信息安全技术丛书

安全协议模型与设计

刘天华　朱宏峰　著

科学出版社

信息安全技术丛书

安全协议模型与设计

刘天华　朱宏峰　著

科学出版社
北京

内 容 简 介

本书介绍了安全协议的整体结构、设计流程与分析方法。第1～3章介绍了安全协议的基本概念以及采用的数学知识与密码工具，第4章介绍了安全协议的可证明理论，第5～7章探讨了不同环境下安全协议的设计与分析。针对现有安全协议中出现的问题，提出了一些针对常见协议的改进协议，经过性能测试具有较好的实用性。

本书适合普通高等院校信息安全方向的教师、研究生以及从事安全协议等研究方向的科研人员阅读参考。

图书在版编目(CIP)数据

安全协议模型与设计/刘天华，朱宏峰著. —北京：科学出版社，2012
(信息安全技术丛书)
ISBN 978-7-03-034326-0

I. ①安… II. ①刘…②朱… III. ①计算机网络-安全技术-通信协议
IV. ①TP393.08

中国版本图书馆CIP数据核字(2012)第096450号

责任编辑：任 静 / 责任校对：李 影
责任印制：张 倩 / 封面设计：迷底书装

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
中国科学院印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2012年8月第 一 版 开本：B5(720×1000)
2012年8月第一次印刷 印张：13 3/4
字数：277 000
定价：48.00元
(如有印装质量问题，我社负责调换)

作者简介

刘天华(1966～),男,博士,沈阳师范大学教授,硕士生导师。中国计算机学会YOCSEF沈阳副主席,中国电子学会高级会员。长期从事计算机网络、网络安全、信息安全、嵌入式系统、教育信息技术方面的教学及科学研究工作。主持及参与国家自然科学基金、省自然科学基金等纵向和横向项目10项,在国内外重要学术刊物以及学术会议上发表论文30余篇,撰写和主编专业著作和教材12部,获省部级有关奖励3项。

朱宏峰(1978～),男,博士,沈阳师范大学副教授。研究方向为分布式网络、网络工程、计算机系统结构、网络安全等。先后参加省级科研项目6项,在国内外重要学术刊物及学术会议上发表学术论文30余篇,曾获得辽宁省自然科学学术成果奖一等奖,辽宁省自然科学学术成果奖论文类三等奖,出版教材2部。

前　言

安全协议(secure protocol)是建立在密码体制基础上的一种高互通协议，运行在计算机通信网或分布式系统中，为有安全需求的各方提供一系列步骤，借助密码算法实现密钥分配、身份认证、信息保密以及安全地完成电子交易等。安全协议由参与协议的主体、与主体之间交换消息的事件序列组成，并要达到一定的设计目标。由于安全协议在网络和分布式系统中提供各种各样的安全服务，有着大量的应用，起到“桥梁”的作用，因此在信息系统中占据重要位置。

安全协议的研究历经近 30 年，取得了丰硕的成果，特别是近些年的发展十分迅猛。本书不强调多、全、杂，而强调少、精、新，在计算密码协议中引入可证明安全、可组合安全以及自由共谋安全等新模式，拓展了安全协议的研究思路。

本书从内容上可分为基础理论、模型与设计 两部分，并在模型与设计部分中穿插作者多年的研究成果。本书在基础理论部分中按照“全书架构→数学基础→基本工具→设计方法与模型”结构逐步进行阐述。在模型与设计部分中按照“领域架构→研究现状→问题提出→问题解决→未来研究”进行编写，在每一小节中提出问题并给出相应的解决方案。各章内容既相互联系又相对独立，紧紧围绕解决安全协议中针对不同服务环境的设计思想、设计方法、所采用的模型以及折中效率与安全等实际问题，并给出安全性证明、通信量和计算量等参数的横向对比结果，使读者对安全协议领域的研究有深刻的认识，从而起到抛砖引玉的作用。

