基于 OpenSSL 的安全密码平台的设计与实现

齐洪喜， 周大水
(山东大学 网络信息安全研究所，山东 济南 250100)

摘 要：在对 OpenSSL 开发包进行研究和分析的基础上，提出了一种基于 OpenSSL 的安全密码平台实现方案。通过对 OpenSSL 密码运算功能的抽象及其 engine 机制的研究，封装了易于上层安全应用调用的接口，保证了网络数据传输的安全性，使该平台不但具有良好的应用性和可移植性，而且具有对各种硬件密码设备的良好的兼容性。

关键词：密码平台； 安全套接层； 引擎； 公钥基础设施； 网络安全
中图法分类号：TP393.08 **文献标识码**：A **文章编号**：1000-7024 (2007) 02-0314-02

Design and implementation of secure crypto platform based on OpenSSL

QI Hong-xi, ZHOU Da-shui
(Institute of Network Security, Shandong University, Jinan 250100, China)

Abstract: By analyzing the OpenSSL, a scheme of secure crypto platform based on it is given. Based on the abstraction of crypto operations of OpenSSL and the research of the mechanism of engine in it, the interface for security application is carefully encapsulated, the security of the data in the network is enhanced, which have the platform practicable, transplantable and compatible to various kinds of crypto devices.

Key words: crypto platform; SSL; engine; PKI; networks security

0 引 言

近年来，各种电子信息服务(电子政务、电子商务等)的安全问题受到人们前所未有的重视。迫切需要一个有效的安全密码平台来实现各个实体数字信息的保密性、完整性，以及相互的身份认证，访问控制以及抗抵赖服务[2]。OpenSSL(open secure sockets layer)是一个优秀的开放源代码的项目，不仅实现了SSL协议，而且拥有功能强大的密码库，能够提供几乎所有的 PKI 服务。本文先 OpenSSL 作了简要介绍，然后给出了一个在OpenSSL包的基础上设的简易而高效安全密码平台的设计方案，对其实现要点进行了介绍，最后对该平台进行详细分析。

1 OpenSSL 简介

OpenSSL 是一个开放源代码的 SSL 协议及相关加密技术的产品实现，它采用C语言作为开发语言，具备了跨系统的性能。OpenSSL项目最早由加拿大人 Eric A. Yang 和 Tim J. Hudson 开发，现在由 OpenSSL 项目小组负责改进和开发。虽然 OpenSSL 使用 SSL 作为其名字的重要组成部分，但其实现的功能确远远超出了 SSL 协议本身。OpenSSL 事实上包括了 3 部分：SSL 协议、密码算法库和应用程序[3]。

密码算法库功能强大完整，是OpenSSL的基础部分，也是很值得一般密码安全技术人员研究的部分，它实现了目前大部分主流的密码算法和标准。主要包括公开密钥算法、对称加密算法、散列函数算法、X509 数字证书标准、PKCS12、PKCS7 等标准。在 0.9.6 版本之后，还提供了 Engine 机制，用于将如加密卡这样的外部加密算法集成到 OpenSSL 中[4]。

OpenSSL 功能十分强大，其内容涵盖了 PKI 应用中所需的几乎所有功能，使用时可以将所提供的库文件直接链接到应用程序中，也可以下载压缩包后，自己编译库函数得到库文件，在 Linux 下得到 libcryp2to.a 和 libssl.a，在 Windows 2000 下得到 libeay32.lib 和 ssleay32.lib 以及两个动态链接 ssleay32.dll 和 libeay32.dll。

2 安全密码平台的设计

一个高效的安全密码平台，必须能满足应用系统需求的各种基本密码服务。我们设计的密码平台的主要密码功能包括：

(1) 密钥管理：一个密码系统的安全性主要取决于对密钥的保护，而不是对系统或硬件本身的保护。具体的密码算法体制可以公开，密码设备可能丢失，但同一型号的密码机仍可以继续使用。而一旦密钥丢失，不但合法用户不能提取信息，而且可能会使非法用户窃取信息，严重影响了系统地可用性和安全性。因而密钥的保密和安全管理在整个系统安全中极

