OpenSSL 是一个强大的安全套接字层密码库，囊括主要的密码算法、常用的密钥和证书封装管理功能及[SSL](http://baike.so.com/doc/1076182-1138848.html)协议，并提供丰富的[应用程序](http://baike.so.com/doc/3417785-3597266.html)供测试或其它目的使用。

在OpenSSL被曝出现严重安全漏洞后，发现多数通过[SSL](http://baike.so.com/doc/1076182-1138848.html)协议加密的网站使用名为OpenSSL的[开源](http://baike.so.com/doc/4975645-5198476.html)软件包。由于这是互联网应用最广泛的安全传输方法，被网银、[在线支付](http://baike.so.com/doc/6295968-6509488.html)、电商网站、[门户网站](http://baike.so.com/doc/5002258-5226794.html)、[电子邮件](http://baike.so.com/doc/928072-980969.html)等重要网站广泛使用，所以该[漏洞](http://baike.so.com/doc/6046899-6259915.html)影响范围广大。

OpenSSL漏洞不仅影响以[https](http://baike.so.com/doc/5404553-5642272.html)开头的网站，黑客还可利用此漏洞直接对个人PC发起"心脏出血"([Heartbleed](http://baike.so.com/doc/7370397-7637792.html))攻击。据分析，Windows上有大量软件使用了存在漏洞的OpenSSL代码库，可能被黑客攻击抓取用户电脑上的内存数据。

基本信息

* 软件名称

开放式[安全套接层协议](http://baike.so.com/doc/2240162-2370194.html)

* 软件版本

1.0.1 g

* 更新时间

2014年4月7日

* 软件授权

开源

* 英文名

Open Secure Sockets Layer

* 软件平台

网络传输层

* 简    称

OpenSSL

|  |  |  |  |
| --- | --- | --- | --- |
| 目录 | 1[简介](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-1)  2[特点](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-2)  3[功能](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-3) | 4[算法](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-4)  5[应用](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-5)  6[漏洞](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-6) | 7[漏洞拦截](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-7)  8[主要版本](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-8)  9[安装方法](http://baike.so.com/doc/5467726-5705638.html#5467726-5705638-9) |

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=1)简介

[SSL](http://baike.so.com/doc/1076182-1138848.html)是Secure Sockets Layer([安全套接层协议](http://baike.so.com/doc/2240162-2370194.html))的缩写，可以在Internet上提供秘密性传输。网景Netscape公司在推出第一个[Web浏览器](http://baike.so.com/doc/1730246-1829293.html)的同时，提出了SSL协议标准。其目标是保证两个应用间通信的保密性和可靠性,可在服务器端和用户端同时实现支持。已经成为Internet上保密通讯的工业标准。

[安全套接层协议](http://baike.so.com/doc/2240162-2370194.html)能使用户/服务器应用之间的通信不被攻击者[窃听](http://baike.so.com/doc/3266977-3441966.html)，并且始终对服务器进行认证，还可选择对用户进行认证。SSL协议要求建立在可靠的传输层协议([TCP](http://baike.so.com/doc/3381795-3560272.html))之上。SSL协议的优势在于它是与应用层协议独立无关的，高层的应用层协议(例如:HTTP，FTP，[TELNET](http://baike.so.com/doc/5504434-5740178.html)等)能透明地建立于SSL协议之上。SSL协议在应用层协议通信之前就已经完成[加密算法](http://baike.so.com/doc/5568345-5783506.html)、通信密钥的协商及服务器认证工作。在此之后应用层协议所传送的数据都会被加密，从而保证通信的私密性。

通过以上叙述，SSL协议提供的安全信道有以下三个特性:

1 数据的保密性

信息加密就是把明码的输入文件用[加密算法](http://baike.so.com/doc/5568345-5783506.html)转换成加密的文件以实现数据的保密。加密的过程需要用到密钥来加密数据然后再解密。没有了密钥，就无法解开加密的数据。[数据加密](http://baike.so.com/doc/6144836-6358013.html)之后，只有密钥要用一个安全的方法传送。加密过的数据可以公开地传送。

2 数据的完整性

加密也能保证数据的一致性。例如:消息验证码([MAC](http://baike.so.com/doc/3374403-3552810.html))，能够校验用户提供的加密信息，接收者可以用MAC来校验加密数据，保证数据在传输过程中没有被篡改过。

