. 遵义师范学院计算机科学系，遵义 563002；2. 桂林电子科技大学信息与通信学院，桂林 541004；3. 西安电子科技大学计算机网络与信息安全教育部重点实验室，西安 710071)

收稿日期　修回日期　网络版发布日期　接受日期

摘要　针对PMAC工作模式，利用模式局部差分恒等原理，给出一种消息伪造攻击方法，指出新攻击下PMAC工作模式是脆弱的。利用该方法可以成功地进行消息和其MAC的伪造。与已有的攻击方法相比，该新攻击所需的碰撞条件更为宽松，并使得实施攻击更为灵活、有效。

关键词　分组密码；消息认证码；PMAC模式；消息伪造攻击

分类号　TN918.1

DOI:

通讯作者:

作者个人主页: 刘彦宾1;韦永壮2;3