<<安全协议分析与设计>>

图书基本信息

书名：<<安全协议分析与设计>>

13位ISBN编号：9787115220028

10位ISBN编号：7115220026

出版时间：2010-11

出版时间：人民邮电出版社

作者：卫剑钒，陈钟　编著

页数：156

前言

随着网络技术的应用与发展，各种安全需求日渐迫切和复杂，安全协议作为网络安全的基础部分，其安全性直接影响着各种网络应用的安全。
针对安全协议的攻击是复杂多样的，如果协议设计缺乏经验或考虑不周，很容易遭受攻击而导致秘密信息的泄露。
最为典型的例子是1978年由密码学专家Needham和Schroeder设计的NSSK协议和NSPK协议，其中，NSSK协议在发布3年后被Denning和Sacco发现一个攻击，该攻击通过重放消息使得合法用户接受一个过期的密钥；而NSPK协议在被多种方法“证明”是安全的情况下，17年后，被Lowe采用CSP模型和FDR。
工具成功地找到一个漏洞，攻击者可以使其中一个主体相信它正在与另一合法主体通信，而实际上是在与攻击者通信。
此外，CCITT X.509草案中的认证协议、SSI。
早期版本、IKE协议以及其他很多安全协议，都或多或少被发现存在缺陷。
通常认为，如果一个问题有如下的特点，就有必要使用形式化方法：问题尺度适中；有大量的处理经验；问题本身可被表述清楚；能清楚描述影响问题的有关环境因素的假设；问题是非直觉的、不易发现的；问题的危害是严重的。
安全协议正好全都满足这些特点，故而，采用形式化方法研究安全协议是很适合的，也是很必要的。
近20年来，安全协议的形式化研究一直是一个热点，各种形式化方法和技术不断涌现，主要有逻辑推理类方法、模型检测类方法、理论证明类方法这3大类。
但大量事实表明，人们对安全协议的了解，虽然经历近20年的研究，仍然停留在初步的阶段。
本书中提及的安全协议，主要是指认证协议（Authentication Protocol）和密钥建立协议（Key Establishment Protocol），这是安全协议中最主要和最关键的部分。
虽然选举协议、公平交易协议、群组通信协议、匿名通信协议、非否认协议、电子商务协议等从广义上讲也是安全协议，但它们都建立在认证协议和密钥建立协议的基础上。

<<安全协议分析与设计>>

内容概要

本书系统地介绍了安全协议(主要是认证协议和密钥建立协议)的基本概念、攻击方法、分析方法和设计方法。
全书分为7章，从安全协议的基本概念和协议记法出发，先介绍安全协议分析采用的假设和对攻击者能力的界定，接着对一些经典的安全协议及其攻击展开分析，然后对逻辑类分析方法、模型检测分析方法和定理证明类分析方法分别进行介绍，并讲述了安全协议的设计原则和设计方法，最后对一些实际使用中的具体安全协议进行讲解和分析。
本书注重知识的系统性和覆盖面的广泛性，部分内容有一定的理论深度。
本书可作为信息安全、计算机、通信专业的本科生和研究生教材，也可作为相关专业的研究人员和工程技术人员的参考书。

<<安全协议分析与设计>>

书籍目录

章节摘录

插图：

编辑推荐

《安全协议分析与设计》使用通俗易懂的语言，力图使一个没有信息安全基础的初学者，在较短时间内，可以较为容易地掌握安全协议相关的基本理论和方法；在章节安排上由浅入深，在读者对协议和攻击有了初步的认识之后，才开始介绍难度较大的理论分析方法和设计方法；《安全协议分析与设计》注重逻辑性和实践性，在通读之后，会对安全协议有一个较为全面的把握，并可具备初步的协议分析能力和设计能力。
透彻易懂的概念诠释,深入浅出的协议分析和讲解,涵盖大量常见安全协议的分析和设计。

<<安全协议分析与设计>>

版权说明