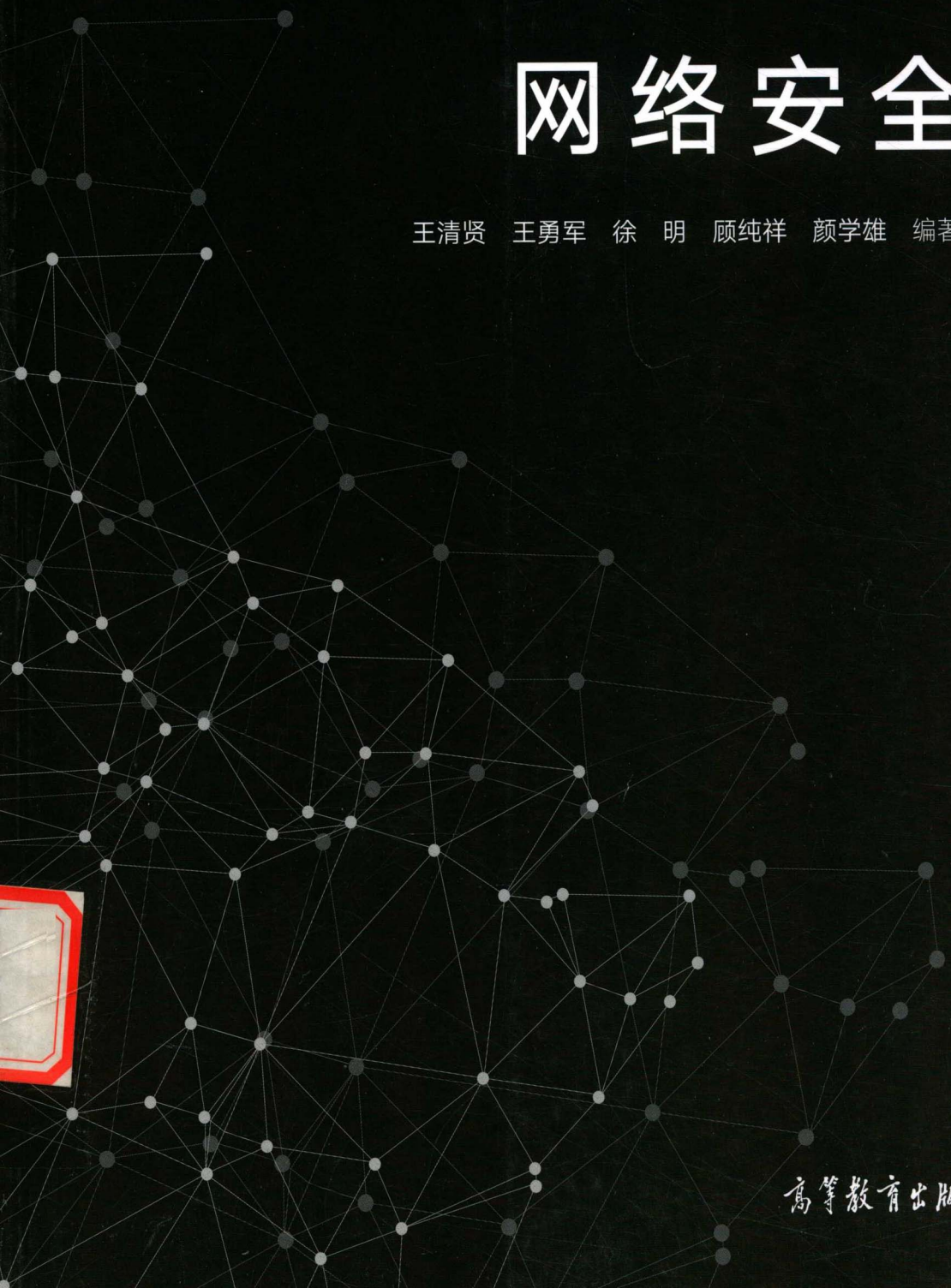
高等学校网络工程系列教材

网络安全

王清贤　王勇军　徐　明　顾纯祥　颜学雄　编著



高等教育出版社

高等学校网络工程系列教材

网络安全

王清贤　王勇军　徐　明　顾纯祥　颜学雄　编著

高等教育出版社·北京

内容提要

本书以计算机网络安全为重点，按照理论结合实践的原则，系统阐述网络安全理论与技术。全书围绕安全策略与模型、安全协议与密码、安全检测与防护、安全漏洞与评估等四个方面组织内容，共分11章，主要内容包括网络安全概述、安全策略、安全模型、密码算法基础、安全认证、网络安全协议、虚拟专用网VPN、防火墙技术、入侵检测技术、漏洞检测与防护、安全评估与审计。

