1 PKI 概述

本章导读：

本章主要介绍公钥基础设施（Public Key Infrastructure，PKI）的概念及发展过程，并简单分析 PKI 的各个组成部分的内容。由于公钥基础设施必须有信息安全作为基础，因此本章也介绍了信息安全基础的相关内容。

学习目标：

- 了解网络信息安全的基本概念
- 掌握公钥基础设施（PKI）的基本概念
- 掌握 PKI 的基本组成以及各组成部分的基本功能

引入案例

网易等 7 家互联网巨头启动网络安全教育活动

2013-08-26 15:41　来源：中国网

日前，网易联合阿里巴巴及支付宝、百度、腾讯、新浪、360 等联合启动名为“守护英雄”的网络安全教育主题活动，旨在通过在线科普网络安全知识，培养用户良好的网络安全使用习惯，增强用户对信息安全保障的信心。

这是继去年 7 月举办“反裸奔”网络安全教育活动后，我国互联网巨头再一次联动科普网络安全知识。

近年，随着互联网应用深入亿万民众的日常生活，围绕网络信息的安全威胁也日渐增加，

而一些网友的安全防范意识薄弱，放任电脑和账号“裸奔”，导致信息被盗等情况时有发生，严重的甚至危及用户资金安全。

为帮助网民防御网络安全威胁，共建互联网健康发展环境，去年 6 月，网易联合阿里巴巴集团及支付宝、微软、百度、腾讯、新浪、人人等互联网巨头共同组建了互联网企业安全工作组（ISWG.CN），通过用户教育和技术创新的方式，双管齐下为用户网络信息安全“保驾护航”。

而“守护英雄”活动，则是今年工作组利用安全教育提升用户安全意识和知识水平的重要举措。据悉，“守护英雄”活动由互联网企业安全工作组成员网易联手阿里巴巴集团及支付宝、新浪、百度、腾讯以及 360 七家互联网企业联合发起，作为去年“反裸奔”活动的延伸，发起方希望帮助用户树立正确的网络安全观。

“我们需要业内企业单位协同合作，给用户提供良好的网络安全防护习惯指引，网聚最广大网民的主动性，共同维护中国互联网用户安全。”网易安全专家表示。

事实上，随着互联网巨头联动协作日渐紧密，网络安全问题已得到很大的改善。据介绍，2013 年上半年，互联网企业安全工作组共拦截 2110 万个钓鱼网站，处理不法信息达 8700 万条，拦截木马达到 365 万次，给用户网络信息安全提供了巨大的保障。再以拥有超过 5.7 亿邮箱用户的网易公司为例，其积极推广 DMARC 技术以支持安全工作组成员单位进行反钓鱼工作，已经取得了极大的成果。目前 DMARC 已保护了中国超过 50%的邮箱用户，而且还有越来越多的企业正在部署 DMARC。

业内人士认为，网易等互联网巨头对网络安全普及教育的持续推动，将深化网络安全防范行动的效果和影响，有助于帮助更多网民树立安全上网意识，提高安全防护技术，从而进一步净化网络环境。

知识模块

1.1 网络攻击与防范

计算机网络出现后，在世界范围内得到了迅猛的发展，网络用户数量每年都呈几何级数增长，中国互联网络信息中心（CNNIC）所做的《第 31 次中国互联网络发展状况统计报告》显示，截至 2012 年 12 月底，我国网民规模达 5.64 亿人，网络购物用户规模达到 2.42 亿人，团购用户数为 8327 万人。

在网络应用普及的背景下，网络上的信息安全问题越来越突出，网络攻击事件逐年增长，越来越受到人们的重视。CNNIC《2012 年中国网民信息安全状况研究报告》显示，84.8%的网民遇到过信息安全事件，总人数为 4.56 亿。安全事件中，垃圾短信和手机骚扰电话发生比例最高，分别有 68.3%和 56.5%的网民遇到过，其他事件比例分别为：欺诈诱骗信息（38.2%）、中病毒或木马（23.1%）、假冒网站（17.6%）、账号或密码被盗（13.8%）、手机恶意软件（10.6%）、个人信息泄露（7.1%）。

在电子商务和电子政务飞速发展的今天，网络信息安全问题更是成为关系所有上网用户切身利益的大问题。

1.1.1 常见的网络攻击方式

对常见的网络安全事件进行分析后，可以总结出基本的网络攻击形式有四种：中断、截获、篡改、伪造。

图 1-1（a）表示的是在没有攻击发生的正常情况下，信息从信源传向信宿的过程。

图 1-1（b）表示的是“中断”攻击，它是以可用性作为攻击目标，它毁坏系统资源，切断通信线路，或使文件系统变得不可用。拒绝服务攻击、制造并传播病毒等属于中断攻击。

图 1-1（c）表示的是“截获”攻击，它是以保密性作为攻击目标，非授权用户通过某种手段获得通信信息，如搭线窃听、非法拷贝、截获个人信息等，这种攻击会给通信带来很大的隐患，因为通信双方可能在不知道的情况下已经泄露了机密信息。

