第一图书网, tushu007.com

<<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：9787811142266

10位ISBN编号：7811142260

出版时间：2008-3

出版时间：秦科、张小松、 郝玉洁 电子科技大学出版社 (2008-03出版)

作者：秦科，等 编

页数：240

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

《网络安全协议》详细讲述了网络安全协议中的基本理论、网络安全协议的主流类型以及网络安全协议的研究分析方法等。

书籍目录

第1章 绪论 1.1 基本概念 1.2 信息安全的目标 1.3 Dolev-Yao攻击模型 1.4 关于本书的约定 第2章 密码学基础 2.1 密码编码学 2.1.1 基本概念 2.1.2 古典密码 2.1.3 一次一密 2.1.4 分组密码 2.1.5 非对称密钥算法 2.2 密码分析学 2.3 信息隐藏 2.4 随机数与伪随机数 2.4.1 伪随机数与伪随机序列 2.4.2 随机数生成器 2.4.3 随机数的随机性检验 2.4.4 随机序列的随机性检验 2.5 哈希函数 2.5.1 基本概念 2.5.2 基本分类 2.5.3 基本性质 2.5.4 具体方案 2.5.5 使用模式 2.6 数字签名 2.6.1 基本概念 2.6.2 数字签名算法 小结 第3章 认证协议及密钥建立协议 3.1 身份认证 3.1.1 基本概念 3.1.2 基于口令的认证 3.1.3 基于单向函数的一次性口令 3.1.4 智能卡认证 3.1.5 基于生物特征的认证 3.1.6 双因素认证 3.1.7 挑战-应答机制（Challenge／Response） 3.1.8 利用带密钥单向函数的挑战-响应机制 3.1.9 利用公开密钥的挑战-响应机制 3.1.10 挑战-响应机制的标准化 3.1.11 利用挑战-响应机制的双向认证 3.1.12 RADIUS认证协议 3.1.13 利用时间戳的认证机制 3.2 认证协议以及密钥建立协议 3.2.1 密钥建立协议的性质 3.2.2 大嘴青蛙协议（Wide Mouth Frog） 3.2.3 Yahalom协议 3.2.4 NSSK协议 3.2.5 Otway-Rees协议 3.2.6 Kerberos 3.2.7 Neuman-Stubblebine协议 3.2.8 NSPK协议 3.2.9 DASS协议 3.2.10 Denning-Sacco协议 3.2.11 Woo-Lam协议 3.2.12 X.509强认证协议 3.3 密钥协商协议 3.3.1 DH密钥协商协议 3.3.2 单步Elgamal密钥协商 3.3.3 认证的密钥交换协议2（AKEP2） 3.3.4 Shamir无密钥协议 3.3.5 工作站对工作站协议（STS） 3.3.6 MTI两步密钥协商协议 3.3.7 会议密钥生成协议 3.4 秘密共享 3.4.1 Shamir门限方案 3.4.2 Asmuth-Bloom门限方案 3.4.3 其他门限方案 小结 第4章 特殊数字签名与阈下信道 4.1 特殊数字签名 4.1.1 不可抵赖的数字签名 4.1.2 指定的确认人签名 4.1.3 代理签名 4.1.4 团体签名 4.1.5 失败-终止签名 4.1.6 批签名 4.1.7 多重签名 4.1.8 同时签名 4.1.9 盲签名 4.2 阈下信道 4.2.1 Ong-Schnorr-Shamir方案 4.2.2 Elgamal 4.2.3 ESIGN 4.2.4 其他阈下信道 小结 第5章 其他安全协议 5.1 零知识协议 5.1.1 基本概念 5.1.2 零知识洞穴协议 5.1.3 H图零知识协议 5.1.4 零知识身份识别协议 5.2 智力扑克协议 5.3 公平抛币协议 5.3.1 有可信第三方的简单抛币协议 5.3.2 利用单向函数的简单抛币协议 5.3.3 利用非对称密钥体制的抛币协议 5.4 不经意传输协议 5.5 非否认协议 小结 第6章 IPsec协议 6.1 IPsec体系结构 6.2 安全联盟 6.2.1 SA的创建 6.2.2 SA的删除 6.2.3 安全参数索引（SPI） 6.2.4 SADB参数 6.3 安全策略 6.4 验证头（AH） 6.4.1.AH头信息 6.4.2 AH工作模式 6.4.3 AH处理过程 6.5 封装安全载荷ESP 6.5.1 ESP头信息 6.5.2 ESP工作模式 6.6 ISAKMP 6.6.1 ISAKMP报文头部格式 6.6.2 ISAKMP载荷 6.6.3 ISAKMP的交换阶段 6.7 IKE 6.7.1 主模式 6.7.2 野蛮模式 6.7.3 快速模式 6.7.4 新组模式 小结 第7章 Kerberos协议与X.509证书 7.1 Kerberos 7.1.1 Kerberos概况 7.1.2 Kerberos的票据 7.1.3 Kerberos的域 7.1.4 Kerberos的工作过程 7.1.5 Kerberos的假设 7.2 X.509证书及认证框架 7.2.1 X.509数字证书格式 7.2.2 CA与数字证书的管理 7.2.3 证书的撤销 7.2.4 X.509认证方式 小结 第8章 SET与SSL协议 第9章 安全协议分析与设计 第10章 信息标准及规范 附录 参考文献