收稿日期：2006-01-12 E-mail：qihongxi@gmail.com
基金项目：国家 863 高技术研究发展计划基金项目 (2001AA141120)。
作者简介：齐洪喜 (1981－)，男，山东济南人，硕士研究生，研究方向为网络信息安全； 周大水 (1963－)，男，山东潍坊人，教授，硕士生导师，研究方向为网络安全相关产品的设计和研发。

为重要，不仅影响系统的安全性，而且涉及到系统的可靠性，有效性和经济性。本文的密钥管理包括密钥的产生、存储、装入、分配、保护、销毁以及保密等，保护密钥、生成临时密钥对、导入导出公私密钥对、备份恢复密钥对等。而他们基本上都是基于对密钥采取严格管理的安全密码设备。密钥不能出设备，在没有权限情况下，即使在设备内使用也是不可能的。

(2) 对称算法加解密：对称算法，即解密密钥不难从加密密钥中推算出来，反过来也成立的一类算法。大多数对称算法中的加解密密钥是相同的。根据著名的 Kerckhoff 原则，对称算法的安全性不能依赖于算法本身，只能依赖于密钥，因此密钥必须保密[1]。采用对称算法来加解密数据比非对称算法快得多，多用于数字信封中的大规模数据加解密。而用非对承算法来实现对称算法的密钥保密。本平台支持现在通用的所有对称算法，另外根据我们国家实际，我们也支持国家密码管理局指定的安全算法，比如 SSF33 算法等。

(3) 非对称算法加解密：采用非对称密钥算法，用作加密的密钥不同于解密的密钥，解密密钥也不能根据加密密钥计算出来。这两种密钥分别称为公钥和私钥。常用的 RSA 算法其安全性基于大数分解的难度，因为公钥和私钥是一对大素数，从一个公钥和密文中恢复出明文的难度等价与分解两个大素数之积。非对称加密既能用于加密会话密钥也能用于数字签名，非对称解密则可用于验证数字签名。

(4) Hash 操作：采用单向散列函数，是将任意长的数字串映射成一个较短的定长输出数字串的函数，具有不可逆性，本平台采用摘要算法 MD5、SHA1，用于验证数据完整性。

(5) MAC 操作：消息鉴别码 MAC (message authentication code)，带有密钥的单向散列函数，验证信息完整性，保证数据在存储，传输和处理过程中的真实有效性和一致性。其过程是使用密码算法对原始报文数据进行加密运算，得到一小段密文数据会加在原文之后。这小段数据与原数据的每一位都相关，使得原数据的每一位的变化都会反映到这小段数据上来，用于签名验证和防伪造。

(6) 随机数生成：一个密码系统的安全性很大程度取决于使用的随机数的好坏。随机数的随机性关系对称算法的密钥优劣，以及其它使用随机数的安全协议的安全性。大多数的软件实现的随机数生成器不如硬件设备的随机性能好。因此，在我们的安全密码平台中采用硬件密码设备中的随机数来保证随机数的强度。

以上是密码支撑平台的基本功能，通过对 OpenSSL 提供的库函数的进一步封装可以实现这些功能，并提供一套完整的 API 函数接口，以供上层应用调用。为此，我们充分利用了 OpenSSL 的 engine 机制，并采用了层次化和模块化的设计方法。图 1 给出了整个安全密码平台的逻辑框架，图中箭头表示调用关系。

3 实现介绍

整个密码平台的实现也是分为 3 层：安全应用层、Engine 实现层和硬件设备层。安全应用层为上层应用系统封装了方便用户调用的密码操作 API，其中包括安全通讯接口和安全密码接口。而硬件设备层则按照接口标准为 Engine 实现层封装了标准 API。整个安全密码平台的实现关键就是位于中间部分的 Engine 实现层处理。由于基于 OpenSSL 的安全密码平台实现起来是个较大系统，本文仅对其中部分关键技术予以介绍。

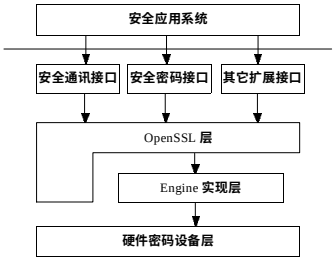

图 1 安全密码平台逻辑结构

在安全应用层中，考虑大部分应用需要网络通讯，特意给出了一组安全通讯接口，提供基本的 SSL 通讯。由于采用模块化设计，也可以根据具体情况予以增删。在安全米密码接口中，本文在对 OpenSSL 开发包认真研究的基础上，封装了 PKI 应用所需的基本密码操作，实现了上述所有功能。另外可以根据需要增加一些其它扩展接口，例如证书处理等。