本书依据教育部高等学校计算机类专业教学指导委员会编制的《高等学校网络工程专业规范》编写，是为高等学校网络工程本科专业主干课程网络安全提供的基本教材，也可以作为网络空间安全、信息安全、计算机、通信工程等专业领域教学、科研和工程技术人员的参考用书。

图书在版编目（CIP）数据

网络安全／王清贤等编著．--北京：高等教育出版社，2018.7

高等学校网络工程系列教材

ISBN 978-7-04-049462-4

Ⅰ.①网… Ⅱ.①王… Ⅲ.①网络安全-高等学校-教材 Ⅳ.①TN915.08

中国版本图书馆CIP数据核字(2018)第033353号

Wangluo Anquan

策划编辑	张海波	责任编辑	张海波	封面设计	李小璐	版式设计	马　云
插图绘制	于　博	责任校对	吕红颖	责任印制	尤　静		

出版发行	高等教育出版社	网　址	http://www.hep.edu.cn
社　址	北京市西城区德外大街4号		http://www.hep.com.cn
邮政编码	100120	网上订购	http://www.hepmall.com.cn
印　刷	廊坊十环印刷有限公司		http://www.hepmall.com
开　本	787mm×1092mm　1/16		http://www.hepmall.cn
印　张	19.5		
字　数	410千字	版　次	2018年7月第1版
购书热线	010-58581118	印　次	2018年7月第1次印刷
咨询电话	400-810-0598	定　价	39.00元

物料号　49462-00

序

自20世纪60年代以来，计算机网络从无到有、从小到大，覆盖和渗透到现代社会的方方面面，极大地促进了信息化社会的发展。网络的互联互通，实现了人、机、物泛在互联，使得网络应用日新月异，衍生出大批相关行业，产业链日臻完整、丰富。

与此相对应，网络专业技术人才培养规模也从无到有、从小到大，努力适应社会各行业飞速发展的需要。众所周知，网络工程专业是在计算机科学与技术、通信工程、信息工程等专业交叉、融合的基础上发展起来的新专业，涉及计算机网络的设计、规划、组网、维护、管理、安全和应用等方面的工程方法学和实践问题。1998年，网络工程作为目录外专业首次出现在教育部的本科专业目录中。2011年，教育部明确网络工程专业为目录内专业，标志着网络工程作为一个独立的本科专业已得到社会的广泛认可。据不完全统计，全国已经有340多所高校设置了网络工程专业。

2015年，为适应网络工程专业发展的需要，教育部高等学校计算机类专业教学指导委员会成立了网络工程专业教学指导工作组（下称工作组）。之后的一项重要工作便是通过一系列的研讨活动研究和制定网络工程专业规范，全面梳理网络工程专业定位、专业能力、知识体系、课程体系、实践体系等方面的内容。专业规范明确了网络工程人才培养的目标定位和培养规格，将课程体系分为基础课程、核心（主干）课程与扩展课程，按知识领域、知识单元和知识点进行专业知识的系统化组织，为具体教学实施提出相应的建议与参考标准。

针对教学的需要，工作组召集了一批具有丰富经验的老师成立教材编写组，首先启动计算机网络、网络管理、网络应用开发、网络安全、网络设计与集成等五门课程的教材编撰工作。教材编写组对五本教材的内容进行了系统规划，安排五位老师各自负责一本教材的编撰，分别是：解放军理工大学陈鸣负责计算机网络、国防科技大学徐明负责网络管理、西安电子科技大学方敏负责网络应用开发、信息工程大学王清贤负责网络安全、国防科技大学曹介南负责网络设计与集成，最后由徐明负责五本教材的审定。其中，陈鸣负责的《计算机网络：原理与实践》已于2013年先期出版，其他四本教材将于近期陆续出齐。