3 安全验证

加密的另外一个用途是用来作为个人的标识，用户的密钥可以作为他的安全验证的标识。SSL是利用[公开密钥](http://baike.so.com/doc/296087-313468.html)的[加密技术](http://baike.so.com/doc/6539431-6753170.html)([RSA](http://baike.so.com/doc/133562-141114.html))来作为用户端与服务器端在传送机密资料时的加密通讯协定。

OpenSSL包含一个命令行工具用来完成OpenSSL库中的所有功能，更好的是，它可能已经安装到你的系统中了。

OpenSSL是一个强大的安全套接字层密码库，Apache使用它加密HTTPS，OpenSSH使用它加密[SSH](http://baike.so.com/doc/1081563-1144523.html)，但是，你不应该只将其作为一个库来使用，它还是一个多用途的、跨平台的密码工具。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=2)特点

众多的密码算法、[公钥基础设施](http://baike.so.com/doc/5497738-5735652.html)标准以及SSL协议，或许这些有趣的功能会让你产生实现所有这些算法和标准的想法。果真如此，在对你表示敬佩的同时，还是忍不住提醒你:这是一个令人望而生畏的过程。这个工作不再是简单的读懂几本[密码学](http://baike.so.com/doc/5540093-5755759.html)专著和[协议](http://baike.so.com/doc/3835905-4027900.html)文档那么简单，而是要理解所有这些[算法](http://baike.so.com/doc/2758411-2911336.html)、标准和协议文档的每一个细节，并用你可能很熟悉的C语言[字符](http://baike.so.com/doc/2529629-2672477.html)一个一个去实现这些定义和过程。我们不知道你将需要多少时间来完成这项有趣而可怕的工作，但肯定不是一年两年的问题。

首先，应该感谢Eric A. Young和Tim J. Hudson，他们自1995年开始编写后来具有巨大影响的OpenSSL[软件包](http://baike.so.com/doc/6788925-7005534.html)，更令我们高兴的是，这是一个没有太多限制的[开放源代码](http://baike.so.com/doc/6270840-6484264.html)的软件包，这使得我们可以利用这个软件包做很多事情。Eric A. Young 和Tim J. Hudson是加拿大人，后来由于写OpenSSL功成名就之后就到大公司里赚大钱去了。1998年，OpenSSL项目组接管了OpenSSL的开发工作，并推出了OpenSSL的0.9.1版，到目前为止，OpenSSL的算法已经非常完善，对SSL2.0、SSL3.0以及TLS1.0都支持。

OpenSSL采用C语言作为开发语言，这使得OpenSSL具有优秀的[跨平台](http://baike.so.com/doc/5131891-5361327.html)性能，这对于广大技术人员来说是一件非常美妙的事情，可以在不同的平台使用同样熟悉的东西。OpenSSL支持Linux、Windows、BSD、Mac、VMS等平台，这使得OpenSSL具有广泛的适用性。但习惯C语言总比使用C++重新写一个跟OpenSSL相同功能的[软件包](http://baike.so.com/doc/6788925-7005534.html)轻松不少。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=3)功能

[折叠](http://baike.so.com/doc/5467726-5705638.html)基本功能

OpenSSL整个软件包大概可以分成三个主要的功能部分:SSL协议库、[应用程序](http://baike.so.com/doc/3417785-3597266.html)以及密码算法库。OpenSSL的目录结构自然也是围绕这三个功能部分进行规划的。

作为一个基于密码学的安全开发包，OpenSSL提供的功能相当强大和全面，囊括了主要的密码算法、常用的密钥和证书封装管理功能以及SSL协议，并提供了丰富的[应用程序](http://baike.so.com/doc/3417785-3597266.html)供测试或其它目的使用。

[折叠](http://baike.so.com/doc/5467726-5705638.html)辅助功能

[BIO](http://baike.so.com/doc/321609-340628.html)机制是OpenSSL提供的一种高层IO接口，该接口封装了几乎所有类型的[IO](http://baike.so.com/doc/6723558-6937685.html)接口，如内存访问、文件访问以及Socket等。这使得代码的重用性大幅度提高，OpenSSL提供API的复杂性也降低了很多。

OpenSSL对于随机数的生成和管理也提供了一整套的解决方法和支持API函数。随机数的好坏是决定一个密钥是否安全的重要前提。

OpenSSL还提供了其它的一些辅助功能，如从口令生成密钥的API，证书签发和管理中的配置文件机制等等。如果你有足够的耐心，将会在深入使用OpenSSL的过程慢慢发现很多这样的小功能，让你不断有新的惊喜。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=4)算法

