<<网络安全协议的形式化分析与验证>>

图书基本信息

书名：<<网络安全协议的形式化分析与验证>>

13位ISBN编号：9787111297260

10位ISBN编号：7111297261

出版时间：1970-1

出版时间：李建华、张爱新、薛质、 等 机械工业出版社 (2010-04出版)

作者：李建华 等 著

页数：214

前言

随着以Internet为代表的信息化浪潮席卷全球，信息技术的应用日益普及和广泛，但Internet所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全也提出了更高的要求，信息安全已成为关系到国家安全和经济发展的重大战略问题。
安全协议（也称密码协议）是一个分布式算法，它规定了两个或多个通信主体在一次通信过程中必须执行的一系列步骤。
安全协议利用密码技术实现开放网络环境下的安全通信，达到信息安全的目的，广泛地应用于身份认证、接入控制、密钥分配、电子商务等领域。
因此，安全协议作为实现信息安全的基础，其自身的安全性间.题已成为安全研究的重要内容。
由于网络安全协议的重要性，从1978年第一个安全协议（Needham-Schroeder协议）诞生以来，人们对它的分析和设计就一直没有停止过，也做出了卓有成效的工作。
.最初，人们基于经验和单纯的软件测试，采用攻击检验方法来分析其安全性。
由于安全协议往往运行在复杂的、不安全的网络环境中，同时，新的攻击方法层出不穷，产生的错误很难完全由人工识别。
因此，很难保证对协议安全性分析的准确性。
人们一致认为，必须采用形式化的方法和工具来分析密码协议的安全性，即采用数学或逻辑模型，通过有效的程序来分析系统及其条件，以此确定一种在系统满足条件情况下所得的证明是否正确的数学理论和方法。
形式化方法在网络安全协议分析中的作用主要体现在：①能使分析概念清晰；②能发现协议设计中的错误；③能证明协议的正确性；④能作为安全协议自动化分析、设计技术的理论指导。
最先提出采用形式化方法分析密码协议的是Needham和Schroeder。
然而，在这一领域中第一项探索性的工作是由Dolev和Yao完成的，随后由Dolev、Even和Karp在20世纪70年代后期和80年代初开发了一系列多项式时间算法来确定密码协议的安全性。
自1983年Dolev.Yao形式化模型提出以后，密码协议形式化方法的研究有了长足的发展，到目前为止已形成了两大流派，并且出现了理论融合的趋势。
一种流派称为计算流派，它基于一个详细的计算模型，安全性推理通常是通过构造一个“归约为矛盾”类型的证明得到的，这里的“矛盾”是指计算复杂性领域中一个困难问题的有效解。
随机预言机模型（ROM）、作为该流派的代表，对于分析密码算法的安全性有着公认的、广泛的应用。
另一流派称为逻辑符号流派，它基于简单而有效的形式化语言方法，对公理的应用可以基于逻辑证明、定理证明或状态搜索技术。
本书着重讨论逻辑符号流派的主要S-作。
目前，形式化理论在安全协议验证中的应用主要集中在形式化分析、形式化设计及自动化工具开发3个方面。
同时，随着密码技术的不断发展和安全应用需求的不断扩大。
安全协议的结构也越来越复杂化，这些都对现有的形式化协议分析技术提出了很大的挑战。

内容概要

《网络安全协议的形式化分析与验证》概述了形式化技术在网络安全协议分析、验证中的主要应用原理及现状；在此基础上详细地叙述了网络安全协议的形式化分析技术、形式化设计技术;最后重点介绍了目前的形式化分析技术对当前典型应用环境下复杂、实用网络安全协议的分析成果，包括IPSec协议、SSL协议、电子商务协议、移动通信安全协议及群组通信安全协议等。

信息安全是关系到国家安全和经济发展的重大战略问题，至关重要。
安全协议作为实现信息安全的基础，其自身的安全性问题已成为安全研究的重要内容。
目前，针对安全协议的安全性验证已形成了许多不同的流派、理论和方法。
《网络安全协议的形式化分析与验证》理论与应用并重，深入浅出地介绍了各类形式化分析技术的基本原理及其在大型复杂安全协议分析中的实际应用。

《网络安全协议的形式化分析与验证》可作为信息安全专业高年级本科生教材，也可作为高等学校电子信息类、计算机类等相关专业的参考书。

<<网络安全协议的形式化分析与验证>>

书籍目录

章节摘录

插图：6.密码系统缺陷密码系统缺陷是指协议中使用的密码算法不合适或对密码算法的实现不当，而导致协议不能完全满足所要求安全需求而产生的缺陷。
应该指出的是，随着攻击手段与技术的不断翻新，以上缺陷并不能涵盖网络安全协议在实际应用中的所有可能出现的漏洞。
一个安全协议在运行过程中，假如有攻击者存在，并且没有被系统或者诚实角色所察觉，同时攻击者在参与协议运行过程中并没有利用任何密码学上的漏洞，那么我们就说该协议存在设计上的漏洞。
本书只讨论由于协议设计漏洞所产生的协议缺陷。
1.1.3 安全协议的攻击手段针对信息系统的攻击主要有两种形式，即被动窃听和主动分析。
前者是通过非法搭线窃听，截取通信信息后进行分析以获得机密内容或敏感信息：后者指对通信信息进行非法修改，包括插入非法信息、重放陈旧信息、删除通信消息和修改通信消息等。
一个被动攻击者可以在线窃听敏感信息，而一个主动攻击者则可截获数据包并对其进行任意的修改，甚至可以伪装成通信主体，欺骗诚实主体与其进行非法的通信。
实现这些攻击的方法很多，比如可以对系统采用的密码系统进行数学分析、旁路攻击以破解机密信息并对系统进行即时监听等；另外，还有一类很重要的攻击方式，那就是利用协议本身的漏洞攻击信息系统，采用这种攻击方式不需要很大的计算量，往往成为黑客的主要攻击手段。
下面简要介绍一些由于协议设计漏洞而产生的针对安全协议的攻击方式。
1.中间人攻击在中间人攻击中，攻击者将自己伪装于两个通信主体之间进行通信，甚至可以冒充任一主体的身份向对方发送消息。
考虑以下协议：在用户Alice、Bob不知道对方私钥的情况下，用户Alice希望采用公钥密码技术向Bob发送一条秘密消息，协议使用：RSA公钥加密算法。

编辑推荐

《网络安全协议的形式化分析与验证》：安全协议及其形式化技术的基本概念、原理和方法,安全协议的形式化分析方法,安全协议的形式化设计技术,形式化技术在复杂安全协议分析中的典型应用。

版权说明