核心课程教材出版还只是第一步，在征集各方面意见与建议的基础上，教材编写组

将适时启动扩展教材以及实验教材的编写工作。

衷心感谢工作组组长杨波教授以及各位专家教授，他们为教材的撰写和出版提供非常好的建议，也特别感谢教材编写组的各位成员，正是他们的辛勤工作和无私奉献，使本系列教材得以如期出版。

近些年来，网络工程专业五门核心课程及其内涵获得了趋于一致的认可，也促使我们第一次以系列教材方式组织编写和出版网络工程专业核心课教材。如何更好地体现网络技术的发展和进步、如何有针对性地配置优质的网络教学资源、如何以能力培养为牵引实现教学相长等还有大量工作需要开展。在这个意义上说，教材的出版并不是终点，而是新的起点。

我们不忘初心，继续前进。

2017.04

前　言

进入21世纪，随着云计算、物联网、社交网络以及移动互联网等各种网络新技术和新业务的不断涌现，网络不再局限于计算机之间的互联，而是将不同的设备、不同的系统乃至不同的物理实体联系起来，更重要的是将每一个人与现实世界广泛地、随时随地联系起来，极大拓展了互联互通的范畴和信息链接的深度。人类生活、工作和思维方式正在发生深刻变革，以互联网为主要载体的网络空间和现实空间不断融合，网络空间成为陆、海、空、天之后的第五维空间，网络空间安全上升到国家战略层面，受到各国高度重视。

随着我国现代化建设和信息化进程不断加快，网络信息技术在国家政治、经济、文化、社会和国防等各领域得到广泛应用，信息资源与关键信息基础设施业已成为国家发展最重要的“战略资产”与“核心要素”，网络安全在整体国家安全中的地位日益凸显。习总书记深刻指出，没有网络安全就没有国家安全。建设网络强国，保卫网络疆域，要有高素质的网络安全人才队伍。为加强网络安全人才建设，2015年6月教育部在工学门类下增设了“网络空间安全”一级学科。2016年7月，中央网络安全和信息化领导小组办公室等发布《关于加强网络安全学科建设和人才培养的意见》，要求加快网络安全学科专业建设，创新网络安全人才培养机制，更明确要加强网络安全教材建设。

在此背景下，《网络安全》教材应运而生。本教材以计算机网络安全为重点，按照理论结合实践的原则，系统阐述网络安全理论与技术，为广大读者提供较为全面的网络安全理论与技术立体图景，为我国网络安全人才培养提供支持。

网络安全内容非常丰富，涉及多个学科，包括计算机、电子、通信、数学、物理、法律、管理学等。同时，随着信息技术的不断发展，新思想、新技术和新方法层出不穷，将会进一步促进网络安全理论和技术的发展，因此，网络安全内容又具有很强的动态发展性。这些特性，为本教材内容的选择增加了难度。

本教材依据教育部高等学校计算机类专业教学指导委员会编制的《高等学校网络工程专业规范》编写，按照“有所为，有所不为”的原则，在内容选择上“突出理论基础，强化动手实践”。全书共11章，具体内容如下。

第一章网络安全概述，介绍了网络安全定义、安全威胁源及基本分类、网络安全应对基本措施、网络安全体系、网络管理体系、网络安全法律法规等。

第二章安全策略，介绍几种典型的网络安全策略，包括黑白名单策略、最小特权策略、分权策略、基于推理的策略等。

第三章安全模型，介绍了信息系统全生存周期的安全防护的P2DRR模型、访问控制模型（基于矩阵的访问控制模型、基于角色的访问控制模型、跨域访问控制模型）、机密性模型、完整性模型等。

第四章密码算法基础，介绍了密码算法数学基础、分组加密算法（DES、AES、IDEA）、公钥加密算法与RSA、散列函数（SHA）、数字签名（DSS）。

第五章安全认证，介绍了消息认证码、实体认证、口令认证（固定口令、一次性口令）、挑战-响应认证协议（基于对称密钥、基于公钥）、密钥协商。

第六章网络安全协议，介绍了Kerberos协议、IPsec协议、SSL/TLS协议、PGP协议、无线安全IEEE 802.11i协议等。

第七章虚拟专用网VPN，介绍了第二层隧道协议（L2F、PPTP、L2TP）、第三层隧道协议GRE、典型VPN应用、Windows配置实现VPN。

第八章防火墙技术，介绍了防火墙技术（静态包过滤、状态检测、代理服务型和复合型技术）、防火墙体系结构（双重宿主主机、屏蔽主机和屏蔽子网体系结构）、防火墙新技术、iptables防火墙的配置与使用。

