国家科学技术学术著作出版基金资助出版

信息安全系列丛书

Cryptographic Protocol
Security Analysis Based on Trusted Freshness

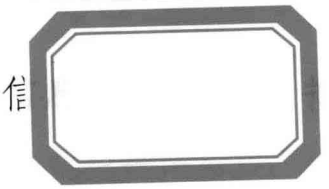
密码协议

基于可信任新鲜性的安全性分析

董玲　陈克非　著

高等教育出版社
HIGHER EDUCATION PRESS

国家科学技术学术著作出版基金资助出版



Cryptographic Protocol

Security Analysis Based on Trusted Freshness

密码协议

MIMA XIEYI

基于可信任新鲜性的安全性分析

JIYU KEXINREN XINXIANXING DE ANQUANXING FENXI

董 玲 陈克非 著

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

图书在版编目(CIP)数据

密码协议：基于可信任新鲜性的安全性分析 / 董玲，陈克非著．— 北京：高等教育出版社，2012.11
（信息安全系列丛书）
ISBN 978-7-04-036250-3

Ⅰ.①密… Ⅱ.①董… ②陈… Ⅲ.①密码协议 Ⅳ.①TN918.1

中国版本图书馆 CIP 数据核字(2012)第 226374 号

策划编辑 陈红英　　责任编辑 陈红英　　封面设计 刘晓翔　　版式设计 余 杨
责任校对 刁丽丽　　责任印制 朱学忠

出版发行 高等教育出版社
社　　址 北京市西城区德外大街 4 号
邮政编码 100120
印　　刷 涿州市星河印刷有限公司
开　　本 787mm × 1092mm　1/16
印　　张 22.5
字　　数 430 千字
购书热线 010-58581118
咨询电话 400-810-0598
网　　址 http://www.hep.edu.cn
　　http://www.hep.com.cn
网上订购 http://www.landraco.com
　　http://www.landraco.com.cn
版　　次 2012 年 11 月第 1 版
印　　次 2012 年 11 月第 1 次印刷
定　　价 55.00 元

物 料 号 36250-00

前言

网络通信协议是计算机节点之间为了通信而对需要交换消息的格式、规则的描述和规定。密码协议，又称安全协议，是一类特殊的通信协议，它通过一些密码学的手段来达到某种特殊的安全性目标。

网络通信协议通常具有层次结构，每一层协议进行相应的操作以逐步完成通信的全过程。通常，安全机制根据需要可以被嵌入到不同的协议层中。例如，众所周知的传输层安全协议 TLS 就是在 TCP 协议之上附加的协议，以实现特定的安全服务功能。事实上，密码协议广泛用于密钥建立、实体认证、消息认证、安全传输数据、不可抵赖等方面。由于通信过程不能保证实时与同步，一些密码协议并不如设计者所期望的安全，经典的例子如 Needham-Schroeder 公钥认证协议，从协议公布到安全漏洞被发现历经了 17 年。

本书的着眼点是密码协议安全性分析，首先引入可信任新鲜性的概念，在此基础上提出了协议安全性分析的新鲜性原则以及一种基于新鲜性原则的有效、易用、新颖的协议安全性分析方法——信任多集形式化方法。所做的这一切，试图要回答下面的问题：

- 协议的安全性（计算上安全，或实际的安全）究竟意味什么？
- 协议的安全性是否可以通过工程的方法检验？
- 如何使安全性的验证简单易行并能自动实现？

本书可作为通信协议安全性研究人员、学生以及工程技术人员的参考书。书中列举了大量密码协议分析的实例，可帮助读者理解、掌握相关概念和方法。这些内容对从事密码协议研究的专业人员，特别对密码协议设计和分析的工程师都将有所启发。本书提出的基于可信任新鲜性的安全性分析方法在实际应用中更加易于操作，分析过程也更为有效，即使是一个没有密码学专业背景的工程师也能很快掌握。

本书分为中、英文两个版本，分别在海内外发行。在写作过程中得到许多专家、同行和朋友的鼓励、支持与帮助，这成为我们完成本书的动力。为此，首先要感谢蔡吉人院士和裴定一教授，他们在得知本书的写作计划时给予了热情的鼓励，并向“国家科学技术学术著作出版基金”作了推荐；特别要感谢来学嘉教授，他对本书的前期工作给出了不少有益的建议；我们还要感谢上海交通大学密码与信息安