本书是作者多年来的研究成果的回顾和总结，真诚希望从事相关研究的同仁们为本书提出宝贵意见，以便共同推动这一领域研究的进一步发展。

本书在写作过程中得到了辽宁省自然科学基金(项目编号：20102202，201102201)、辽宁省百千万人才项目(项目编号：2011921046)的资助，在此表示衷心的感谢。

作　者

2011 年 12 月于沈阳

目　录

第1章 引　言

没有基础可以盖一间简陋的小屋，却不能建成永久的大厦。

——Oded Goldreich

学习和钻研，要注意两个不良，一个是营养不良，没有一定的文史基础，没有科学理论上的准备，没有第一手资料的收集，搞出来的东西，不是面黄肌瘦，就是畸形发展；二是消化不良，对于书本知识，无论古人今人或某个权威的学说，要深入钻研，过细咀嚼，独立思考，切忌囫囵吞枣，人云亦云，随波逐流，粗枝大叶，浅尝辄止。

——马寅初

1.1 安全协议的基本概念

信息安全保障是一个没有尽头的任务，信息社会存在一天，信息安全的需求就会存在一天。攻防共生共存，魔高一尺，道高一丈，反之亦然。完美的理论并不一定能够解决信息安全的实际问题，理论到实践是一个系统工程，而安全协议的模型与设计是这个工程的核心，是承载信息安全体系的脊梁，是应用选择理论的载体：设计安全协议不单单基于技术本身，还要考虑应用的成本、代价和用户体验。

1.1.1 定义

所谓协议(protocol)[1]，就是两个或两个以上的参与者为完成某项特定任务而采取的一系列步骤。这包含三层含义：第一，协议自始至终是有序的过程，每一个步骤必须依次执行。在前一步没有执行完之前，后面的步骤不可能执行。第二，协议至少需要两个参与者。一个人可以通过执行一系列的步骤来完成某项任务，但这不构成协议。第三，通过执行协议必须能够完成某项任务。

协议还有其他特点：①协议中的每人都必须了解协议，并且预先知道所要完成的所有步骤。②协议中的每人都必须同意遵循它。③协议必须是不模糊的，每一步必须

明确定义，并且不会引起误解。④协议必须是完整的，对每种可能的情况必须规定具体的动作。

安全协议(security protocol)是建立在某种体系(密码体制、量子禀性)基础上且提供安全服务的一种交互通信协议，它运行在计算机通信网络或分布式系统中，借助特定算法来达到密钥分配、身份认证等目的。安全协议的密码基础是由三类基石构造的，如图 1.1 所示。