第九章入侵检测技术，介绍了入侵检测的基本概念、入侵检测系统的基本结构、入侵检测系统分类、入侵检测分析技术、入侵检测响应机制、入侵防御系统（IPS）、Snort配置与使用。

第十章漏洞检测与防护，介绍了漏洞的基本概念、典型漏洞、国内外漏洞信息库、漏洞扫描、漏洞安全防护等。

第十一章安全评估与审计，介绍了信息安全风险评估的基本概念、方法分类、安全评估标准体系、安全评估标准流程和工具、网络安全审计原理、网络安全审计技术和工具。

阅读本教材应具备操作系统、计算机网络和信息安全数学基础等方面的基础知识。

本教材是为高等学校网络工程本科专业主干课程“网络安全”编写的基本教材，但也可以作为网络空间安全、信息安全、计算机、通信工程等专业领域的教学、科研和工程技术人员的参考用书。

参加本教材编写的人员有：王清贤，王勇军，徐明，顾纯祥，颜学雄。本教材的第一、二、三章由颜学雄编写，第四、五章由顾纯祥编写，第六、十、十一章由王勇军编写，第七、八、九章由徐明编写。全书由王清贤进行统稿和审校。信息工程大学网络空间安全学院奚琪老师协助进行了统稿和审校，周天阳、郑永辉老师提出了宝贵的修改意见，对他们所做出的贡献表示衷心的感谢！

特别感谢哈尔滨工业大学张宏莉教授！作为本教材的主审专家，张宏莉教授认真审阅了全书并提出了许多宝贵的意见和建议，作者在此向她表示衷心的感谢！

由于作者水平有限，书中难免存在不足和欠妥之处，恳请广大读者给予批评和指正。

编　者

2017 年 12 月

目　录

Kerberos 服务器。Kerberos 服务器实际上又由票据授权服务器（ticket granting server，TGS）和认证服务器（AS）两部分组成。

Kerberos 协议参与者和主要工作流程如图 6-1 所示，假设客户要访问网络上的一个应用服务器（如远程登录或类似的登录请求方式）。服务器接受请求的前提是要有一张 Kerberos 的“入场券”，也就是协议中说的“票据”（ticket）。因此，Kerberos 协议的大体工作流程就是两步。

① 票据请求：客户向 Kerberos 服务器请求访问应用服务器的服务授权票据（service granting ticket，SGT）。

② 获得服务：客户利用获得的服务授权票据，通过应用服务器的身份鉴别，获得应用服务。

服务授权票据会被打上时间戳，允许客户在某个特定时间段内直接访问同一服务。一个客户可以同时拥有多个不同应用服务器的服务授权票据。

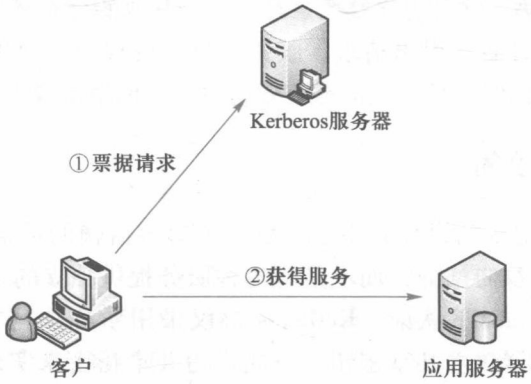


图 6-1　Kerberos 协议参与者和主要工作流程

Kerberos 协议实际的工作过程要复杂得多，以版本 4 为例，图 6-2 中给出了 Kerberos 协议多方之间进行信息交互的过程。

该过程分为三个阶段，共 6 条消息。

第一个阶段是用于获取票据授权票据（ticket granting ticket，TGT）的认证服务交换，协议交互双方是客户和 Kerberos 服务中的认证服务器 AS，由图 6-2 中①和②两步消息构成。由于最终应用服务器的服务授权票据是由票据授权服务器 TGS 发给客户的，因此客户要先获得 TGT 用于访问 TGS 服务。客户在①中向 AS 发出申请请求访问 TGS，AS 在②中向客户返回票据授权票据 $\text{Ticket}_{\text{TGS}}$。该票据由 AS 和 TGS 预先设置的共享密钥 K_{TGS} 进行加密，票据主要组成是 AS 分配的用于保护消息④的客户与 TGS 间共享密钥 $K_{\text{C,TGS}}$ 以及客户的地址 AD_{C}，该票据可防止被客户解密篡改，并由客户所保存。在②中，AS 利用客户口令派生的密