全实验室的龙宇博士以及博士生王亮亮、硕士生程正杰、本科生傅婧、罗施博等人，他们为本书分担了不少从英文版到中文版的翻译、校对等工作。最后，我们要感谢高等教育出版社的编辑陈红英女士，正是她的鼓动与建议才使我们下决心写作本书，在长达两年多的时间里，我们保持着很好的沟通与相互理解，她为本书付出了许多辛勤劳动。

本书得到“国家科学技术学术著作出版基金”的支持，同时也部分地得到国家自然科学基金（60970111，61133014）、国家 973 计划项目（2007CB311201）、国家 863 计划项目（2006AA01Z422）的支持，在此一并表示感谢。由于作者水平的局限，错误和不妥之处在所难免，恳请读者批评指正。

董玲 陈克非
上海交通大学
2012 年 6 月

目录

第1章　密码协议概述

所谓协议是一个规则集合，通过这些规则，明确两方或多方之间如何交换消息。密码协议也称安全协议，作为一种特殊的通信协议，它主要是借助基础的密码算法，为网络和通信提供安全保障，以实现保密性、认证性、完整性或者不可否认性等安全目标。密码协议中主要使用的基础密码算法（有时也称密码学原语）包括加密、签名、杂凑函数、随机数生成器等。

例1.1　图1.1给出了一个密码协议的实例，其中Alice是发起者，她希望借助可信第三方Trent与Bob建立一个安全的会话密钥。Alice想与Bob建立连接，为此她选择一个随机数 N_A 发送给Trent，Trent随即返回分别用长期共享密钥 K_{AS}（Alice与Trent间共享）和 K_{BS}（Bob与Trent间共享）加密的 N_A 以及Trent为Alice和Bob的会话新选的通信密钥 k_{AB}。这个协议执行成功后，可以实现Alice和Bob之间共享密钥 k_{AB} 的建立，因此可用于Alice和Bob间的保密通信。

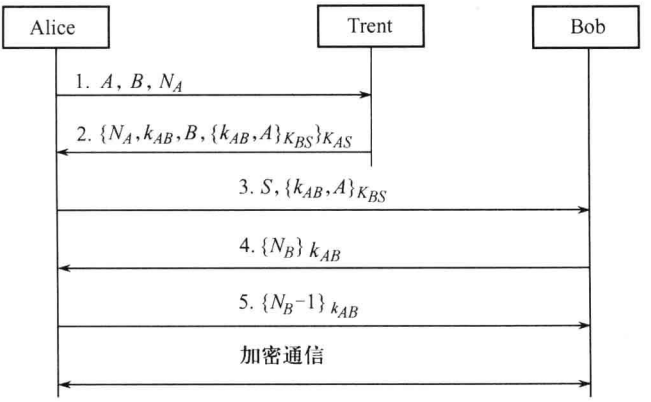


图1.1　密码协议举例

1.1　信息安全与加密

以往，消息通常由纸来记录、传递并保存，然而在当代，消息变为由磁性介质来记录、存储，并通过计算机网络来传递。正如我们所知道的，用电子手段来复制以

及替换所记录或者传递的信息，比用纸简单得多。信息安全致力于为数字信息提供安全服务。信息安全包括保密性、数据完整性、认证性、不可否认性、访问控制、有效性、公平性等。计算机网络安全研究专注于前四个常见的安全服务，其它如访问控制、公平性等可以通过这四种性质来推导得到[1-5]。本书中许多术语和概念均源于文献[1]，有兴趣的读者可从文献[1]获得更多细节的内容。

