<<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

<<网络安全协议>>

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。

<<网络安全协议>>

书籍目录

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。

<<网络安全协议>>

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。

<<网络安全协议>>

版权说明