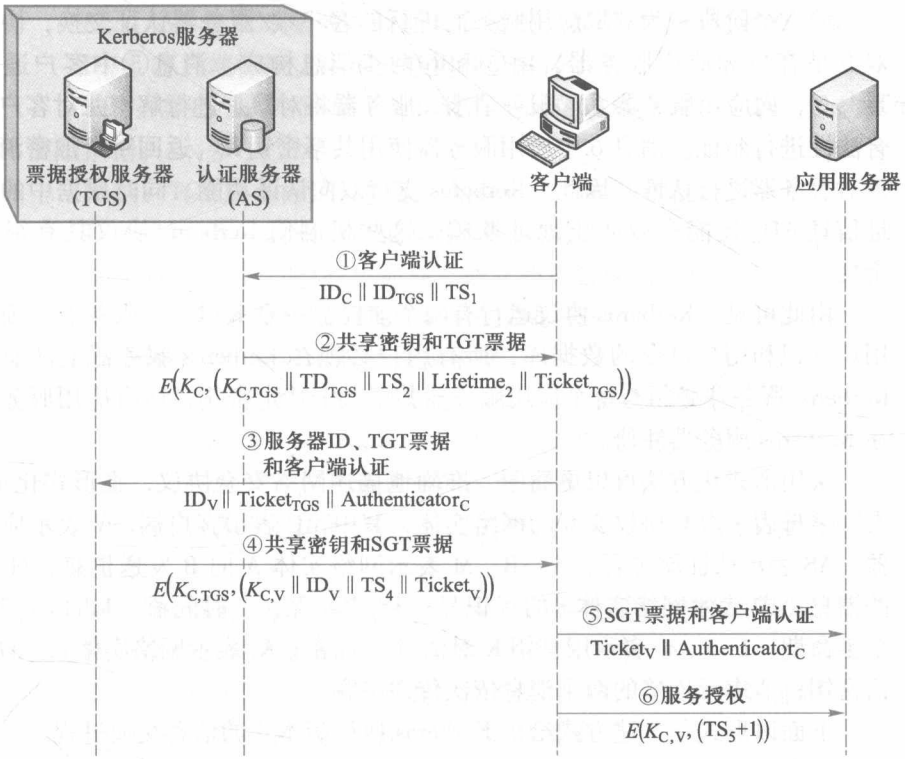


图 6-2 Kerberos 协议信息交换

钥 K_C 加密票据，客户端提示用户输入口令，生成密钥，解密传来的消息，如果口令正确则可以成功获得票据。由于 $Ticket_{TGS}$ 可以重用，为了防止攻击者使用该票据欺骗 TGS，票据中还包含带有日期和时间的时间戳，以及票据合法使用时间长度（如 8 小时）的生命期（life time）。

第二个阶段是用于获取应用服务授权票据的服务授权票据交换，协议交互双方是客户和 Kerberos 服务中的票据授权服务器 TGS，由③和④两步消息构成。消息③中客户通过发送应用服务器标识和 $Ticket_{TGS}$，向 TGS 发起服务请求，TGS 对得到的票据进行解密，通过其标志验证该票据的正确性，确定该票据的生命期未超时，并且比较客户标识和网络地址是否与消息来源一致。如果用户被允许访问服务器，则在消息④中 TGS 返回一个特定应用服务的授权票据 $Ticket_V$。类似地，该票据使用应用服务器和 TGS 预先设置的共享密钥 K_V 进行加密，票据组成主要包括 TGS 分配的用于保护消息⑥的客户与应用服务器间共享密钥 $K_{C,V}$ 和客户的地址 AD_C，该票据可防止被客户解密篡改，并由客户所保存。在④中，TGS 利用与客户的共享密钥 $K_{C,TGS}$ 加密票据。同样，为了防止攻击者使用 $Ticket_V$ 欺骗应用服务器，票据中也包含了时间戳和生命期。