[折叠](http://baike.so.com/doc/5467726-5705638.html)密钥和证书管理

密钥和证书管理是[PKI](http://baike.so.com/doc/2865132-3023522.html)的一个重要组成部分，OpenSSL为之提供了丰富的功能，支持多种标准。

首先，OpenSSL实现了ASN.1的证书和密钥相关标准，提供了对证书、[公钥](http://baike.so.com/doc/6626282-6840081.html)、[私钥](http://baike.so.com/doc/5284811-5519118.html)、证书请求以及CRL等数据对象的DER、PEM和BASE64的编解码功能。OpenSSL提供了产生各种[公开密钥](http://baike.so.com/doc/296087-313468.html)对和对称密钥的方法、函数和[应用程序](http://baike.so.com/doc/3417785-3597266.html)，同时提供了对[公钥](http://baike.so.com/doc/6626282-6840081.html)和[私钥](http://baike.so.com/doc/5284811-5519118.html)的DER编解码功能。并实现了[私钥](http://baike.so.com/doc/5284811-5519118.html)的PKCS#12和PKCS#8的编解码功能。OpenSSL在标准中提供了对[私钥](http://baike.so.com/doc/5284811-5519118.html)的加密保护功能，使得密钥可以安全地进行存储和分发。

在此基础上，OpenSSL实现了对证书的X.509标准编解码、PKCS#12格式的编解码以及PKCS#7的编解码功能。并提供了一种文本数据库，支持证书的管理功能，包括证书密钥产生、请求产生、证书签发、吊销和验证等功能。

事实上，OpenSSL提供的CA[应用程序](http://baike.so.com/doc/3417785-3597266.html)就是一个小型的证书管理中心(CA)，实现了证书签发的整个流程和证书管理的大部分机制。

5.SSL和TLS协议

OpenSSL实现了SSL协议的SSLv2和SSLv3，支持了其中绝大部分算法协议。OpenSSL也实现了TLSv1.0，TLS是SSLv3的标准化版，虽然区别不大，但毕竟有很多细节不尽相同。

虽然已经有众多的软件实现了OpenSSL的功能，但是OpenSSL里面实现的SSL协议能够让我们对SSL协议有一个更加清楚的认识，因为至少存在两点:一是OpenSSL实现的SSL协议是开放源代码的，我们可以追究SSL协议实现的每一个细节;二是OpenSSL实现的SSL协议是纯粹的SSL协议，没有跟其它协议(如HTTP)协议结合在一起，澄清了SSL协议的本来面目。

[折叠](http://baike.so.com/doc/5467726-5705638.html)对称加密算法

OpenSSL一共提供了8种对称加密算法，其中7种是分组加密算法，仅有的一种流加密算法是RC4。这7种分组加密算法分别是AES、DES、Blowfish、CAST、IDEA、RC2、RC5，都支持电子密码本模式(ECB)、加密分组链接模式(CBC)、加密反馈模式(CFB)和输出反馈模式(OFB)四种常用的[分组密码](http://baike.so.com/doc/6619133-6832928.html)加密模式。其中，AES使用的加密反馈模式(CFB)和输出反馈模式(OFB)分组长度是128位，其它算法使用的则是64位。事实上，DES算法里面不仅仅是常用的DES算法，还支持三个密钥和两个密钥3DES算法。

[折叠](http://baike.so.com/doc/5467726-5705638.html)非对称加密算法

OpenSSL一共实现了4种非对称[加密算法](http://baike.so.com/doc/5568345-5783506.html)，包括DH算法、[RSA](http://baike.so.com/doc/133562-141114.html)算法、[DSA算法](http://baike.so.com/doc/1480275-1565299.html)和[椭圆曲线算法](http://baike.so.com/doc/5813902-6026710.html)(EC)。DH算法一般用于密钥交换。RSA[算法](http://baike.so.com/doc/2758411-2911336.html)既可以用于密钥交换，也可以用于[数字签名](http://baike.so.com/doc/2871106-3029793.html)，当然，如果你能够忍受其缓慢的速度，那么也可以用于[数据加密](http://baike.so.com/doc/6144836-6358013.html)。[DSA算法](http://baike.so.com/doc/1480275-1565299.html)则一般只用于[数字签名](http://baike.so.com/doc/2871106-3029793.html)。