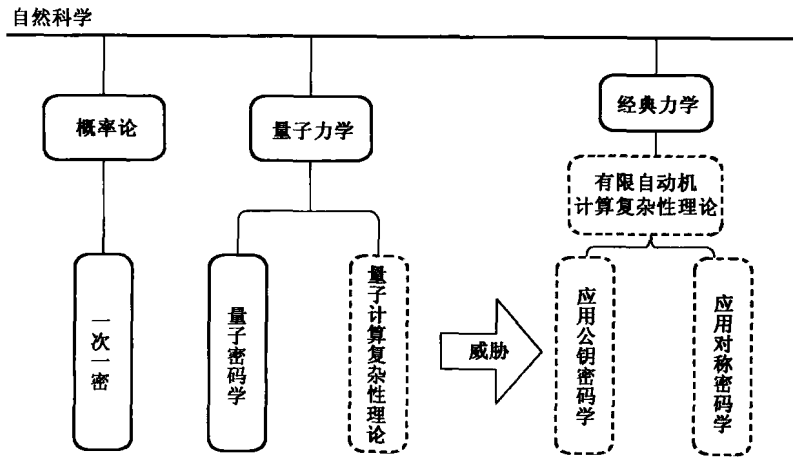


图 1.1 三类密码学的理论基础

安全协议的通信系统基本安全模型如图 1.2 所示。

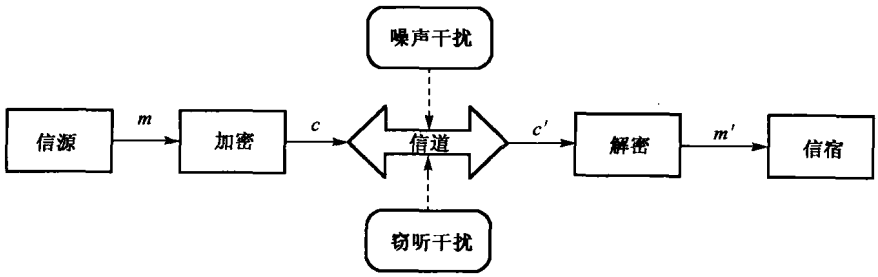


图 1.2 通信系统的安全模型

安全协议的参与者可能是可以信任的实体，也可能是攻击者和完全不信任的实体。安全协议的目标不仅仅是实现信息的加密传输，参与协议的各方还可能希望通过分享部分秘密来计算某个值、生成某个随机序列、向对方表明自己的身份或签订某个合同等。解决这些安全问题就需要在协议中采用密码技术，因为它们是防止或检测非法用户对网络进行窃听和欺骗攻击的关键技术措施。对于采用了这些技术的安全协

议来说，如果非法用户不可能从协议中获得比协议自身所体现的更多的、有用的信息，那么就可以说协议是安全的。安全协议中采用了多种不同的密码体制，其层次结构如表1.1所示。

表1.1 安全协议层次结构

层 次	计算密码	量子密码
高级协议	身份认证、不可否认、群签名	量子密钥分发、博弈量子密钥协商
基本协议	数字签名、零知识、秘密共享	量子签名
基本算法	对称加密、非对称加密、Hash函数	量子Hash函数
基础	核心断言、数论、抽象代数、数学难题	不可克隆、真随机性

从表1.1可看出，安全协议构建在数学或量子信息科学基础和基本算法之上，并且往往涉及秘密共享、加密、签名、承诺、零知识证明等许多基础协议，因此安全协议的设计往往庞大而复杂，设计满足各种安全性质的安全协议成为一项具有挑战性的研究工作。

当前存在着大量的实现不同安全服务的安全协议，其中最常用的基本安全协议按照其完成的功能可分类起名，如电子支付协议、分布式环境下的身份鉴别协议、不可否认协议、密钥协商协议等。

1.1.2 目的

在日常生活中，几乎所有的事情都有非正式的协议：电话订货、玩扑克、选举中投票，人们都知道怎样使用它们，而且它们也很有效。随着信息技术的高速发展，将这些现实的协议功能转化为数字，从而在计算机世界中实现是顺理成章的事情。越来越多的人通过计算机网络交流代替面对面的交流，计算机需要正式的协议来完成人们不用考虑就能做的事情，虽然方便大众，但并不都容易实现：如果你从一个城市迁移到另一个城市，可能会发现投票亭与你以前使用的完全不同，你会很容易去适应它，但计算机就不那么灵活了。

许多面对面的协议依靠人的现场存在来保证公平和安全。你会交给陌生人一叠现金去为你买食品吗？如果你没有看到他洗牌和发牌，你愿意和他玩扑克吗？如果没有匿名的保证，你会将秘密投票寄给政府吗？

那种假设使用计算机网络的人都是诚实的想法，是天真的。天真的想法还有假设计算机网络的管理员是诚实的，假设计算机网络的设计者是诚实的。当然，绝大多数人是诚实的，但是不诚实的少数人可能招致很多损害。通过规定协议，可以查出不诚实者企图欺骗的把戏，还可开发挫败这些欺骗者的协议。