- 保密性是一种保证除了授权的参与者外的其他参与者和未参与者不能获得相关信息的服务。也就是说，在计算机系统中的信息或者正在传输的信息不能被未授权者所解读。保密性与机密性、私密性是同义术语。
- 完整性是一种防止数据被进行未授权修改的服务。数据修改涉及对传输消息的创建、写入、删除、改变、改变状态、延时或者重放。
- 认证性是一种可鉴别的服务，包括主体认证和数据来源认证。主体认证确保协议参与者确实参与了会话，数据来源认证隐含保障了数据的完整性（因为如果消息被修改过，即不具有数据完整性，那么它的源也一定改变了）。在许多应用中，通过认证意味着主体可以使用相应的资源。
- 不可否认性是一种用于防止主体否认先前的承诺或者动作的服务。一个主体可能否认某些承诺或者动作，这将造成纠纷，因此需要一个包括可信第三方参与其中的过程来解决这样的纠纷。通常使用的电子商务协议中的公平性安全机制可由不可否认性推导而出。
- 访问控制是一种用于处理主体访问信息资源时的授权问题的服务。只有授权的主体能够访问目标系统的信息资源。为了能够访问一个信息资源（诸如计算机账户、打印机或者应用软件），用户需要输入用户名和口令，并且直接地或者间接地指明了将要访问的资源。这里用户名是对主体身份的一个声明，口令则为这个声明提供了保证。系统会检测口令是否与系统保存的相应用户的有关数据匹配，以及这个声明的身份是否已被授权访问指定的资源。这个对于口令合法性的验证，在系统中等同于对于主体身份的证实。
- 有效性是一种保证信息资源处于有效性工作状态的服务，只要授权用户需要，系统就应该可使用。
- 公平性是一种用于保证每一个诚实的协议参与者都能持有充分证据来解决两方或多方之间的纠纷的服务，这样的纠纷可能会在协议运行中或者运行后产生。这是电子商务协议中最为重要的安全服务。

密码学研究的是信息安全中所涉及的数学理论和技术，例如保密性、数据完整性、主体认证性以及数据来源认证性。这其中也包括预防和发现欺骗以及其它恶意行为。密码技术是提供信息安全最常用的技术方法。然而，信息安全目标并不能单靠基础密码算法和密码协议来实现，还需要通过制度规范以及相应的法律手段才能达到期望的安全目标[1]。

1.2 密码协议的分类

密码协议是由一系列准确定义的步骤来描述的分布式算法,这些步骤指明两个或更多主体所需要完成的消息交互,以达到指定的安全目标。进行消息交互的密码协议既要对双方用于交换的消息进行精确定义,也要对各方所应采取的动作进行准确定义。按照密码协议的安全目标来划分,密码协议大致可分为四类:(身份)认证协议、密钥建立协议、电子商务协议以及安全多方协议。

1.2.1 身份认证协议

身份认证协议用于某一方主体获得所声称的另一方主体的某种身份信息的证明。通过取得某些确切的证据,身份鉴别或者主体认证技术能够使某一方主体确信:另一方的主体是存在的,并在当下的会话中处于活跃状态(例如,刚刚产生或接收了证据)。除了给出是某个特别主体的声明外,认证协议通常不包含其它有意义的消息。认证协议可进一步分为单向认证协议、双向认证协议。Woo-Lam 协议[6]、零知识身份证明协议[7]以及 Okamoto 协议[8]都是这样的例子。

- 单向认证协议(或单向主体认证协议),也称为单方认证协议或单边认证协议,它保证只有持有确切的证据,通信协议的其中一方主体才能确定另一方主体在正在运行的协议实例中是活跃的。
- 双向认证协议(或双向主体认证协议),也称为双方认证协议或双边认证协议,它保证只有持有确切的证据,通信协议的双方主体才能确定对方主体在正在运行的协议实例中是活跃的。通信双方分别将单方认证协议运行一遍,从而证实另一方主体在当下的会话中处于活跃状态,则可以获得双方认证安全的协议。

1.2.2 密钥建立协议

密钥建立协议用于建立共享秘密,这个秘密被称为会话密钥,或用于导出会话密钥。密钥建立是一个共享密钥在两个或多个主体之间成为可能的过程,生成的密钥将用于后续需要密码操作的过程。理想情况下,一个会话密钥是一个短暂存在的秘密,也就是说,它的使用寿命被限制在一个很短的时间范围内,例如一个远程通信连接,在这个连接使用期过后,所有关于这个会话密钥的记录将被删除。在密钥建立协议中,由于会话密钥的私密性要求,一般需要进行数据源的认证。要保证这些安全属性,在密钥建立过程中常使用加密和签名等密码操作。密钥建立协议大致可进一步细分为密钥传输协议和密钥协商协议。