第三个阶段是为获取应用服务而进行的客户端/服务器认证交换，协议交互双方是客户和应用服务器，由⑤和⑥两步消息构成。消息⑤中客户通过发送 Ticket_V，向应用服务器发起服务请求，服务器将对票据进行解密并对客户的身份合法性进行验证。消息⑥中应用服务器使用共享密钥 $K_{C,V}$ 返回一个加密消息供客户对服务器进行认证。因此，Kerberos 支持双向认证功能，同时票据中的客户地址信息 AD_C 还能有效防止地址欺骗，这些机制使 Kerberos 协议具有很高的安全性。

由此可见，Kerberos 协议运行有两个前提：一是 Kerberos 服务器必须有存放用户标识和用户口令的数据库，所有用户必须在 Kerberos 服务器上注册。二是 Kerberos 服务器必须与每个应用服务器共享一个特定密钥，所有应用服务器必须在 Kerberos 服务器注册。

采用形式化方法可以更简明、准确地描述网络安全协议，在形式化描述中，大写字母表示参与协议交互的网络实体，其中，C 表示客户端，V 表示应用服务器，AS 表示认证服务器；A→B：M 表示网络实体 A 向 B 发送消息，M 为发送的消息；ID_i 表示网络实体 i 的标识号；TS_j 表示第 j 个时间戳；Lifetime_j 表示第 j 个生命期；$E(K,m)$ 表示用密钥 K 对消息 m 加密；K_{IJ} 表示网络实体 I,J 的共享会话密钥；‖ 表示连接的两个消息依次传递串联。

下面以形式化描述方式给出 Kerberos 协议版本 4 的信息交换过程。

阶段一：用于获取票据授权票据的认证服务交换。

消息①：客户端申请访问票据授权服务器 TGS

$$\text{C}\rightarrow\text{AS}:\text{ID}_C \parallel \text{ID}_{TGS} \parallel \text{TS}_1$$

其中，ID_C：客户端的用户标识；

ID_{TGS}：用户请求访问的 TGS 服务标识；

TS_1：时间戳，使 AS 可以验证客户的时钟与 AS 的时钟是否同步。

消息②：AS 向客户返回票据授权票据

$$\text{AS}\rightarrow\text{C}:E(K_C,(K_{C,TGS} \parallel \text{ID}_{TGS} \parallel \text{TS}_2 \parallel \text{Lifetime}_2 \parallel \text{Ticket}_{TGS}))$$

$$\text{Ticket}_{TGS} = E(K_{TGS},(K_{C,TGS} \parallel \text{ID}_C \parallel \text{AD}_C \parallel \text{ID}_{TGS} \parallel \text{TS}_2 \parallel \text{Lifetime}_2))$$