除了规定协议的行为外，协议还根据完成某一任务的机理，抽象出完成此任务的

过程。由于基本底层通信协议是相同的，对于高层的安全协议是一个黑盒子，所以我们专注设计协议流程与分析，而不用受限于具体的实现上。

1.1.3 游戏角色

为了帮助说明协议，通常选出几个人作为助手：Alice 和 Bob 是开始的两个人。他们将完成所有的两人协议。按规定，由 Alice 发起所有协议，Bob 响应。如果协议需要第三或第四人，Carol 和 Dave 将扮演这些角色。由其他人扮演的专门配角，参见表 1.2。

表 1.2 剧中人与角色

剧中人	角 色
Alice	所有协议中的第一个参加者
Bob	所有协议中的第二个参加者
Carol	在三、四方协议中的参加者
Dave	在四方协议中的参加者
Eve	窃听者
Mallory	恶意的主动攻击者
Trent	值得信赖的仲裁者
Walter	监察人：在某些协议中保护 Alice 和 Bob
Peggy	证明人
Victor	验证者

1.2 安全协议的分类

1.2.1 第一种分类方法

根据两点特质——认证和密钥交换，首先将协议分为三大基本类，再按照参与方数量分为两方安全协议和多方安全协议两大类，如表 1.3～表 1.5 所示[2]。

表 1.3 基本安全协议

协 议 名 称	协 议 描 述
认证协议	提供给一个参与方关于其通信对方身份的一定确信度
密钥交换协议	在参与协议的两个或者多个实体之间建立共享的秘密
认证及密钥交换协议	为身份已经被确认的参与方建立一个共享秘密

表 1.4 两方安全协议

协 议 名 称	协 议 描 述
零知识协议	指一个参与方希望另一个参与方相信某种声称的正确性，同时不泄露任何额外信息

续表

协议名称	协议描述
承诺协议	产生保密的承诺和公开秘密(解诺)的安全协议
掷币协议	指两个参与方试图协商一位或多位信息,即使某个参与方试图使输出趋近于某一个值,该位信息也仍然能够来自于一个均匀分布
不经意传输	指某个参与方传送两个消息,另一个参与方提供一位信息,协议结束后消息的提供者不知道接收者获得了哪个消息,消息的接收者不知道另一个消息的内容
可否认认证	能够使接收者鉴别消息的来源,但是接收者不能向第三方证明消息来源,接收者通过"仿真"发送者和接收者之间的消息实现可否认认证。签名认证机制不具有可否认性

表 1.5 多方安全协议

协议名称	协议描述
基本多方协议	如秘密共享、可验证秘密共享、匿名处理、多方 Ping-Pong 协议等
电子选举	根据各种上下文综合考虑协议的正确性、公正性、私密性和可否认性
电子商务	解决传输过程中的公平性以及以某种可接受的方式来处理争议,还包括结果的公平发布
数据库交叉查询	多个数据库可以联合起来进行数据查询。除查询的结果之外,数据库中的其他数据将保持私有状态
匿名信任系统	参与者匿名多身份问题
路由协议	安全路由协议是一类特殊的安全多方计算协议

1.2.2 第二种分类方法

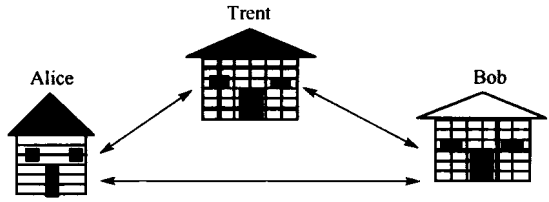
根据可信第三方参与协议与否可以将安全协议分为仲裁协议、裁决协议和自动执行协议三类。三类协议的结构类型如图 1.3 所示。