章节摘录

版权页： 插图： 这种协议是比较简单的密钥建立协议，该协议的安全性依赖于KDC的绝对安全性。
如果攻击者破坏了KDC，便得到了KDC与每个用户共享的所有秘密密钥，从而可以阅读Alice与Bob的所有通信内容。
此外，该协议存在着单点失效问题（Single Point Failure）。
KDC可能成为整个系统的瓶颈，因为KDC必须参与每一次密钥建立，如果KDC出现故障，整个系统的通信就会中断。
Alice和Bob也可以使用基于非对称密钥体制进行会话密钥的建立，并用协商的会话密钥加密会话内容。
在一些实际的实现中，Alice和Bob签了名的公开密钥可在数据库中获得。
这使得密钥交换协议更容易，即使Bob从来没有听说过Alice，Alice也能够把信息安全地发送给Bob。
Alice与Bob的密钥建立过程如下：（1）Alice从KDC得到Bob的公开密钥。
（2）Alice产生随机会话密钥，用Bob的公开密钥加密它，然后将它传给Bob。
（3）Bob用他的私钥解密Alice的信息。
（4）他们两人用同一会话密钥对他们的通信进行加密。
这是一种比较简单的基于非对称密钥密码的密钥建立协议，但是，该协议有一个重大的缺陷：不能抵御中间人攻击。
为了抵御中间人攻击，可以采用数字签名技术。
KDC对Alice和Bob的公开密钥签名。
签名的密钥包括一个已签名的所有权证书。
当Alice和Bob收到密钥时，他们每人都能验证KDC的签名。
那么，他们就知道公开密钥到底是属于谁的，密钥的交换就能进行了。
由于攻击者不知道Alice和Bob的私钥，因此攻击者不能进行冒充。
同样攻击者也不能用他自己的公开密钥代替Alice或Bob的公开密钥，因为Alice和Bob的公开密钥使用了KDC的签名，攻击者是不能冒充KDC进行签名的，除非他知道KDC的私钥。
这种协议也需要KDC的参与，但KDC遭受损害的风险比第一种协议小。
如果攻击者竭尽全力地获取了KDC的私钥，这只能导致攻击者可以冒充KDC用这个新的私钥对Alice和Bob的密钥进行签名，但不会让他对任何会话密钥解密，或者读取任何报文。
如果攻击者真的获取了KDC的私钥，那么他就能够冒充Alice和Bob，拦截Alice和Bob的会话内容并解读。
因此，保持KDC的安全是非常重要的。
上面两个密钥建立协议是非常简单的协议。
虽然它们有各自的缺点，但很多协议都是在这两种协议的基础上发展而来的，例如下面将要介绍的一些著名协议。
需要说明的是，这些协议也是不完善的，存在着很多问题。
由于缺乏一套强有力的协议设计工具，要设计一条完美的协议是很困难的事。

编辑推荐

《普通高等学校信息安全"十一五"规划教材:网络安全协议》既可作为计算机、通信、信息安全专业本科生或硕士生的参考教材，也可供从事相关领域的科研和工程技术人员参考。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com