图 1-1（d）表示的是“篡改”攻击，它是以信息的完整性作为攻击目标，非授权用户不仅获得对系统资源的访问，而且对文件进行篡改，如改变文件中的数据或修改网上传输的信息等，可以用消息摘要的方式防范这种攻击。

图 1-1（e）表示的是“伪造”攻击，它是以信源的完整性作为攻击目标，非授权用户要么将伪造的数据插入到正常的系统中，要么发布欺诈诱骗信息、假冒网站，要么未经授权使用、获取系统资源和权限。

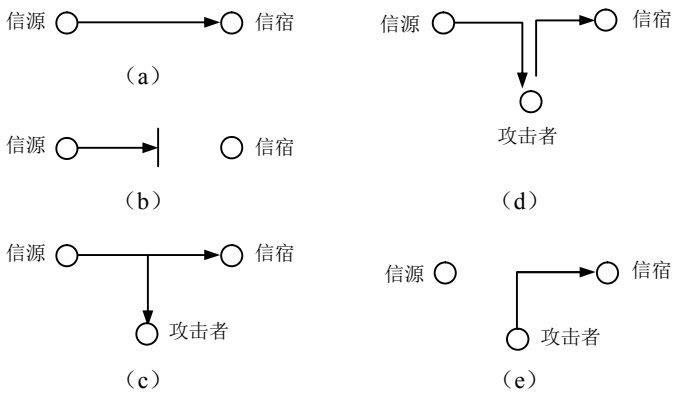


图 1-1　网络攻击的几种形式

1.1.2　网络信息安全的概念

网络信息安全是一个复杂领域，是涉及计算机科学、网络通信、密码学、应用数学、数论、信息论等多学科的综合学科。信息安全又与系统的硬件、软件、网络、数据等复杂系统有关，是与信息、人、组织、网络、环境有关的技术安全、结构安全和管理安全的总和，要求确保信息在存储、处理和传输过程中的可靠性、可用性、保密性、完整性、不可抵赖性和可控性。

（1）可靠性（Reliability）：指信息系统能够在规定条件下和规定时间内完成规定功能的特性。

（2）可用性（Availability）：指信息可被授权实体访问并按需求使用的特性，是系统面向用户的安全性能。

（3）保密性（Confidentiality）：指信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

（4）完整性（Integrity）：指网络信息未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。

（5）不可抵赖性（Non-repudiation）：指在信息交互过程中，确信参与者的真实同一性，即所有参与者都不可否认或抵赖曾经完成的操作和承诺的特性。

（6）可控性（Controllability）：指对信息传播及内容具有控制能力的特性。

为了提供上述安全特性，ISO7498-2 建议的安全机制主要有：

（1）密码机制（Encipherment）：密码技术提供数据或信息交互的保密性，而且对其他安全机制也起着非常重要的基础作用。

（2）数字签名机制（Digital Signature Mechanisms）：应用公钥密码体制，使用私钥进行签名，公钥进行验证，防止否认、仿造、篡改和冒充等安全方面的问题。

（3）访问控制机制（Access Control Mechanisms）：访问控制机制是从计算机系统的处理

能力方面对信息提供保护。防止资源的非授权使用或越权使用。

（4）数据完整性机制（Data Integrity Mechanisms）：通常使用消息摘要加时间戳信息的形式判断消息是否被篡改或重发，消息摘要很多时候使用杂凑函数来产生。

此外还有验证交换机制、业务流填充机制、仲裁机制、可信功能等。

1.2 PKI 的基本概念

1.2.1 基础设施的概念和特点

在学习 PKI 的概念前，我们先了解下一般基础设施的概念。

基础设施一般是由政府提供给公众享用或使用的公共产品，所以经常称为“公共基础设施”。基础设施建设是经济发展的奠基石，在经济学上，是一种“社会先行资本”（Social Overhead Capital，SOC），例如各地的招商引资，在招商之前都要做大量的基础设施建设，以达到吸引资金的目的。基础设施建设也是保障和改善民生的需要，其建设水平直接影响和决定人民的生活水平和质量，影响民众的幸福指数。

基础设施出现在人们生活的方方面面，主要有：

（1）交通。包括：地面交通、航空、水道和港口、联合运输设施、公共交通。

（2）电力。包括：电力生产和电力传送设施，如水电站、煤、石油、天然气发电站、高压电传输线、变电站、电力分配系统和控制中心、服务和保护设施和核电站等。

（3）给水和污水处理设施。包括：给水供应设施，如给水和水处理厂、主要供水线、井、机械和电力设备；供水的构筑物，如大坝、临时性的支路、构筑物、水道和沟渠；污水处理设施，如污水管线、化粪池、污水处理厂。