Engine 层的实现中，既要符合 OpenSSL 的 Engine 机制，又要符合我们硬件密码设备的要求，需要心研究。由于硬件密码设备中的密钥(非对称算法私钥)不可出设备，而用户又必须利用相应的私钥进行运算。这就需在 Engine 层根据 OpenSSL 的特点对此进行精细处理，我们的思想是通过获取该私钥对应的公钥来填充私钥中公钥部分，并利用私钥结构体中的某个分量来记录该私钥在硬件设备中的信息来获取该私钥，如图 2 所示，其中的私钥结构体符合 PKCS#1 标准。通过此方法获取的虚拟私钥，由于私钥信息不完整，并不能直接用于非对称算法的运算。为此，需在 OpenSSL 的 Engine 的非对称算法的私钥运算部分进行独特设计，来引导私钥运算执行硬件操作。

bits	modulus	publicExponent	exponent	prime	primeExponent
从设备中获取的公钥部分			根据私钥在硬件设备中信息填充		

图 2 私钥构造

在 Engine 层的实现中另一个重要的部分就是从硬件加密设备中获取用户的一些特殊数据，如获取在硬件设备中存放的证书等。这一点可在硬件密码设备中的用户存储区获得，这也需要根据 Engine 机制本身和硬件密码设备特点来予以研究。

在硬件密码层，主要是按照前述设计的标准接口，对硬件密码操作予以封装，使其能够满足 Engine 层的要求，符合安全密码平台对硬件密码设备的兼容性要求。

4 性能分析

在对 OpenSSL 开发包的研究基础上，本安全密码平台具有很高的安全性、良好的可扩展性和设备兼容性。

(1) 安全性：该安全密码平台依赖 OpenSSL 开发包和硬件密码设备的安全性。OpenSSL 开发包已在全球范围内研究和使用，而且是开放源代码的，其安全性是可靠的。硬件密码设备的安全性在于其严格的操作权限控制，且需要得到国家密码管理局的安全审查，也是安全可靠的。现在密码系统的安全关

(下转第 319 页)

过程，证明了合法的验证数组隐含了σ的关于证实者(C)的签名数据(有的是二次签名数据)。而这些是C'所无法生成的。

(5)交互式下知识证明的不可转移：通过上述算法，在交互式情况下，使得其只能由合法的请求验证者(V)得到基于零知识的证据，任何第3方即使得到验证数组，也不能推断出有效的证据，从而保证的证明过程的不可转移。然而，若出现请求验证者(V)失信的情况，它可能通过利用其私有信息而对验证数组进行修改，得出可为任何人验证的(s_1,s_2,s_3,s_4,s_5)而泄漏给某个第3方。如何保证严格意义上的知识证明不可转移，是一个有待深入的问题。

5 结束语

在弱信任模型下，我们提供了一种完全基于RSA算法的可证实签名的方案，由于RSA算法兼具加解密及签名的功能，验证过程较为直观高效。在安全性方面，该方案具有产生可证实签名的惟一性、知识证明过程的不可模拟以及知识证明的不可转移等特点。

参考文献:

[1] Ateniese G.Efficient verifiable encryption (and fair exchange) of digital signatures [C]. Singapore: Proc ACM Conference on Computer and Communications Security, 1999.138-146.

[2] Nenadic A,Zhang N,Barton S.A security protocol for certified E-goods delivery[C]. Las Vegas, Nevada, USA: Proceedings of IEEE International Conference on Information Technology,Coding and Computing (ITCC 2004)-Information Assurance and Security Track, IEEE Computer Society, 2004.22-28.

[3] Wang G,Qing S,Wang M,et al.Threshold undeniable RSA signatures scheme[C]. LNCS2229, Berlin: Springer-Verlag, 2001. 221-232.

[4] Camenisch J,Michels M.Confiremer signature schemes secure against adaptive adversaries (extended abstract)[C].Berlin:Proc of the Advances in Cryptography,Spinger-Verlag, 2000.243-258.

