应用密码学实践书籍

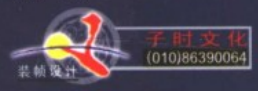
OpenSSL与网络信息安全

——基础、结构和指令

王志海　童新海　沈寒辉　编著

清华大学出版社
北京交通大学出版社

责任编辑：刘 洵

封面设计： 

· 俞兆君

OpenSSL与网络信息安全

——基础、结构和指令

2007

ISBN 978-7-81123-006-2

9 787811 230062 >

定价：26.00元

OpenSSL 与网络信息安全
——基础、结构和指令

王志海　童新海　沈寒辉　编著

清华大学出版社
北京交通大学出版社
· 北京 ·

内 容 简 介

本书结合 OpenSSL 的结构和应用指令，对密码算法、公钥基础设施、数字证书和密码应用协议等内容进行了全面的具体阐述。本书试图通过对 OpenSSL 的具体介绍，一方面让读者能够熟悉和掌握 OpenSSL 这个强大的工具库，另一方面更希望读者能够在实践中深入理解密码学理论、思想及其相关应用的实质。

本书共分 12 章。第 1 章对密码学理论、密码学相关应用和本书的情况作了一个概要的说明；第 2～3 章主要介绍密码学的基本概念、密码技术的基本实现、对称加密算法、公开密钥算法和单向散列函数算法等密码学知识；第 4～6 章介绍 OpenSSL 的结构、编译和安装方法及其使用的基本概念；第 7～12 章是本书的重点，详细介绍了 OpenSSL 的应用程序（指令）的使用方法和各项参数的意义。

本书可以作为密码技术设计研发人员的参考书籍，在校的本科学生、研究生入门级的密码学和信息安全技术方面的参考书籍，还可以作为信息安全培训和密码技术培训教材。

图书在版编目（CIP）数据

OpenSSL 与网络信息安全：基础、结构和指令/王志海，童新海，沈寒辉编著. —北京：清华大学出版社；北京交通大学出版社，2007.4

ISBN 978－7－81123－006－2

Ⅰ. O…　Ⅱ. ①王…　②童…　③沈…　Ⅲ. 计算机网络-安全技术　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 051086 号

责任编辑：刘　洵
出版发行：清 华 大 学 出 版 社　邮编：100084　电话：010－62776969　http：//www.tup.com.cn
　　北京交通大学出版社　邮编：100044　电话：010－51686414　http：//press.bjtu.edu.cn
印 刷 者：北京瑞达方舟印务有限公司
经　　销：全国新华书店
开　　本：185×260　印张：16.25　字数：362 千字
版　　次：2007 年 4 月第 1 版　2007 年 4 月第 1 次印刷
书　　号：ISBN 978－7－81123－006－2/TP・345
印　　数：1～4 000 册　定价：26.00 元

前　言

近几年来，密码学得到了越来越广泛的应用和关注，例如新出现的内网安全、SSL VPN、网上银行安全和数据保密等新安全热点领域，都离不开密码技术。密码技术为什么能够在短短几年内得到如此强烈的关注，究其背景，主要在两个方面：一是随着信息化程度的提高，对信息安全的控制越来越细致，甚至已经深入到文件级的数据单元，简单的安全控制措施已经不能满足要求，而密码技术由于其先天的完整理论体系备受青睐；二是由于近年来国内外接触密码技术的研发设计人员越来越多，密码技术的应用有了一定的群众基础。

在中国乃至世界密码技术的推广应用中，OpenSSL 的功劳是不可忽视的，目前涉及密码技术的产品，相当大一部分直接或者部分引用了 OpenSSL 的类库或者例程。对于密码技术的研发设计人员，没有听说过 OpenSSL 的更是少之又少。目前国内外和密码技术、公钥基础设施（PKI）相关的资料，大部分偏重理论、数学算法和协议介绍，与实际应用尚有一段差距，不利于普通研发设计人员对密码技术的理解和应用。鉴于此，笔者自 2002 年创办 www. OpenSSL. cn 以来，便一直试图结合 OpenSSL 本身丰富的内容和应用，对密码技术进行理论结合实际的疏理，试图编写一本简单易懂的密码技术入门资料。