（4）通信。包括电话网、电视网、无线和卫星网络、信息高速公路网络。

（5）垃圾处理。包括：垃圾填埋、处理厂、循环利用设施。

（6）煤气供应及管道设施。如煤气生产、管道、控制中心、储存柜、维护设施等。

（7）石油运输设施。如输油管道等。

（8）公共建筑设施。包括：学校、医院、政府办公楼、警察局、消防站、邮局、监狱、法庭、剧场、会议中心、展览中心、体育馆、电影院等。

（9）休闲设施。主要是指公园和广场。

分析上述基础设施，不难总结出基础设施的一些共同点：

（1）由可信机构（政府）兴建和管理。

（2）有统一的标准。如电力基础设施中，有统一的供电标准、统一的用电标准（市电 220V 等）、统一的接口规范（电源插座的设计规范等）。网络基础设施中，有统一的数据传输规范、统一的接口规范、统一的网络协议等。

（3）使用便捷（接入）。只要遵循相关设施的使用原则，不同的实体都可以方便地使用

基础设施提供的服务。

（4）根据环境的不同，实现方式可以略有不同。如在网络基础设施中，不同的物理层接口规范等。

（5）不同实现方式之间具有互操作性。如手机可以拨打座机，移动终端上网和台式 PC 上网可以互联等。

（6）支持新的应用扩展。如新的电器设备可以在旧的电力基础设施上应用等。

1.2.2 公钥基础设施的概念

公钥基础设施（Public Key Infrastructure，PKI）是利用公钥理论和技术建立的提供信息安全服务的基础设施，是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的硬件、软件、人员、策略和规程的总和，提供身份鉴别和信息加密，保证消息的数据完整性和不可否认性。

PKI 是一种普遍适用的网络信息安全基础设施，最早是 20 世纪 80 年代由美国学者提出来的概念，实际上，授权管理基础设施、可信时间戳服务系统、安全保密管理系统、统一的安全电子政务平台等系统的构筑都离不开它的支持，是目前公认的保障网络信息安全的最佳体系。

PKI 包括权威认证机构 CA（如政府部门）、证书库、密钥备份及恢复系统、证书作废管理系统、PKI 应用接口系统等主要组成部分。各部分的主要功能如下：

（1）认证机构 CA，是证书的签发机构，它是 PKI 的核心，是 PKI 中权威的、可信任的、公正的第三方机构。

（2）证书库，数字证书的集中管理和存放地，提供公众查询。数字证书（Digital Certificate）就是标志网络用户身份信息的一系列数据，用来在网络通信中识别通信各方的身份，数字证书是一个经证书授权中心数字签名的包含公开密钥（简称公钥）拥有者信息以及公开密钥的文件。证书包含的信息：证书使用者的公钥值、使用者的标识信息、证书的有效期、颁发者的标识、颁发者的数字签名等。

（3）密钥备份及恢复系统，对用户的解密密钥进行备份，当丢失时进行恢复，而签名密钥不能备份和恢复。

（4）证书作废管理系统，当证书由于某种原因（密钥丢失、泄密、过期等）需要作废、终止使用时，将证书放入证书作废列表（CRL）进行管理、存放，提供公众查询。

（5）PKI 应用接口系统，为各种各样的应用提供安全、一致、可信任的接口与 PKI 系统进行交互，确保所建立起来的网络环境安全可信，并降低管理成本。

1.2.3 公钥基础设施的特点

PKI 作为一种信息安全基础设施，其目标就是要充分利用公钥密码学的理论基础，建立起一种普遍适用的基础设施，为各种网络应用提供全面的安全服务。公开密钥密码为我们提供了一种非对称性质，使得安全的数字签名和开放的签名验证成为可能，而这种优秀技术的使用却

面临着理解困难、实施难度大等问题。正如让每个人自己开发和维护发电厂有一定的难度一样，要让每一个开发者完全正确地理解和实施基于公开密钥密码的安全系统有一定的难度。PKI 希望通过一种专业的基础设施的开发，让网络应用系统的开发人员从繁琐的密码技术中解脱出来同时享有完善的安全服务。

PKI 作为基础设施，提供的服务必须简单易用，便于实现。将 PKI 在网络信息空间的地位与电力基础设施在工业生活中的地位进行类比可以更好地理解 PKI。电力基础设施，通过延伸到用户的标准插座为用户提供能源，而 PKI 通过延伸到用户本地的接口，为各种应用提供安全的服务。有了 PKI，安全应用程序的开发者可以不用再关心那些复杂的数学运算和模型，而直接按照标准使用一种插座（接口）。正如电冰箱的开发者不用关心发电机的原理和构造一样，只要开发出符合电力基础设施接口标准的应用设备，就可以享受基础设施提供的能源。

PKI 与应用的分离也是 PKI 作为基础设施的重要特点。正如电力基础设施与电器的分离一样。网络应用与安全基础设施实现分离，有利于网络应用更快地发展，也有利于安全基础设施更好地建设。正是由于 PKI 与其他应用能够很好地分离，才使我们能够将其称为基础设施，PKI 也才能从千差万别的安全应用中独立出来，有效地、独立地发展壮大。PKI 与网络应用的分离，实际上就是网络社会的一次分工，有效促进各自独立发展，并在使用中实现无缝结合。

