<<网络安全协议>>

图书基本信息

书名：<<网络安全协议>>

13位ISBN编号：9787302279037

10位ISBN编号：7302279039

出版时间：2012-10

出版时间：清华大学出版社

作者：赖英旭，杨震，刘静　编著

页数：237

字数：370000

<<网络安全协议>>

内容概要

《网络安全协议》比较全面地介绍了网络安全协议的关键技术和主要应用模式。
特别对vpn网络的特点、分类及应用模式等方面进行了比较深入的分析和探讨。

《网络安全协议》对数据链路层安全协议、网络层安全协议、传输层安全协议、会话层安全协议和应用层安全协议等方面进行了比较深入的分析，并介绍了各层协议的安全缺陷、易受到的攻击以及在相应层协议中所增强的安全机制。
在网络安全协议应用方面，本书重点阐述了3种常见的vpn网络应用模式，并比较详细地介绍了vpn网络的工作原理和配置。

《网络安全协议》通俗易懂，注重可操作性和实用性。
通过对典型vpn网络应用模式案例的讲解，使读者能够举一反三。
本书可作为广大计算机用户、计算机安全技术人员的技术参考书，特别是可用做信息安全、计算机与其他信息学科本科生的教材，也可用做计算机信息安全职业培训的教材。

<<网络安全协议>>

作者简介

赖英旭

女，博士，1973年6月出生，现为北京工业大学计算机学院信息安全系副教授。

2003年到北京工业大学信息安全系任教后，一直从事网络安全、可信计算等方面的科研工作，主持和参与了多个国家及省部级科研项目，包括北京市高等学校人才强教深化计划、北京市教委面上项目、国家自然科学基金等。

相关研究成果已申请专利5项，获授权2项，国内学报、国际会议论文多篇。

现为中国密码学会会员、中国计算机学会会员。

<<网络安全协议>>

书籍目录

章节摘录

版权页： 插图： 3.7 IPSec协议安全性分析 IPSec协议的安全特性基本上解决了前述8种网络攻击行为，但一些特殊的攻击还是能够实现。
1.利用IPSec进行重放攻击 防重放工作原理是通过丢弃序列号早于本地滑动窗口中最小的序列号分组来实现：在一对一通信时，首先双方建立SA。
然后由发送方生成每个数据包的序号，为防重放做好必要的准备。
最后通过接收方利用滑动窗口技术来实现防重放服务。
发送方对输出包的处理分为4个步骤：查询SA、生成序号、计算ICV和分片。
发送方的计数器在建立SA时被初始化为0。
发送方不断增加该SA的序号，并向“序号”字段中插入新的值。
这样，用给定的SA所发送的第一个数据包的序号就为1。
发送方通过检查，以保证计数器在插入新值前没有出现循环。
如果计数器出现循环，那么发送方就会建立一个新的SA和密钥。
接收方对输入包的处理分为4个步骤：重组、查询SA、校验序号和校验ICV。
建立SA时，接收方的包计数器初始化为0，然后每接收一个数据包，都要首先检查序号是否出现重复。
接收过程主要应用了滑动窗口技术。
在这里，窗口大小的最小值为32，默认值为64，接收方也可以选择其他值。
窗口的最大值表示当前SA下有效的最大序号，窗El的最小值表示当前SA下有效的最小序号，两者之差为窗口大小。
而数据包“序号”字段中的值如果小于窗口容器的最小值，该包就会被丢弃。
只有数据包序列号大于窗口最小值，才会继续检查其ICV，如果ICV检查通过，就更新滑动窗口，即下一个可以接受的序列号范围，继续接收后面的数据包。
因为序号比目前滑动窗口的最小序号还小的包是已经接受过的包，即为重放的包，而这些包又都被丢弃，这样就防止了重放攻击。
IPSec协议的一些重要特性如下。
（1）在安全关联中，不包括源地址，每个安全关联（SA）都由一个3元组＜SPI，目标地址，所用协议>唯一标识。
其中，安全参数索引用于区别具有相同目标地址和相同协议的不同SA；目标地址表示该SA下接收方的IP地址，当前只能是单播地址；所用协议是指选用了AH还是ESP，二者必须并且只能选择其一。
但是安全关联中并不包括任何与源地址有关的信息。
（2）对特殊ICMP报文建立SA后，不检查源地址是否匹配，虽然安全关联中不包括任何与源地址有关的信息，但是在建立SA之后，本地策略会确定一个SA选择器，还要检查数据包中的源地址与SA选择器是否匹配，这样才可保证源验证。
但是对由路由器生成的受AH或ESP保护的ICMP错误消息而言，只能为这种消息报文建立隧道模式的SA，而且此时并不检查这种ICMP报文中的源地址是否与SA选择器相匹配。
（3）当建立SA时，通信双方的序号计数器都要被始化为0。
利用以上特性，下面两种方法可以实现对IPSec的重放。
（1）简单实现。
在多对一的通信中，让多个发送方都与接收方之间建立同一个SA，就可以简单实现对IPSec的重放。
假设A和B是发送方，C为接收方，其工作过程如下：A与C建立SA，双方计数器归0，正常收发若干报文，C的计数器达到某一值；B截获到A发送给C的若干报文，这些报文具有一定的序号；B与C建立同一个SA，此时C的计数器将再次归零；B把所截获的报文重放给C，这些报文的序号就会落在C的滑动接收窗口的内部或右侧，而不会被认为是重放的报文。
但通过源验证，就可以知道是谁在进行重放攻击。
（2）利用ICMP错误报文实现。

如果利用对ICMP错误报文，在隧道模式下建立SA来实现对IPsec保护之下报文的重放，就无法通过源验证确定谁在进行重放。
因为在对这种特殊的ICMP报文进行处理时，并不检查源地址，也就无法实现源验证。
具体过程如下：捕获在隧道模式下建立SA的ICMP错误报文；与攻击目标之间建立相同的SA；重放数据包，对目标实施重放攻击。

<<网络安全协议>>

版权说明