《OpenSSL 与网络信息安全——基础、结构和指令》一书从分析介绍 OpenSSL 本身的体系结构、设计思想和应用程序（指令）入手，让读者逐步领会密码学、公钥基础设施（PKI）及相关应用协议等方面的理论内涵、设计思想、应用场景及实现方法等，能够将编程开发工作和密码学理论联系起来，从而融会贯通。阅读本书，要想取得上述的效果，需要从两方面着手：一是提前阅读密码学理论和公钥基础设施方面的资料；二是阅读本书的时候，一定要结合 OpenSSL 的实际环境，多动手。

本书完成历经近四年，非常缓慢，除了个人事务繁多的因素外，更主要的是由于其中很多细节之处，都需要试验和编程来进行仔细的考究。在本书的编写过程中，虽然笔者力求做到仔细，但是错误肯定还是难以避免，希望同行们在阅读的过程中发现后能够及时在 www. OpenSSL. cn 网站上更正，假若能告知我们，那就更不胜感谢！

王志海

2007. 4

目　录

第 1 章

概　述

1.1 信 息 安 全

信息安全是本书要解决的主要问题，本节将介绍信息安全的基本概念和本书将要涉及的信息安全的内容。

1.1.1 信息安全概念

信息安全是自古以来就存在的概念，比如以前为了保证传递书信的保密性，使用腊封或其他方式将书信封装在信封内；还有使用暗号口令确认接受信息的人的身份等方法。需要注意的是，信息安全技术是跟信息的载体形式和传送媒介密切相关的，信息载体的变化和信息传送媒介的变化必然会导致信息安全技术的变化发展。

在过去的二十多年中，信息技术取得了令人惊异的发展，越来越多的有价值的信息和资料以数字信息存放在计算机等数字信息存储设备中。与此同时，信息共享技术也获得了巨大的突破，以 Internet 的发展为代表，短短的时间内，从美国军方的一个专用网络发展到联系着全世界千千万万人的庞大信息网络。这些客观的变化导致对信息安全的要求发生了重大的变化。

随着信息数字化及计算机应用的发展，对存储在计算机中的文件和其他数字信息的保护需求成为了一种必然，尤其对一个能够通过公共网络进入的共享系统来说，这种需求显得尤为迫切。针对这种需求，目前发展起来的技术有防病毒技术和防火墙技术，等等。有些文献将这些保护数据、阻挡非法数据访问的技术统称为计算机安全技术或系统安全技术。

信息安全技术的另外一个重要变化是由网络和通信设施的产生和应用引起的。这些网络和通信设施用于在用户的各种终端及计算机之间传输数据信息，这种传输过程很容易受到非法窃听等攻击，这就需要对在网络中传输的数据采取安全的保护措施。针对这种需求发展起来的技术有 VPN、SSL 等。有些文献将这种类型的技术统称为网络安全技术。

事实上，因为现在的绝大部分数据终端设备（包括计算机）基本上都是跟网络相联的，所以无论是计算机安全、系统安全还是网络安全，都不是完全相互独立的。而且，这些名词由于其笼统性，反而有概念不清和误导的可能。所以，本书更愿意用具体一点的技术名词来说明不同的信息安全技术。

本书关注的是使用基于密码学原理来进行数据信息保护的技术，尤其偏向于利用该技

术保护在网络中传输的数据。对于防火墙、防病毒及入侵检测（IDS）等技术涉及的安全问题和解决方案，本书不作介绍。在本书后面的章节中，如果没有特别指明，信息安全的范围仅仅包括使用基于密码学原理来进行数据信息保护的安全技术。

1.1.2 信息安全内容

正如 Bruce Schneier[2] 所说，安全问题就如一条链子一样，必须保证每一个环节的安全才能达到使整个链子具有安全性。所以，在解决任何一个实际的或抽象的系统的安全问题之前，都应该首先分析其可能存在的安全缺陷，进而采取相应的安全措施。为了使读者了解本书涉及的领域和需要解决的问题，下面介绍一下与本书内容相关的安全问题，并举一些相关的安全漏洞的例子，加深读者的理解。