CA 认证系统要在满足安全性、易用性、扩展性等需求的同时，从物理安全、环境安全、网络安全、CA 产品安全以及密钥管理和操作运营管理等方面按严格标准制定相应的安全策略；要有专业化的技术支持力量和完善的服务系统，保证系统 7×24 小时高效、稳定运行。

1.3 PKI 的功能

PKI 可以解决绝大多数信息安全问题，并初步形成了一套完整的解决方案，它是基于公开密钥理论和技术建立起来的安全体系，是提供信息安全服务的具有普适性的安全基础设施。PKI 体系为网上金融、网上银行、网上证券、电子商务、电子政务、网上交税、网上工商等多种网上办公、交易提供了完备的安全服务功能，这是 PKI 最基本、最核心的功能。

PKI 提供的系统功能是指 PKI 的各个功能模块分别具有的功能，主要包括证书的审批和颁发、密钥的产生和分发、证书查询、证书撤销、密钥备份和恢复、证书撤销列表管理等，这些内容将在第 3 章详细介绍。

PKI 体系提供的安全服务功能主要包括：身份认证、数据完整性、数据机密性、不可否认性、时间戳等。

1. 身份认证

认证的实质就是证实被认证对象是否属实和是否有效的过程，常常被用于通信双方相互确认身份，以保证通信的安全。其基本思想是通过验证被认证对象的某个专有属性，达到确认被认证对象是否真实、有效的目的。被认证对象的属性可以是口令、数字签名或者指纹、声音、视网膜这样的生理特征等。

目前，实现认证的技术手段很多，通常有口令技术+ID（实体唯一标识）、双因素认证、挑战应答式认证、著名的 Kerberos 认证系统，以及 X.509 证书及认证框架。这些不同的认证方法所提供的安全认证强度不一样，具有各自的优势和不足，以及所适用的安全强度要求的应用环境也不一样。

PKI 的认证技术使用的是基于公钥密码体制的数字签名。PKI 体系通过权威认证机构 CA，为每个参与交易的实体签发数字证书，数字证书中包含证书所有者、公开密钥、证书颁发机构的签名、证书的有效期等信息，私钥由每个实体自己掌握并防止泄密。在交易时，交易双方就可以使用自己的私钥进行签名，并使用对方的公钥对对方的签名进行认证。

2. 数据完整性

数据完整性就是防止篡改信息，如修改、复制、插入、删除等。在交易过程中，要确保交易双方接收到的数据和从数据源发出的数据完全一致，数据在传输和存储的过程中不能被篡改，否则交易将无法完成或所做交易违背交易意图。

但直接通过观察原始数据的状态来判断其是否改变，在很多情况下是不可行的。如果数据量很大，将很难判断其是否被篡改，即完整性很难得到保证。在密码学中，通过采用安全的杂凑函数（散列函数，Hash 函数）和数字签名技术实现数据完整性保护，特别是双重数字签名可以用于保证多方通信时数据的完整性。这种方法实际就是通过构造杂凑函数，对所要处理的数据计算出固定长度（如 128bit）的消息摘要或称消息认证码（MAC）。Hash 算法的特点决定任何原始数据的改变都会在相同的计算条件下产生不同的 MAC。这样我们在传输或存储数据时，附带上该消息的 MAC，通过验证该消息的 MAC 是否改变，可高效、准确地判断原始数据是否改变，从而保证数据的完整性。

Hash 算法的设计依赖于构造合理的杂凑函数。可以设计专用的 Hash 算法，例如，目前比较成熟的、标准的 Hash 算法有 SHA-l、MD5 等，也可以通过标准的分组密码算法来构造 Hash 算法。在实际应用中，通信双方通过协商以确定使用的算法和密钥，从而在两端计算条件一致的情况下，对同一数据应当用相同的算法来计算以保证数据不被篡改，实现数据的完整性。

3. 数据机密性

数据机密性就是对传输数据进行加密，从而保证数据在传输和存储过程中，未授权的人无法获取真实的信息。数据的加解密操作通常用到对称密码，这就涉及到会话密钥分配的问题，PKI 体系下进行密钥分配可以通过公钥密码分配方案很容易地解决。

4. 不可否认性

不可否认性是指参与交互的双方都不能事后否认自己曾经处理过的每笔业务。具体来说主要包括数据来源的不可否认性、发送方的不可否认性，以及接收方在接收后的不可否认性，还有传输的不可否认性、创建的不可否认性和同意的不可否认性等。PKI 所提供的不可否认功能是基于数字签名及其所提供的时间戳服务功能的。