其中，K_C：基于用户口令派生的加密密钥，使 AS 和客户端可以验证口令，并保护消息②的内容；

$K_{C,TGS}$：由 AS 创建的用户与 TGS 服务之间共享的会话密钥，以实现客户端和 TGS 之间安全信息交换；

ID_{TGS}：TGS 服务标识，确认此票据是为 TGS 生成的；

TS_2：时间戳，以通知客户端此票据的发放时间；

Lifetime_2：通知客户端此票据的有效生命期；

Ticket_{TGS}：客户端用来访问 TGS 的票据授权票据；

K_{TGS}：AS 与 TGS 服务之间的共享密钥，加密票据授权票据，以防篡改；

ID_C：客户端标识，标识此票据的合法所有者；

AD_C：客户端网络地址，防止除开始时请求票据的客户端之外的其他客户端使用票据；

ID_{TGS}：TGS 服务标识，使服务器确认票据被正确的解密；

TS_2：时间戳，通知 TGS 此票据的发放时间；

$Lifetime_2$：票据的有效生命期，防止票据过期后的重放。

阶段二：用于获取服务授权票据的票据交换。

消息③：客户端请求服务授权票据

$$C \rightarrow TGS: ID_V \parallel Ticket_{TGS} \parallel Authenticator_C$$

$$Authenticator_C = E(K_{C,TGS}, (ID_C \parallel AD_C \parallel TS_3))$$

其中，ID_V：告知 TGS 用户请求访问的服务器 V 的标识；

$Ticket_{TGS}$：客户端访问 TGS 的票据授权票据，以向 TGS 确认此用户是通过 AS 认证的；

$Authenticator_C$：客户端认证符，由客户端生成，使服务器确认票据出示者即是被授权票据的客户端，有效期很短，以防止重放；

$K_{C,TGS}$：客户端与 TGS 之间共享的会话密钥，用来加密认证符；

ID_C：客户端标识，标识此票据的合法所有者；

AD_C：客户端网络地址；

TS_3：时间戳，通知 TGS 认证符的生成时间。

消息④：TGS 返回服务授权票据

$$TGS \rightarrow C: E(K_{C,TGS}, (K_{C,V} \parallel ID_V \parallel TS_4 \parallel Ticket_V))$$

$$Ticket_V = E(K_V, (K_{C,V} \parallel ID_C \parallel AD_C \parallel ID_V \parallel TS_4 \parallel Lifetime_4))$$

其中，$K_{C,TGS}$：C 与 TGS 之间的共享密钥，用来保护消息④；

$K_{C,V}$：由 TGS 创建的由客户端与服务器 V 之间共享的会话密钥，以实现客户端和服务器之间安全信息交换；

ID_V：服务器 V 的标识，以确认票据由 V 生成；

TS_4：时间戳，通知客户端此票据的发放时间；

$Ticket_V$：客户端用来访问服务器 V 的服务授权票据；

K_V：TGS 与服务器 V 之间的共享密钥，服务授权票据被只有 TGS 和服务器知道的密钥加密，以防篡改；

ID_V：服务器 V 的标识；

TS_4：时间戳，通知服务器票据发放时间；

$Lifetime_4$：票据的有效生命期，防止票据过期后的重放。

阶段三：为获取服务而进行的客户端/服务器认证交换。

消息⑤：客户端申请服务

$$C \rightarrow V: Ticket_V \parallel Authenticator_C$$

$$Authenticator_C = E(K_{C,V}, (ID_C \parallel AD_C \parallel TS_5))$$

其中，$Ticket_V$：客户端访问服务器 V 的服务授权票据；

$Authenticator_C$：客户端认证符，由客户端生成，使服务器确认票据出示者即是被授权票据的客户端，有效期很短，以防止重放。

TS_5：时间戳，通知服务器认证符生成的时间。

消息⑥：可选的客户端对服务器的验证

$$V \rightarrow C: E(K_{C,V}, (TS_5+1))$$

其中，TS_5+1：使客户端确认这个应答不是一个先前应答的重放。

6.2.3　Kerberos 协议应用及安全

微软 Windows 2000 和后续的操作系统都默认 Kerberos 为其网络认证方法，其中，Windows Server 2003 操作系统实现了 Kerberos 版本 5 的身份认证协议，同时也实现了公钥身份认证的扩展。另外，苹果的 Mac OS X、Red Hat Enterprise Linux 4 和后续的操作系统也使用了 Kerberos 的客户和服务器版本。

在 Windows 中，Kerberos 用户身份认证是跟微软窗口登录（winlogon）的单点登录（single sign on，SSO）架构集成在一起的。SSO 是指用户只需输入一次身份验证信息，就可以凭借此验证获得的票据访问多个应用服务。在 Windows 中，Kerberos 服务器被称为密钥分发中心（key distribution center，KDC），KDC 和 Windows Server 域控制器（domain controller，DC）上的安全服务集成在一起，KDC 使用域的活动目录数据库作为它的安全账户数据库，默认的 Kerberos 实现要求支持活动目录（active directory，AD）。

Kerberos 协议虽然有强大的认证功能，但是由于其自身实现的缺陷，还存在以下安全问题。

① 单点失效。协议运行依靠中心服务器的持续响应，一旦服务器宕机，则整个系统瘫痪。这个协议缺陷可以通过构建 Kerberos 服务器集群等机制进行弥补。

② 要求参与通信的主机时钟同步。由于票据具有一定有效期，如果主机的时钟与 Kerberos 服务器的时钟不同步，认证会失败。默认设置要求时钟的时间相差不超过 10 分钟。在实践中，通常用网络时间协议（network time protocol，NTP）后台程序来保持主机时钟同步。

③ 密钥的安全。由于所有用户使用的密钥都存储于中心服务器中，危及服务器安全的行为将对密钥的安全产生危害。