（1）机密性

机密性是指保护信息免受主动的非法窃取、阅读等攻击。在信息数字化之前，信息的机密性是依靠严格的管理制度和强大的物理手段来实现的，如戒备森严的房子和难以破坏的保险箱。对于独立的设备（没有联网的计算机）中的数字信息，当然也可以依赖传统的保密手段，但是对于一般的共享系统或联网的系统来说，传统的方法就显得难以胜任，必须采用新的针对数字信息的手段。

机密性涉及的内容是多方面的，主要包括内容的机密性和信息量的机密性。

内容的机密性是很容易理解的，就是确保数字信息的内容不被没有授权的人访问。内容的机密性既可以针对计算机中的一个重要文件，也可以针对网络中传输的一些数据。对于计算机中的一个文件内容的保护显得可能简单一点，最简单的处理方法是只需要采用足够强大的加密算法将文件的内容加密即可。对于网络上传输的信息的保护，需要考虑的情况就会多一点，其中之一就是可能需要考虑对数据做不同层次的保护。比如，对一般的计算机之间的通信，可能只是选择其中重要的数据信息进行保护；而对于机密性要求非常高的办公室之间的两台计算机，可能会对它们之间传输的所有数据都进行保护。

信息量的机密性源于网络传输中通信量分析技术的产生，但本书认为不仅仅限于网络通信量的分析，在本地的计算机系统中，一样存在类似的安全危险，本书将它们统称为信息量的机密性。采用通信量分析进行攻击要求攻击者能够在通信设施上监听到通信的源地址和目的地址、通信频度、通信的数据长度、通信的时长等特征。对于本地计算机系统中的普通加密保护的文件，一样可以通过获取文件的长度信息、修改时间来获得有用的信息。更进一步，对一些结构化的文件，可以通过分析其各个结构的长度信息等来获得更多有用的信息，比如对加密数据库中各个字段长度的分析就可能得到大量的有用信息。信息量的分析还可以针对计算机系统中运行的程序，比如对加密程序的攻击就已经成功破解了 RSA 私钥。信息量的机密性在以前远远没有得到重视，但在今后的时间里，随着其相关攻击手段和事件的增加，必然会得到更大的发展。

（2）完整性

完整性是指确保信息没有被修改，也可以防止假冒的信息。对于一个计算机中存储的信息来说，完整性的概念就是确保信息在存储的过程中没有被非法进行修改或替换。

对于网络信息来说，情况就复杂多了，主要分成面向连接和无连接两种情况。对于面向连接的情况来说，完整性是针对信息流的服务，它需要确保接收到的信息和发送的信息

是一样的，没有被篡改、插入、重排序、重复或者延迟，同时也要确保通信结束后数据在网络上的销毁。所以，面向连接的完整性服务不仅仅可以确保消息没有被非法篡改，还可以在一定程度上防止拒绝服务攻击（DOS）。对于无连接的网络信息传输来说，完整性的内容跟计算机系统中的文件对象完整性含义是一样的，即保护信息没有被篡改或替换。

(3) 鉴别

鉴别是指确认访问者的身份或消息的来源，防止冒充他人的行为发生。对于计算机中存储的信息来说，鉴别的功能就是确保访问者的身份，如最简单的是使用口令和密码来确保访问者的身份，安全一点的解决方案是通过 USB Key、IC 卡或其他形式的令牌进行身份鉴别。

对于网络传输中的信息来说，鉴别所需要确认的对象有很多种，可能是消息传输操作的用户，也可能是特定的应用程序，也可能是特定的 IP 地址，有时候可能是这些特征的综合，本书统称这些为实体。也就是说，在网络传输信息的过程中，鉴别的功能首先是确保通信双方的两个实体都是可信的，都是它们所宣称的实体；其次，鉴别还要确保在信息传输的过程中防止第三方假冒两个合格方的任何一方来达到未授权接收信息或发送信息的目的。