在进行数字签名时，签名私钥只能被签名者自己掌握，系统中的其他参与实体无法得到该密钥，因此只有签名者自己能做出相应的签名，其他实体是无法做出这样的签名的。这样，

签名者从技术上就不能否认自己做过该签名。为了保证签名私钥的安全，一般要求这种密钥只能在防篡改的硬件令牌上产生，并且永远不能离开令牌，以保证签名私钥的安全。

再利用 PKI 提供的时间戳功能，来证明某个特别事件发生在某个特定时间或某段特别数据在某个日期已存在。这样，签名者对自己所做的签名将无法进行否认。

5. 时间戳

时间戳也叫做安全时间戳，是一个可信的时间权威，使用一段可以认证的完整数据表示的时间。最重要的不是时间本身的精确性，而是相关时间、日期的安全性。支持不可否认服务的一个关键因素就是在 PKI 中使用安全时间戳，也就是说，时间源是可信的，时间值必须特别安全地传送。

PKI 中必须存在用户可信任的权威时间源，权威时间源提供的时间并不需要正确，仅仅供用户作为一个参照“时间”，以便完成基于 PKI 的事物处理，如事件 A 发生在事件 B 的前面等。一般的 PKI 系统中都设置一个时钟系统来统一 PKI 的时间。当然也可以使用世界官方时间源所提供的时间，其实现方法是从网络中的这个时钟位置获得安全时间。要求实体在需要的时候向这些权威请求在数据上盖上时间戳。一份文档上的时间戳涉及到对时间和文档内容的杂凑值（哈希值）的数字签名，而权威的签名提供了数据的真实性和完整性。

虽然安全时间戳是 PKI 支撑的服务，但它依然可以在不依赖 PKI 的情况下实现安全时间戳服务。一个 PKI 体系中是否需要实现时间戳服务，完全依据应用的需求来决定。

1.4 PKI 的发展概况

自 20 世纪 80 年代，美国学者提出了 PKI 的概念以来，PKI 已经经过了 30 多年的发展历史，下面简要回顾具有标志性意义的时间节点，以加深对 PKI 发展的了解。

1996 年，美国成立了联邦 PKI 指导委员会，以推进 PKI 的开发、应用。

1996 年，由 Visa、MasterCard、IBM、Netscape、MS、数家银行推出 SET 协议，推出 CA 和证书概念。

1999 年，PKI 论坛成立，制定了 X.500 系列标准。

2000 年 4 月，美国国防部宣布采用 PKI 安全倡议方案。

2001 年 6 月 13 日，在亚洲和大洋洲推动 PKI 进程的国际组织宣告成立，该国际组织的名称为“亚洲 PKI 论坛”，其宗旨是在亚洲地区推动 PKI 标准化，为实现全球范围的电子商务奠定基础，其成员包括日本、韩国、新加坡、中国、中国香港、中国台北和马来西亚。论坛呼吁加强亚洲国家和地区与美国 PKI 论坛、欧洲 EESSI 等 PKI 组织的联系，促进国际间 PKI 互操作体系的建设与发展。

1996－1998 年，国内开始电子商务认证方面的研究，中国电信率先派专家到美国学习 SET 认证安全体系。

1997 年 1 月，科技部下达任务，中国国际电子商务中心（外经贸委）开始对认证系统进

行研究开发。

1999 年，上海 CA 中心开始试运行。

1999 年 10 月 7 日，《商用密码管理条例》颁布。

1999－2001 年，中国电子口岸执法系统建设完成。

2000 年 6 月 29 日，中国金融认证中心 CFCA 挂牌成立，是经中国人民银行和国家信息安全管理机构批准成立的国家级权威的安全认证机构，也是《中华人民共和国电子签名法》颁布后，我国首批获得电子认证服务许可的电子认证服务机构之一。

国内 PKI 发展有过一段过热期，先后建设了大小 70 多家 CA，目前常用的在 10 家左右。全国性的 CA 有金融 CA、电信 CA、海关 CA 等；地方性的 CA 有北京 CA、上海 CA、福建 CA、山东 CA 等，各自的应用领域不尽相同。

多数 CA 采用的都是国内厂商的技术，CFCA 采用的是加拿大 Entrust 公司的技术，核心加密部分实现国产化。目前来看国外的安全技术依然高出国内相当水平。

1.5 典型应用案例

1.5.1 网上银行应用

网上银行业务是指商业银行将其传统的柜台业务拓展到 Internet 上，用户访问其 Web Server 进行在线查询、转账、汇款、支付等业务。随着电子商务的普及，网上银行的 PKI 应用也越来越普及，其应用示意图如图 1-2 所示。

在进行网上银行业务时，用户对其发出的指令用其签名私钥进行签名，银行校验签名，并且保存此次签名，从而使银行用户所发出的指令具有不可抵赖性，签名及校验的过程保证了用户指令的真实性和完整性；用户发出的交易内容用指定银行的公钥进行加密，银行用银行私钥才能解秘，此环节保证了银行指令信息的私密性。这样在整个交易的过程中确保了网上信息安全。