[折叠](http://baike.so.com/doc/5467726-5705638.html)信息摘要算法

OpenSSL实现了5种信息摘要算法，分别是MD2、MD5、MDC2、SHA(SHA1)和[RIPEMD](http://baike.so.com/doc/2490194-2631617.html)。SHA算法事实上包括了SHA和SHA1两种信息摘要算法。此外，OpenSSL还实现了DSS标准中规定的两种信息摘要算法DSS和DSS1。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=5)应用

[折叠](http://baike.so.com/doc/5467726-5705638.html)功能

OpenSSL的[应用程序](http://baike.so.com/doc/3417785-3597266.html)已经成为了OpenSSL重要的一个组成部分，其重要性恐怕是OpenSSL的开发者开始没有想到的。如OpenCA，就是完全使用OpenSSL的应用程序实现的。OpenSSL的应用程序是基于OpenSSL的密码算法库和SSL协议库写成的，所以也是一些非常好的OpenSSL的API使用范例，读懂所有这些范例，你对OpenSSL的API使用了解就比较全面了，当然，这也是一项锻炼你的意志力的工作。

OpenSSL的应用程序提供了相对全面的功能，在相当多的人看来，OpenSSL已经为自己做好了一切，不需要再做更多的开发工作了，所以，他们也把这些应用程序成为OpenSSL的指令。OpenSSL的应用程序主要包括密钥生成、证书管理、格式转换、[数据加密](http://baike.so.com/doc/6144836-6358013.html)和签名、SSL测试以及其它辅助配置功能。

[折叠](http://baike.so.com/doc/5467726-5705638.html)机制

Engine机制 Engine机制的出现是在OpenSSL的0.9.6版的事情，开始的时候是将普通版本跟支持Engine的版本分开的，到了OpenSSL的0.9.7版，Engine机制集成到了OpenSSL的内核中，成为了OpenSSL不可缺少的一部分。 Engine机制目的是为了使OpenSSL能够透明地使用第三方提供的[软件加密](http://baike.so.com/doc/1090059-1153480.html)库或者[硬件加密](http://baike.so.com/doc/1090070-1153486.html)设备进行加密。OpenSSL的Engine机制成功地达到了这个目的，这使得OpenSSL已经不仅仅使一个加密库，而是提供了一个通用地加密接口，能够与绝大部分加密库或者加密设备协调工作。当然，要使特定加密库或加密设备OpenSSL协调工作，需要写少量的接口代码，但是这样的工作量并不大，虽然还是需要一点密码学的知识。Engine机制的功能跟Windows提供的CSP功能目标是基本相同的。包括:CryptoSwift、[nCipher](http://baike.so.com/doc/4988817-5212447.html)、Atalla、Nuron、UBSEC、Aep、SureWare以及IBM 4758 CCA的[硬件加密](http://baike.so.com/doc/1090070-1153486.html)设备。当然，所有上述Engine接口支持不一定很全面，比如，可能支持其中一两种[公开密钥](http://baike.so.com/doc/296087-313468.html)算法。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=6)漏洞

[折叠](http://baike.so.com/doc/5467726-5705638.html)发现

2014年4月8日，OpenSSL的大漏洞曝光。这个漏洞被曝光的黑客命名为"heartbleed"，意思是"心脏流血"--代表着最致命的内伤。利用该漏洞，黑客坐在自己家里电脑前，就可以实时获取到约30%https开头网址的用户登录账号密码，包括大批网银、购物网站、电子邮件等。

"心脏流血"首先被谷歌(微博)研究员尼尔·梅塔(Neel Mehta)发现，它可从特定服务器上随机获取64k的工作日志，由于数据是随机获取的，所以攻击者也不一定可以获得想要的信息，因此整个过程如同钓鱼，攻击可能一次次持续进行，大量敏感数据可能泄露。由于一台服务器的密钥也记录在其工作日志中，并且在大量数据中可被轻易辨别，因此将是首当其冲的获取目标，获取密钥后，攻击者可以掌握某网站或服务的实时流量情况，甚至可以破解被加密的以往流量日志。

安全专家介绍说，OpenSSL此漏洞堪称网络核弹，网银、网购、网上支付、邮箱等众多网站受其影响。无论用户电脑多么安全，只要网站使用了存在漏洞的OpenSSL版本，用户登录该网站时就可能被黑客实时监控到登录账号和密码。

根据相关媒体的报导，研究人员发现OpenSSL漏洞遍及全球互联网公司，并为其起了个形象的名字"心脏出血"，中国超过3万台主机受波及，国内网站和安全厂商技术人员为检查、抢修彻夜未眠。截至昨天，有超30%的主机已经修复，但技术人士称，消费者敏感信息是否泄露还有待日后观察。