(4) 抗抵赖

抗抵赖是指保证消息的制造者或发出者不能在事后否认他制作或发出的消息。对于计算机中存储的信息，抗抵赖的功能就是确保文件在被合法授权用户修改后该用户不能否认自己做过这样的修改。这在传统的书面文件中，可以使用手写签名来解决这个问题，相应地，对于数字信息，可以使用数字签名来达到相同的目的。

对于网络信息传输的过程而言，抗抵赖的功能要求接收方能够验证消息的发送方，同时要求发送方能够验证消息的接收方，并能够在发生争议后向第三方（比如法庭）证明消息的发送方或接收方。

(5) 攻击举例

为了进一步说明上述四种信息安全措施的必要性，下面举一些有针对性的攻击例子，加深读者的理解。

Susn 使用 Mail 通过 Internet 向 Tom 传送一个带有机密信息的文件，但是由于没有使用安全措施保护该传送的信息，与 Susn 在同一公司局域网内工作的怀有不良目的 Jim 通过使用 Sniffiner 监听了 Susn 发送 Mail 的整个过程，因为 Internet 上的信息是明文传送的，所以 Jim 成功获取了这个带有机密信息的文件。这是一个针对机密性攻击的例子。

Susn 是公司的总裁，她想给表现不错的 Eric 加 2 000 元工资，起草了一份电子文件，叫秘书 Anna 发给财务部。Anna 是 Jim 的女朋友，而 Jim 正好跟 Eric 在同一个部门，于是 Anna 就将电子文件的名字 Eric 改成了 Jim，然后发给财务部，后果可想而知。这是针对完整性攻击的例子。

计算机 Server 上存有公司重要的客户资料，只有公司的客户部部门经理 Tom 有权限访问这些重要资料。Jim 是该公司一个员工，他准备跳槽，为了获得更多的客户资料，他一直想访问 Server 上的客户资料。有一天 Jim 无意中获得了 Tom 的账号和密码（偷看的），然后就连接上 Server，告诉 Server 是 Tom 要访问客户资料，并按 Server 的要求输入了密码，顺利取得了想要的客户资料。这是针对鉴别攻击的例子。

Jim 在一个电子商务网站购买了一台笔记本电脑，并通过网络告诉银行从自己的账户

给电子商务网站转账。Jim在取得笔记本电脑后，发现自己其实并不需要笔记本电脑，但是退货已经不可能，于是就打算抵赖，他跟银行说自己其实并没有购买笔记本，是别人冒充了他，银行要负责任。如果银行没有一套针对这种情况的措施和方法，情况就会很麻烦。这是针对抗抵赖攻击的一个例子。

上述只是举了一些攻击的简单例子，事实上，实际的情况可能复杂得多，涉及的攻击可能也是多方面的。这些攻击采取的措施都是基于密码学原理的，下面本书将要介绍密码学的基本知识。

1.2 密 码 学

本节将概要地介绍密码学的功能、内容和应用，使读者对密码学有一个初步的了解。

1.2.1 密码学作用

最原始的密码学的作用是进行信息保密，即解决前面所述的机密性问题。但现代发展起来的密码学的作用已经远远超出了这个范围，它可以用来解决包括机密性、完整性、鉴别及抗抵赖相关的各种难题，囊括了本书前面介绍的各种安全问题。

机密性问题是密码学最早关心的问题，也是核心的问题。目前针对机密性问题，密码学提出了各种算法，主要分为对称加密算法和公开密钥算法。不管是什么算法，都是为了在各种复杂和苛刻的条件下实现信息保密的功能。对称加密算法主要适用于通信双方已经共享了秘密的密钥的情况，而公开密钥算法则适用于通信双方没有共享的密钥的情况。目前常用的对称加密算法有DES，3DES，AES，等等，常用的公开密钥算法有RSA、DH算法，等等。

完整性问题在现代密码学中也得到了较好的解决，主要是采用了散列函数和数字签名相结合的算法。散列函数是一种单向映射函数，是密码学中确保数据完整性的核心算法，目前常用的有MD5，SHA和SHA1算法，等等。