[5] Wenbo Mao.现代密码学的理论与实践[M].北京:电子工业出版社, 2004.627-639.

[6] 王尚平,王育民,张亚玲.基于DSA及RSA的证实数字签名方案[J].软件学报, 2003,14(3):588-593.

[7] 王贵林,卿斯汉. 一个证实数字签名方案的安全缺陷[J]. 软件学报, 2004,15(5):752-756.

[8] 徐明,陈纯,应晶.一个基于交互式零知识证明的身份鉴别和数字签名协议[J].计算机研究与发展, 2002,39(9):1051-1056.

[9] 蔡满春. 一个基于零知识证明的非否认电子现金方案[J]. 计算机应用研究, 2005,9:113-114.

[10] Ray I. An optimistic fair exchange E-commerce protocol with automated dispute resolution[C]. LNCS1875, Berlin: Spinger-Verlag, 2000.84-93.

(上接第315页)

键就是如何保护系统使用的密钥，尤其是非对称算法之私钥。密钥的泄密将直接导致整个密码安全系统的崩溃。而使用硬件密码设备来产生、保存和管理密钥在极大程度上能防止密钥的泄密。另外国家密码管理局也公布了一些我国自主设计的密码算法：SSF33、SDBI等。它们大多在硬件设备中实现，使用硬件密码设备能够很好的使用这些性能良好的算法。

(2)可扩展性：一个良好的密码平台还需有良好的可扩展性，这主要通过模块化设计实现。我们这个密码平台可以很容易的根据具体用户的需求增删某些模块。比如通过增加一个证书管理模块可极大的方便用户对证书的处理。而不需要安全通讯服务的应用也可通过卸载安全通讯模块实现。良好的可扩展性能够提高平台的应用范围和节省开发及维护成本。

(3)兼容性：硬件密码设备在安全性和运算速度上的优势，使其在很多安全系统中得到广泛应用。这就要求安全密码平台能够对各种密码设备具有很好的兼容性。OpenSSL的Engine机制和硬件密码设备接口共同保证了安全密码平台的设备兼容性。我们通过定义一个硬件密码设备接口标准和充分利用OpenSSL的Engine机制来实现平台对各种设备(加密机、加密卡、智能Key)兼容性。只要硬件密码设备满足我们的标准接口，就完全可以通过配置直接整合到我们的平台中。目前已经很好的兼容济南得安公司开发的加密机、加密卡和智能Key。

在设计和实现中，我们充分考虑了密码平台的实用性和经济性。安全密码平台在提供了PKI应用中所需要的最基本的功能操作的前提下，通过在其中使用Engine机制，使其能够具有很好的设备兼容性，对于各种密码设备不需要重新设计与开发，节省了开发成本，利用密码平台的广泛应用。

5 结束语

本文是笔者参与研发的项目基础上总结经验写出的，较好处理了OpenSSL与我国硬件密码设备融合的问题，取得良好效果。对安全密码平台不同的应用需要使用者根据实际需要进一步改造和扩充。开发基于OpenSSL的应用，需要仔细阅读OpenSSL源代码和帮助文档。PKI应用需要安全密码平台提供的其它服务仍需要进一步研究。

参考文献:

[1] Bruce Schneider.应用密码学[M].北京:机械工业出版社, 2000.

[2] 冯登国.网络安全原理与技术[M].北京:科学出版社, 2003.

[3] Welcome to the OpenSSL project[DB/OL]. http://www.openssl.org.

[4] 中国OpenSSL专业论坛[DB/OL].2005.http://www.openssl.cn.

[5] 谭晓青.利用OpenSSL建立PKI数字证书系统[J].科学技术与工程, 2005,5(20):552-554.

[6] 张浩然,曾文潇,蒋同海.用Java和OpenSSL实现认证中心[J].计算机应用研究, 2004,21(5):157-159.

[7] 谭良. OpenSSL Engine安全平台下的Engine对象分析[J].四川师范大学学报(自然科学版), 2004,27(4):427-430.

[8] 钟源,崔树鹏,容晓峰,等.基于OpenSSL的密码支撑平台的研究与开发[J].计算机与现代化, 2004,(8):47-50.