通信学报

Journal on Communications

主管单位：中国科学技

主办单位：中国通信学

李龙海,付少锋,苏锐丹,车向泉.对一种混合结构洋葱路由方案的密码学分析[J].通信学报,2013,(4):88~98

对一种混合结构洋葱路由方案的密码学分析

Cryptanalysis of a hybrid-structured onion routing scheme

投稿时间： 2012-01-13

DOI： 10.3969/j.issn.1 000-436x.2013.04.010

中文关键词: 匿名通信 洋葱路由 通用重加密 混合结构

英文关键词: anonymous communication onion routing universal re-encryption hybrid structure

基金项目:国家自然科学基金资助项目(61101142)；中央高校基本科研基金资助项目(K50510030012)

作者	单位
李龙海，付少锋，苏锐丹，车向泉	西安电子科技大学 计算机学院，陕西 西安 710071

摘要点击次数: **553**

全文下载次数: **357**

中文摘要:

对时金桥等提出的混合结构洋葱路由方案进行了分析，发现存在的安全漏洞。第一个漏洞来源于其密码学报文结构的可展性。攻击者能够利用该漏洞改变洋葱消息的路由或在其入标签以追踪消息路由。另一个漏洞表现在匿名转发服务器容易遭受选择密文攻击。展示了3种不同的能够以较低代价破坏发送者和接收者不可关联性的攻击过程。为了避免所提到击，提出了能够利用反向调查捕获恶意节点的修正方案。

英文摘要:

SHI Jin-qiao et al’ s hybrid-structured onion routing scheme was analysed and some security flaws were found in their design. The first flaw was derived from the malleability of its cryptogra message format which could be exploited by attackers to redirect an onion message or embed tags into it for tracing its routing path. The second flaw was the vulnerability of relay servers to chose ciphertext attack. Three different attacks were presented that each broke the sender-receiver unlinkability entirely at a relatively low cost. To evade these attacks, a modified scheme was also prop which could capture malicious nodes by using upstream investigation.

查看全文 查看/发表评论 下载PDF阅读器

关闭