1)仲裁协议

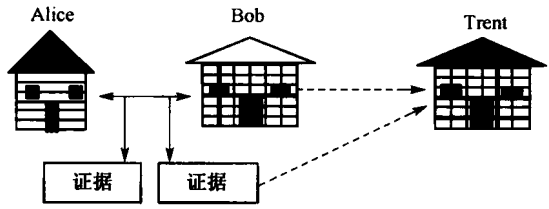
仲裁者是在完成协议的过程中,值得信任的公正的第三方(图 1.3(a)),"公正"意味着仲裁者在协议中没有既得利益,对参与协议的任何人也没有特别的利害关系。"值得信任"表示协议中的所有人都接受这一事实,即仲裁者说的都是真实的,他做的是正确的,并且他将完成协议中涉及他的部分。仲裁者能帮助互不信任的双方完成协议。

在现实社会中,律师经常作为仲裁者。实例:Alice 要卖汽车给不认识的 Bob。Bob 想用支票付账,但 Alice 不知道支票的真假。在 Alice 将车子转给 Bob 前,她必须查清支票的真伪。同样,Bob 也并不相信 Alice,就像 Alice 不相信 Bob 一样,在没有获得所有权前,也不愿将支票交与 Alice,这时就需要双方都信任的律师。在律师的帮助下,Alice 和 Bob 能够用下面的协议保证互不欺骗:①Alice 将车的所有权交给律师。

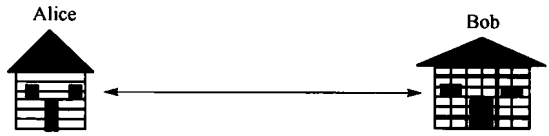
②Bob 将支票交给 Alice。③Alice 在银行兑现支票。④在等到支票鉴别无误能够兑现的时间之后，律师将车的所有权交给 Bob。如果在规定的时间内支票不能兑现，Alice将证据出示给律师，律师将车的所有权和钥匙交还给 Alice。



(a) 仲裁协议



(b) 裁决协议



(c) 自动执行的协议

图 1.3 协议类型

在这个协议中，Alice 相信律师不会将车的所有权交给 Bob，除非支票已经兑现；如果支票不能兑现，律师会把车的所有权交还给 Alice。而 Bob 相信律师有车的所有权，在支票兑现后，将会把车主权和钥匙交给他。而律师并不关心支票是否兑现，不管在什么情况下，他只做那些他应该做的事，因为不管在哪种情况下，他都有报酬。在这个例子中，律师起着担保代理作用。律师也作为遗嘱和合同谈判的仲裁人，还作为各种股票交易中买方和卖方之间的仲裁人。

仲裁人的概念与人类社会一样悠久。总是有那么一些人——统治者、牧师等，他们有公平处理事情的权威。在我们的社会中，仲裁者总是有一定社会地位和声望的人。而背叛公众的信任是很危险的事情。例如，视担保为儿戏的律师几乎肯定会被开

除出律师界。现实世界里并不总是如此美好,但它的确是理想的。这种思想可以转化到计算机世界中,但数字世界中的仲裁者面临下面几个问题。

合同-签字协议可以归纳为下面形式。

非仲裁子协议(每次都执行):①Alice 和 Bob 谈判合同的条款;②Alice 签署合同;③Bob 签署合同。

裁决子协议(仅在有争议时执行):①Alice 和 Bob 出现在法官面前;②Alice 提出她的证据;③Bob 也提出他的证据;④法官根据证据裁决。

2)裁决协议

由于雇用仲裁者代价高昂,仲裁协议可以分成两个低级的子协议。一个是非仲裁子协议,这个子协议是想要完成协议的各方每次都必须执行的;另一个是仲裁子协议,仅在例外的情况下执行,即有争议时才执行,这种特殊的仲裁者叫做裁决人(参见图 1.3(b))。

裁决人也是公正的和可信的第三方。他不像仲裁者,并不直接参与每一个协议。只有为了确定协议是否被公平地执行,才将他请来。

法官是职业的裁决者。法官不像公证人,仅在有争议时才需要他出场,Alice 和 Bob 可以在没有法官的情况下订立合同。除非他们中有一个人把另一人拖到法院,否则法官决不会看到合同。合同-签字协议的特点如下。

