计算机工程与应用 2008 44 (5): 158-161 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于SPIN的IKEv2协议高效模型检测

吴 昌, 肖美华

南昌大学 信息工程学院，南昌 330031

收稿日期 2007-6-5 修回日期 2007-8-20 网络版发布日期 2008-1-31 接受日期

摘要 论文先简单介绍了互联网密钥交换协议IKEv2，然后利用著名的模型检测工具SPIN对其进行了建模和分析。在建模的过程中，作者发现现有的建模方法很难对结构复杂的协议IKEv2进行建模，而且用现有的建模方法建立的模型可读性差、自动化程度不高，验证效率也比较低，因此现有的建模方法只适用于对简单协议进行建模。针对这些不足之处，提出了一种程序可读性、自动化程度及验证效率均较好的建模方法，而且这种建模方法特别适合对复杂的安全协议进行建模。最后利用SPIN对IKEv2协议的模型进行了验证，发现IKEv2协议不能抵御主动攻击，并给出了两个攻击序列图。针对IKEv2协议不能保护发起者身份的缺陷，提出了自己的一种改进意见。

关键词 IKEv2 模型检测 SPIN Promela IP隧道

分类号

Effective model checking of IKEv2 protocol based on SPIN

WU Chang,XIAO Mei-hua

College of Computer Information and Engineering，Nanchang University，Nanchang 330031，China

Abstract

This paper first gives a simple introduction of the Internet Key Exchange Protocol IKEv2，then conducts a modeling and analysis of the protocol by using the famous model checking tool SPIN.The author finds the existing modeling method hardly applicable because of the highly complex structure of IKEv2 protocol，and that it can only be used for some simple protocols due to its poor readability，low automatization and verification efficiency.Thus the paper proposes another method of modeling which overcomes all the above mentioned disadvantages and which is particularly useful for complicated protocols.At last，the verification of the IKEv2 protocol model based on SPIN shows that this protocol is incapable of resisting initiative attack.Based on this discovery，two charts are given describing the attack and a personal view is presented to improve IKEv2 protocol’s ability to protect the identity of initiator.

Key words IKEv2 model checking SPIN Promela IP Tunnel

DOI:

通讯作者 吴 昌