- 密钥传输协议是一种密钥建立技术,是指协议运行的某一方产生或者获得一个秘密数值,将其作为一个会话密钥,并且能够安全地传输给另一方。
- 密钥协商协议也是一种密钥建立技术,是指协议运行的双(或更多)方分别产生

或者获得一个秘密数值,并将它们作为导出会话密钥的函数的输入值。因此,在这个密钥建立过程中,每一个主体都不可能提前预知会话密钥值。

认证的密钥建立协议在两个或多个主体之间建立共享密钥,同时要保证共享密钥的另一方主体的身份能够被证实。Needham-Schroeder 公钥协议[9]、Internet 密钥交换(Internet Key Exchange, IKE)协议[10]、Kerberos 认证协议[11]、X.509 协议[12]、分布式认证安全服务(Distributed Authentication Security Service, DASS)协议[13]等都属这类协议。

1.2.3 电子商务协议

电子商务协议为网络中双方或多方之间电子交易的安全提供保证。电子商务协议主要着眼于协议的公平性和不可否认性。典型的例子如安全电子交易(Secure Electronic Transaction, SET)协议[14]和因特网安全支付(Internet Keyed Payments, IKP)协议[15]等。

1.2.4 安全多方协议

安全多方协议为分布式系统中多方主体在协作过程中的安全性提供保证,即协议的运行不会危及任何一方主体的隐私或秘密。群密钥交换协议、多方认证协议、网络电子选举协议、电子竞标协议、电子现金协议等都属于这类协议。

与大部分有关密码协议的文献一样,本书所指的认证协议通常包括身份认证协议和密钥建立协议。

1.3 密码协议的安全

一个主动的协议攻击者(当然,他既可以是一个独立的黑客,也可以是通过一个开放的分布式网络与他人合作的攻击者团队),他能够监听、拦截、修改、注入消息,并熟练掌握协议规则的操作。密码协议是安全的就意味着,即使同时存在主动攻击者和通信传输,密码协议仍然能够达到其所有声称的安全目标。对于一个密钥建立协议来说,它应当是**可用的**,并且是**抗扰的**。密钥建立协议的可用性意味着能够确保密钥保密性和密钥认证性,还意味着,如果没有主动攻击者和通信传输错误,只要诚实的参与者遵守协议的规定,通信各方总是能在协议的运行完成后计算出共同的密钥,并且能够确认与之共享密钥的另一方主体的身份。密钥认证性意味着共享密钥的各方主体的身份是确认的,因此可以抵御假冒攻击和替代攻击。密钥建立协议的抗扰性意味着,一个主动的攻击者不可能成功误导一个诚实的协议参与者,使之相信最终达成的协议安全目标[1]。

密码协议,特别是认证协议或者认证的密钥建立协议,是非常难以设计和查错

的。例如,IEEE 802.11 的有线等价协议(Wired Equivalent Privacy,WEP)[16],用来保护链路层通信,防止窃听和其它攻击,但之后却发现这个协议存在严重的安全缺陷。在早期的安全套接层(Secure Socket Layer,SSL)协议[17]、后来的 IEEE 802.11i 的无线认证协议(Wireless Authentication Protocols,WAP)[18]、Kerberos[11]等标准和建议标准中也或多或少发现了可能存在的安全缺陷。

一个针对认证协议或者认证的密钥建立协议的成功攻击,通常并不需要如基于计算复杂性理论的密码分析那样破解密码算法。相反地,一个针对协议的成功攻击通常指非授权攻击者在没有破解密码算法的情况下仍然能够不被察觉地获得密码学上的信任凭证,或者使通信者期望的密码服务无效。当然,这些都是由于协议设计上的错误而不是密码算法上的错误造成的[3]。

针对密码协议的可能攻击方式包括:中间人攻击、源替换攻击、消息重放攻击、平行会话攻击、反射攻击、交错攻击、类型缺陷攻击、基于身份遗漏的攻击、基于密码学服务误用的攻击等。在这里,我们只是列出了所有已知攻击的主要类型,而无法穷尽所有可能的攻击类型。事实上,因为攻击者的能力在不断地提升,所以必然会出现新的攻击类型。另外,从更底层的通信协议来看(例如网络层),攻击者不需要掌握非常高深的技术就可以运用各种类型的攻击。因此,一个密码协议,特别是认证协议和密钥建立协议,尽管由专家精心设计和维护,还是难免会出现某些安全缺陷。