网上银行的证书应用也分证书管理和证书应用两部分。证书管理中心 CA 和注册审核机构 RA 一般设立在银行的总部，也是个多层的结构，其使用操作员证书进行证书相关的管理操作。证书应用是和其网银应用结合在一起的，将安全部分嵌入到网银中，这中间包括互相交换证书、验证身份、建立安全通道、加密、数字签名等应用操作。

网上银行的证书应用模式大同小异，真正的差别还是取决于具体业务的应用。网上银行应用具有如下特点：

- 客户端和银行服务器端各自自动进行黑名单（CRL）查询，减少交易风险。
- 双重密钥（加密密钥、签名密钥）支持数字签名的不可否认性。
- 高强度加密机制（对称 128 位，非对称 1024 位）保证数据传输保密性强。
- 具有完善的密钥和证书生命周期管理，客户端证书到期前，可自动进行更新，不需人

工办理任何手续，极大地方便了用户。

- 客户端、服务器端操作简便，透明性强。

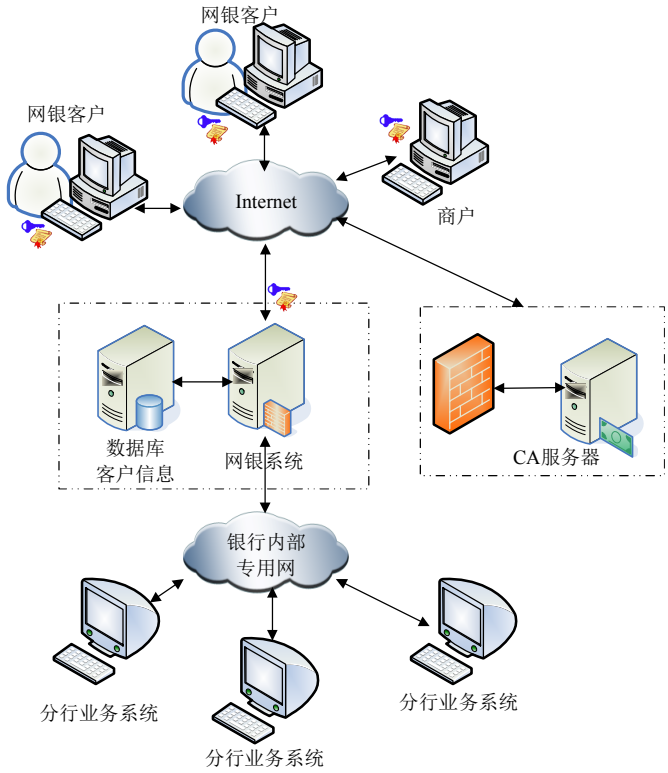


图 1-2　网上银行应用示意图

1.5.2　税务网上申报缴税

国税证书签发中心 CA 与国税系统的网络连接采用 DDN 专线的方式，国税 CA、RA 和 CFCA 都在 CFCA 内部网中进行管理，如图 1-3 所示。

证书发放管理由操作员（LRA）来进行，只要具有操作员证书及上网的条件就可以安全地连接到 RA 系统。网上缴税证书发布流程如下：①操作员安全登录到 RA 系统；②输入需要制作证书的纳税人识别号；③RA 系统将相关的请求发送到国税发行平台查询并返回相关信息；④CA 系统接收制证请求并签发证书；⑤操作员获得证书存放到存储介质中封装并分发。纳税人凭借证书及个人私钥就可以登录 Web Server 进行网上申报缴税。