[折叠](http://baike.so.com/doc/5467726-5705638.html)成因

此次漏洞的成因是OpenSSL Heartbleed模块存在一个BUG，当攻击者构造一个特殊的数据包，满足用户心跳包中无法提供足够多的数据会导致memcpy把SSLv3记录之后的数据直接输出，该漏洞导致攻击者可以远程读取存在漏洞版本的OpenSSL服务器内存中长达64K的数据。

"心脏流血"这个名字听起来有点夸张，但这个漏洞的威力似乎当得起它的名字。不管是从可能感染的电脑数量还是从可能被泄露的数据规模，"心脏流血"的破坏力都超过在2014年早些时候狠狠羞辱了苹果公司的"GoToFail "漏洞。"心脏流血"漏洞可以帮助黑客获得打开服务器的密钥，监听服务器数据和流量。更糟糕的是，这并不是一个新的漏洞， "心脏流血"其实已经存在两年了，但具体何时被人发现其危险性尚不得而知。

[折叠](http://baike.so.com/doc/5467726-5705638.html)补救措施

在各个网站尚未解决安全漏洞的近两天，用户尽量不登录或者少登录涉及资金、个人隐私的网站或系统，已经多次登录的用户请尽快修改密码、绑定手机、设置支付密码，最好采用手机令牌类软件如号令手机令牌等，确保通过实时变化的动态口令保障账号安全。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=7)漏洞拦截

备受关注的OpenSSL"心脏出血"漏洞有了最新进展:不法分子可以通过漏洞获取网站[私钥](http://baike.so.com/doc/5284811-5519118.html)，并通过盗取的证书伪造假冒网站，或可躲避一些安全软件及安全浏览器的拦截。

[折叠](http://baike.so.com/doc/5467726-5705638.html)漏洞风险

此前曝出的"心血漏洞"由于影响范围之广而引起了国内互联网业界及用户的极大关注。黑客可能利用"心脏出血"漏洞，攻击网民的个人电脑，盗取帐号密码、登陆认证cookies、网银密钥等私密数据。

[折叠](http://baike.so.com/doc/5467726-5705638.html)漏洞影响

据专家介绍，由于Windows上用OpenSSL的软件很多，且多数使用自己安装目录下的 SSLeay32.dll 和 Libeay32.dll，没有统一的升级管理机制，该漏洞可能会长期存在。

专家解释，由于网站证书被认为是网址安全可信的标志，因此黑客会利用漏洞盗取网站私钥从而冒名顶替合格的网站证书。此种情况下，安全系统或杀毒软件很可能不能判断网站的真实性。

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=8)主要版本

| **版本** | **发布时间** | **备注** |
| --- | --- | --- |
| 老版本，不再支持: 0.9.1c | 1998年12月23日 |  |
| 老版本，不再支持: 0.9.2c | 1999年3月22日 | 取代0.9.1c |
| 老版本，不再支持: 0.9.3 | 1999年5月25日 | 取代0.9.2b |
| 老版本，不再支持: 0.9.4 | 1999年8月9日 | 取代0.9.3a |
| 老版本，不再支持: 0.9.5 | 2000年2月28日 | 取代0.9.4 |
| 老版本，不再支持: 0.9.6 | 2000年9月25日 | 取代0.9.5a |
| 老版本，不再支持: 0.9.7 | 2002年12月31日 | 取代0.9.6h |
| 老版本，不再支持: 0.9.8 | 2005年7月5日 | 取代0.9.7h |
| 老版本，不再支持: 1.0.0 | 2010年3月29日 | 取代0.9.8x |
| 老版本，不再支持: 1.0.1 | 2012年3月14日 | 取代1.0.0e  支持TLS v1.2  SRP支持 |
| 当前稳定版本:**1.0.1g** | 2014年4月7日 | 当前版本  修补"血崩"  漏洞 |

展开

[折叠](http://baike.so.com/doc/5467726-5705638.html)[编辑本段](http://baike.so.com/create/edit/?eid=5467726&sid=5705638&secid=9)安装方法

OpenSSL的编译安装需Perl的支持，下载最新版ActivePerl和OpenSSL源码包。

安装ActivePerl。

执行VC安装目录下vcvarsall.bat 配置默认环境。

进入openssl目录，执行如下指令(X64环境)

> perl Configure VC-WIN64A

> msdo\_win64a

> nmake -f msntdll.mak

> cd out32dll

> ..mstest

具体详情可参考openssl目录下Install.w32等文件。