本小节将展示密码协议的这种微妙性,尤其是认证和密钥建立类协议的易错性。

例 1.2 Needham-Schroeder 公钥认证密码协议是基于非对称密码体制的密钥协商协议,是最为著名的认证密钥协议[9],如图 1.2 所示。该协议的目标是在两个主体 Alice(A)和 Bob(B)之间建立一个基于会话密钥的安全通道,新会话密钥由协议的参与者 A、B 分别给出的随机输入 N_A、N_B 共同生成,协议中各方都对这个新会话密钥做出了自己的贡献,N_A、N_B 还用于双方主体身份的认证。

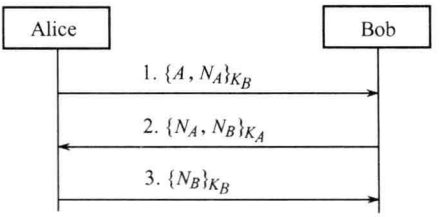


图 1.2 Needham-Schroeder 公钥协议

符号

A 代表 Alice,B 代表 Bob,他们都是协议参与主体。K_A(K_B)和 K_A^{-1}(K_B^{-1})是

$A(B)$的公、私钥对，k_{AB}是A和B在本次认证协议中希望建立的新会话密钥。N_A是A选择的随机数，N_B是B选择的随机数，用于生成新的会话密钥k_{AB}。$\{Y\}_{K_X}$表示用主体X的公钥K_X对数据Y加密（比如RSA）；$\{Y_1, Y_2\}_{K_X}$表示用X的公钥K_X对消息片段Y_1、Y_2的串联进行公钥加密。

前提

$K_A(K_A^{-1})$是Alice的公（私）钥，$K_B(K_B^{-1})$是Bob的公（私）钥，Alice和Bob都知道对方的公钥，否则，需要额外的消息来传输包括主体公钥的公钥证书。

协议动作

1）在消息1中，A发起一个新的协议运行，发送A的身份和一个随机数N_A给B。

2）在收到消息1后，B使用私钥K_B^{-1}恢复出随机数N_A。在消息2中，B随机选取随机数N_B并将N_A和N_B一起发送给A。

3）在收到消息2后，A使用私钥K_A^{-1}恢复出随机数N_A和N_B，并检测N_A是否与消息1中的N_A相同。假定N_A在这次协议运行之前从来没有被使用过，此时A收到的N_A如果正确，那么这将为A提供B的主体身份认证，且A可以确信B知道了N_A这个关键信息。A随后会向B发送消息3。

4）在收到消息3之后，B使用私钥K_B^{-1}恢复出随机数N_B，并检测N_B是否与消息2中的N_B相同。新会话密钥能够通过$f(N_A, N_B)$计算得出，其中f是一个A和B都知道的恰当的不可逆函数。

协议的一次成功运行将在A和B之间生成新会话密钥的输入N_A、N_B，这是只有Alice和Bob共享的秘密信息。需要进一步注意的是，由于协议双方都对这些共享秘密的生成做了贡献，因此他们对N_A、N_B的新鲜性有信心。A和B也都相信N_A和N_B具有随机性，因为它们选自一个很大的空间，所以用N_A和N_B来生成共享密钥$f(N_A, N_B)$能够用于建立Alice和Bob之间的进一步安全通信。

不幸的是，Lowe在Needham-Schroeder公钥认证协议公开提出的17年之后，发现这个协议存在安全漏洞[19]。在Lowe的攻击中，Malice拦截了消息1、消息2、消息3，并且用自己的修改版本替换了这些消息。

例1.3　针对Needham-Schroeder公钥认证协议的攻击如图1.3所示。这个攻击包括两个平行运行的Needham-Schroeder公钥认证协议实例。在第一个协议运行实例中（消息1、消息2、消息3），Alice与Malice建立了一个有效的会话；在第二个协议运行实例中（消息1′、消息2′、消息3′），Malice冒充Alice欺骗了Bob，在Alice和Bob之间建立了一个假的会话。最后，Bob相信Alice（实际上是Malice）和Bob成功地建立了一个会话，并且共享了生成新会话密钥的秘密信息N_A、N_B。