1.5.3　网上证券交易

网上证券交易可分为网上炒股和网上银证转账，网上炒股是股民和证券公司之间发生的

两方交易。网上银证转账是指股民通过因特网将资金在银行股民账户和证券公司账户之间划入或划出，是涉及到股民、证券公司、银行的三方交易。

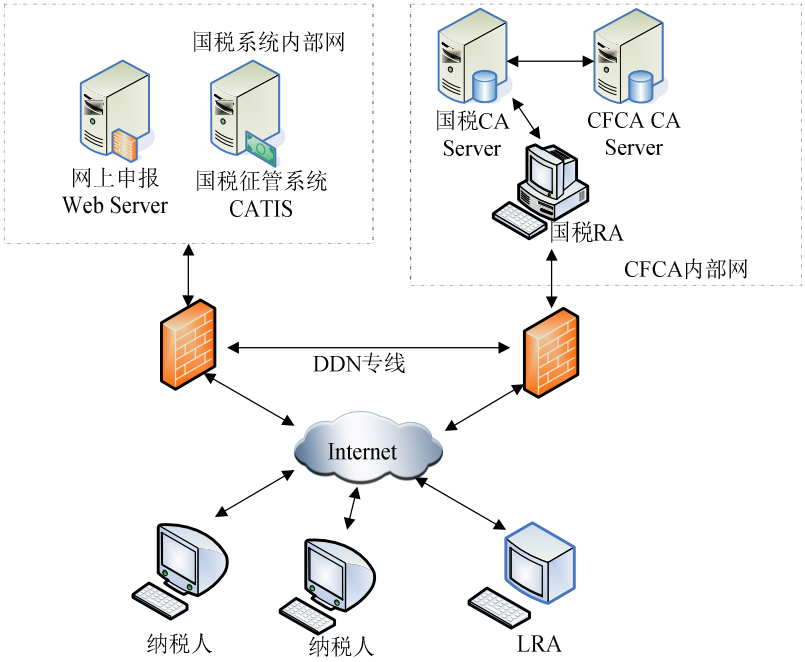


图 1-3　国税 CA 网络连接示意图

股民在使用证书进行网上交易时，对其网上交易指令也要进行加密和签名，以确保交易数据的有效性、机密性、完整性和不可抵赖性。网上证券交易对交易的实时性和方便性要求比较高，应用 CFCA 证书可以较好地解决安全和效率之间的矛盾。

实际的做法是在证券公司总部设立 RA，将证书的申请、使用、管理等功能集成到客户端软件中去。客户申请开通网上交易并下载使用证书后，在一定的时间去签署一份书面的协议即可正常使用。

学习项目

1.6　项目一　身份认证安全性演示

1.6.1　任务 1：在 DOS 环境中调试远程登录 Telnet 命令

实训目的：让学生掌握如何在 DOS 环境下进行远程登录，理解其安全性。

实训环境：装有 Windows XP 及以上操作系统的计算机

●项目内容

远程登录（Telnet）是 Internet 的一种特殊服务，它是指用户使用 Telnet 命令，通过网络登录到远在异地的主机系统，把用户正在使用的终端或主机虚拟成远程主机的仿真终端。仿真终端等效于一个非智能的机器，它只负责把用户输入的每个字符传递给主机，再将主机输出的每个信息回显在屏幕上，从而使用户可以像使用本地资源一样使用远程主机上的资源。提供远程登录服务的主机一般都位于异地，但使用起来就像在身旁一样方便。

使用 Telnet 登录远程计算机有以下几种方式：

1. 远程登录（Telnet）服务

使用 Telnet 一般分为三步：

（1）在本地主机登录。

（2）运行本地的 Telnet 程序，在“运行”对话框中或命令提示符下执行 Telnet。

（3）与远程主机 192.168.0.65 建立连接，如图 1-4 所示。即可执行远程计算机上的各种命令。

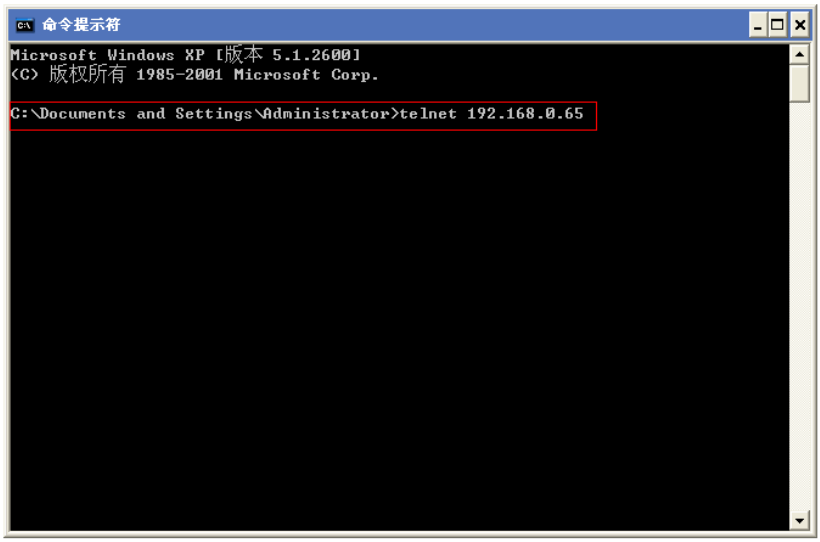


图 1-4　远程登录

2. 用 IE 浏览器方式登录远程主机系统

打开 IE 浏览器，在地址栏中输入：telnet://<远程主机名>，如 telnet://192.168.0.65，即可打开超级终端窗口，同时打开远程主机，在登录后便可以使用远程资源。

登录后试验 Telnet 的常用命令：

（1）open

格式：open hostname

用它来建立到主机的 Telnet 连接，要求给出目标机器的名字或 IP 地址。如果未给出机器名，Telnet 就将要求你选择一个机器名，如果连接到了远程主机，系统将提示你输入用户名和密码，只有输入正确的用户名和密码才能登录成功。