鉴别问题和抗抵赖问题在密码学中的解决不仅仅依赖密码算法本身，还依赖一套严格执行的密码协议或网络协议。这些协议以密码算法为基础，达到了鉴别和抗抵赖的功能。虽然设计一个好的密码协议并非如想像的那么容易，但目前密码协议还是种类繁多，我们熟悉的有Kerberos，SKID等，网络协议有SSL，SET等。这些协议基本上都具备了鉴别和抗抵赖的功能。

1.2.2 密码学内容

目前现代密码学基本可以分为两大部分：密码算法和密码协议。密码协议是在密码算法的基础上实现的，但其完成的功能比单一的密码算法所能完成的功能丰富得多。

密码算法根据其完成的功能可以分为对称加密算法、公开密钥算法、数字签名算法及信息摘要（散列函数）算法。对称加密算法主要完成了明文数据到密文数据的转换功能，其加密密钥和解密密钥是相同的。公开密钥算法完成的功能跟对称加密算法是相同的，但是其加密密钥和解密密钥不相同。数字签名算法的功能是实现鉴别和抗抵赖的功能，其具体的实现有时候可以采用对称加密算法或公开密钥算法实现，也有专门设计用于数字签名

的算法。信息摘要算法主要是实现将大量的信息不可逆映射成一段定长或较短的信息而基本保持其独特性。所谓独特性，也就是说不同的信息经过相同的信息摘要算法映射后得到的结果应该是不同的。

密码协议是基于密码学的协议，它包含了某种密码算法，但通常不仅仅是为了加密，而是为了更加复杂的特定目的设计的。参与协议的各方可能是各种各样的人，可能是相互信任的朋友，也可能是敌人，他们的目的可能是为了共享秘密、确定相互身份或者共同签署合同。在密码协议中使用密码算法一般来说是为了防止和发现窃听、攻击和欺骗等。

1.2.3 密码学应用

随着网络尤其是 Internet 的发展，密码学的应用已经越来越广泛。目前主要的应用领域有电子商务、电子政务、私人邮件、Web 安全访问及虚拟专用网（VPN），等等。

电子商务是密码学迄今为止应用最成功的领域之一，主要涉及网络交易中的保密性、身份鉴别、完整性及抗抵赖等功能。例如用户在某电子商务网站使用信用卡进行购物时，必须保证整个过程是保密的而且是安全的，对于电子商务网站和银行来说，也必须确保用户的身份是可信的，并且能够向第三方证明用户确实执行了相关的操作。目前电子商务中成功的协议之一是 SET 协议。

电子政务及办公自动化系统的使用已越来越广泛，与之密切相关的安全性也出现了需求。比如公文的签发，需要数字签名，用户权限的控制需要进行身份确认，等等。

电子邮件是普通网络用户使用最为广泛的 Internet 工具，因为邮件涉及个人隐私等机密信息，所以保护电子邮件的安全早就成为了一个热点话题。目前，安全邮件系统 PGP 取得了很大的成功。PGP 不仅仅实现了邮件信息在网络传输中的机密性，而且能够建立用户之间的信任关系，确认用户的身份，并保证邮件信息的完整性。

Web 已经成了信息发布的一条重要途径，一些企业可能希望一些重要的资料文件不被未经授权的用户访问，另一方面，用户为了安全可能也需要验证服务器的身份。SSL 协议是解决这种需要的一个成功协议之一。

虚拟专用网技术（VPN）是解决大型的地理位置分布分散的公司或机构的低成本联网方案，该技术使用密码算法和密码协议通过 Internet 建立起分支机构之间的虚拟专用网络，使得各分支机构之间能够安全地进行通信。

1.3 公钥基础设施

公钥基础设施（PKI）是近年来受到非常多关注的一项技术，本节介绍公钥基础设施的基本概念及其组件，并介绍数字证书的基本作用。

1.3.1 公钥基础设施的必要性

公钥基础设施（PKI）是一种基于公开密钥算法的安全基础标准，它提供了一个框架，在这个框架内建立了可以创建鉴定和验证过程需要的身份和相关信任关系，建立了可以管理的公开密钥加密系统。

虽然公钥基础设施是建立在密码学的公开密钥算法的基础上，但其解决了仅仅依靠密