(1)真实性:如果你知道对方是谁,并能见到他的面,就很容易找到和相信中立的第三方。互相怀疑的双方很可能也怀疑在网络中并不露面的仲裁者。

(2)费用:计算机网络必须负担仲裁者的费用。

(3)分布延迟性(无全局时钟):在任何仲裁协议中都有延迟的特性。

(4)单点失效:仲裁者必须处理每一笔交易。任何一个协议在大范围执行时,仲裁者是潜在的瓶颈。增加仲裁者的数目能缓解这个问题,但费用将会增加。

(5)单点安全:由于在网络中每人都必须相信仲裁者,对试图破坏网络的人来说,仲裁者便是一个易受攻击的弱点。

裁决者和仲裁之间的不同是裁决者并不总是必需的。如果有争议,法官被请来裁决。如果没有争议,就没有必要请法官。在好的裁决协议中,裁决者还能确定欺骗人的身份。裁决协议是为了发现欺骗,而不是为了阻止欺骗。裁决协议起到了防止和阻碍欺骗的作用。

3)自动执行协议

自动执行协议是协议中最好的。协议本身就保证了公平性(图 1.3(c))。不需要仲裁者来完成协议,也不需要裁决者来解决争端。协议的构成本身不可能发生任何争端。如果协议中的一方试图欺骗,其他各方马上就能发觉并且停止执行协议。无论欺

骗方想通过欺骗来得到什么，他都不能如愿以偿。最好让每个协议都能自动执行。不幸的是，在所有情形下，没有一个是自动执行的协议。

1.2.3 其他方法

根据 ISO 的七层参考模型，又可以将安全协议分成高层协议和低层协议；按照安全协议中采用密钥算法的种类，又可以分成双钥（或公钥）协议、单钥（或私钥）协议或混合协议等；依据安全协议应用的环境，又可以分为互联网中的安全协议、卫星通信网络中的安全协议、无线传感器网络中的安全协议、RFID 系统中的安全协议等；对于参与实体间拥有预共享长期密钥的安全协议，根据长期密钥的安全强度，又可以分为基于口令的安全协议和一般的预共享密钥安全协议。除此之外，还可以从其他角度出发对安全协议进行分类。

1.3 安全协议的模型与分析方法

安全协议的分析方法主要分为计算机安全方法、计算复杂性方法和物理禀性方法，如图 1.4 所示。攻击者能力模型及安全协议形式化设计与分析方法如表 1.6 和表 1.7所示。

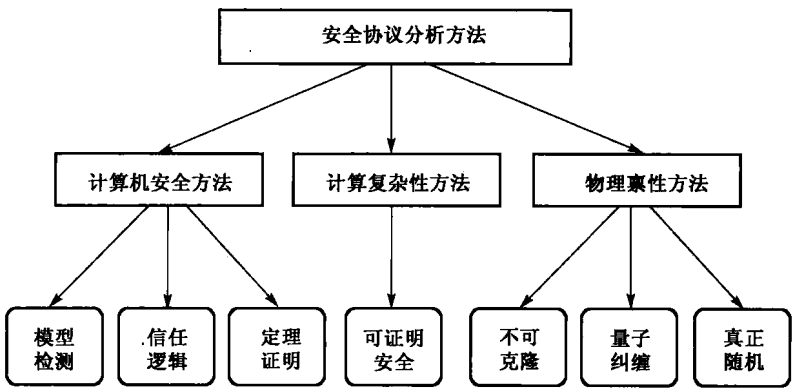


图 1.4 安全协议分析技术

表 1.6 攻击者能力模型

攻击能力	分 类	能力描述
Corruption 模型（攻陷能力）	非自适应攻击者（静态攻击者）	仅仅能够在协议开始前攻陷参与方，协议开始之后，未攻陷者仍然是未攻陷者，攻击者控制着一个任意但是固定的参与方集合
	自适应攻击者（动态攻击者）	在协议执行过程中或基于实时的信息收集中随意选择攻陷参与方