（2）display

使用 display 命令可以查看 Telnet 客户端的当前设置。

（3）close

close 命令用来终止远程连接，但并不中止 Telnet 程序的运行。

（4）quit

quit 命令用来终止 Telnet 程序。若一个远程连接程序仍是运行的，quit 也将会终止它。

1.6.2 任务 2：在 Windows 环境中调试远程桌面功能

实训目的：让学生掌握在 Windows 环境中调试远程桌面功能，登录远程系统。

实训环境：装有 Windows XP 及以上操作系统的计算机。

●项目内容

1. 用远程桌面登录远程系统

（1）远程登录机器：右击“我的电脑”→“属性”→“远程”标签→勾上“允许用户远程连接到此计算机”，如图 1-5 所示。

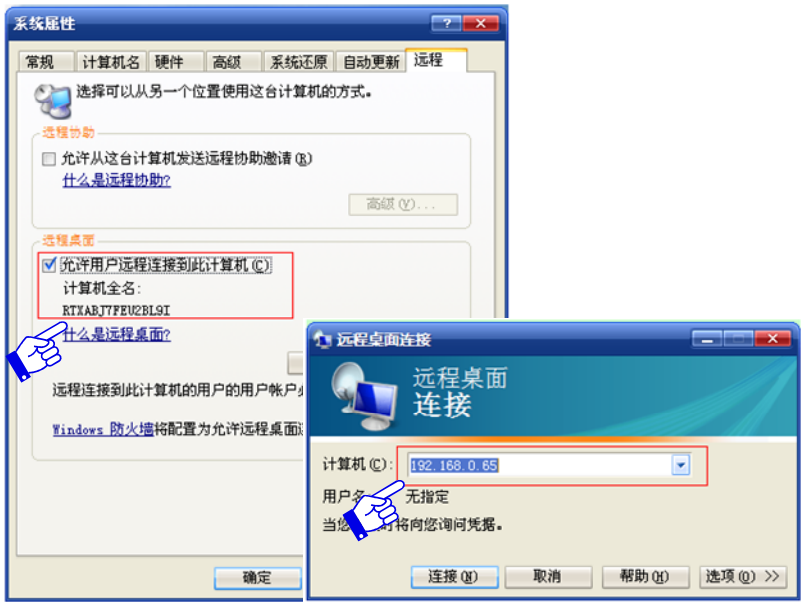


图 1-5　远程桌面连接

（2）登录远程计算机：“开始”→“程序””→“附件”→“通讯”→“远程桌面连接”

→输入远程计算机 IP→输入用户名和密码，如图 1-5 所示。

2. 用超级终端窗口式软件登录远程主机系统

单击“开始”→“程序”→“附件”→“通讯”→“超级终端”→“新建连接”→输入连接的名称，单击“确定”→选择连接时使用：TCP/IP（Winsock）→输入主机 IP 地址，单击“确定”→输入用户名、密码（注：这是使用的是 Windows 操作系统的 Server 版本自带的“超级终端”软件，也可以使用其他终端软件）

1.6.3 任务 3：登录腾讯 QQ 聊天软件调试远程协助功能

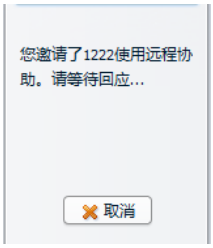
实训目的：让学生掌握互联网环境下如何进行远程协助，并理解其安全性。

实训环境：装有 Windows XP 及以上操作系统的计算机，计算机需要接入 Internet。

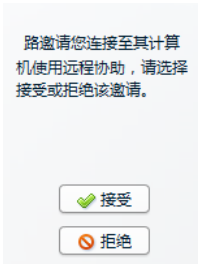
●项目内容

QQ 有远程协助功能，主要操作过程如图 1-6、图 1-7 所示。需要注意的是，受控方主动邀请控制方进行远程控制，而控制方接受受控方邀请。双方协商一致后，被邀请方即获得邀请方桌面的控制权，可以进行远程协助。

图 1-6 远程协助按钮



（a）邀请方界面



（b）被邀请方界面

图 1-7 会话双方的界面

知识巩固

一、选择题

1. 网络安全的基本属性是（ ）。

A. 机密性 B. 可用性 C. 完整性 D. 上面 3 项都是

2．Telnet 协议主要应用于哪一层（　　）。

A．应用层　　B．传输层　　C．Internet 层　　D．网络层

3．在制定网络安全策略时，经常采用的思想方法是（　　）。

A．凡是没有明确表示允许的就要被禁止

B．凡是没有明确表示禁止的就要被允许

C．凡是没有明确表示允许的就要被允许

D．凡是没有明确表示禁止的就要被禁止

4．信息被（　　）是指信息从源结点到目的中途被攻击者非法截获，攻击者在截获的信息中进行修改或插入欺骗性的信息，然后将修改后的错误信息送给目的结点。

A．伪造　　B．窃听　　C．截获　　D．篡改

5．（　　）是指保证存储在连网计算机上的信息不被未授权用户非法使用。

A．信息存储安全　　B．信息传输安全 C．信息转换安全 D．信息加工安全

二、名词解释

保密性　完整性　可用性　可控性　非否认性　防火墙　PKI

三、简答题

1．说出信息安全，计算机安全和网络安全的关系？

2．你有没有网上购物的经历？有没有想过交易过程中的安全保障问题？