基于 ZUC 的 OpenVPN 安全性能研究*

吴建斌 费潇潇 王年丰
(华中师范大学 武汉 430079)

摘 要：为提高 OpenVPN 技术的安全性，在介绍基于 SSL 协议的 VPN 技术的基础上，针对其密码算法弱强度的问题，通过编写包含 ZUC 算法的自定义引擎，用被国际认可的高强度加密算法 ZUC 算法替换 OpenVPN 中原本的弱强度算法，实现了对 ZUC 算法的调用，提高了 OpenVPN 技术的安全性，具有修改代价小，安全性高的特点。在系统测试过程中经过了 Sniffer Pro 嗅探器的抓包测试和 TCP/UDP 调试助手的数据通信测试，结果表明，客户端与服务器的通信数据能够被 ZUC 算法进行加密以达到安全通信的目的，该系统的高强度密码算法很大程度上满足了政府、军队和金融等对安全性要求较高的领域的需求，具有较强的实用价值。

关键词：安全性；OpenVPN ；高强度算法；引擎
中图分类号：TP2 **文献标识码**：A **国家标准学科分类代码**：510.1050

OpenVPN safety research based on the ZUC

Wu Jianbin Fei Xiaoxiao Wang Nianfeng
(Central China Normal University, Wuhan 430079, China)

Abstract: In order to improve the security of OpenVPN technology, this paper introduces the VPN technology, based on SSL protocol, and then find the existing password algorithm of weak strength of the technology, put forward the method of high strength encryption algorithm which represented by ZUC has been internationally recognized to replace the original weak strength algorithm in OpenVPN, realised the call of ZUC algorithm by writing a custom engine including ZUC algorithm, and has the characteristics of low cost and high security. After the Sniffer Pro capture test and TCP / UDP debugging assistant data communications test, the results show that, data communication between the client and the server can be encrypted by zuc algorithm in order to achieve the purpose of communication security, and high strength encryption algorithm of the system, to a great extent, meet the such as government, military and financial security requirements in areas of higher demand, has a strong practical value.

Keywords: security; OpenVPN; high strenth algorithms; engine

1 引 言

随着互联网技术的飞速发展，虚拟专用网络(virtual private network，VPN)技术得到了越来越广泛的应用。目前 VPN 技术的实现方式主要有两种形式。一种是基于网络层采用 IPSec 协议来实现远程接入的 IP 协议安全(internet protocol security，IPSec)VPN 技术[1]。另一种是基于传输层采用 SSL 协议来实现远程接入的的安全套接层(secure sockets layer，SSL)VPN 技术[2]。为提高 VPN 技术的安全性，很多学者从多个角度对这两种实现方法进行了深入的研究。王凤领[3]从节省网络费用的角度对 IPSecVPN 技术的体系结构和工作模式进行了研究，但发现其在网络地址转换时可能存在冲突，并且配置和使用比较复杂，容易带来操作系统的安全隐患问题。朱意秋[4]、周勇[5]比较了 SSLVPN 技术和 IPSecVPN 技术的异同，发现基于 SSL 协议的 VPN 技术比基于 IPSec 协议的 VPN 技术更灵活，也更符合各类企业网络安全远程接入的需求。但美国对出口密码产品的管制比较严格，在 SSLVPN 技术的实现中，各种密码算法的密钥长度较短，并且强度较弱，不符合政府、军队和金融等高安全领域的要求，诸晔等人[6]针对该问题，实现了一种通过 OpenSSL 的引擎机制添加自定义算法的方案。进一步分析发现该方法虽然可保留 SSLeay 中原有的算法，但其需要修改 OpenSSL 的源代码对新算法进行注册，代码开销较大。为进一步减小代码开销，解决密码算法强度问题，本文提出了利用 OpenSSL 动态引擎机制将 OpenSSL 的 SSLeay 模块中弱强度密码算法

收稿日期：2015-12
* 基金项目：华中师范大学中央高校基本科研业务研究基金(CCNU15A02040)资助项目

替换为高强度密码算法的方法，这样可实现在不修改 SSLeay 的基础上实现新的加密算法的添加，该方法通过 OpenSSL 调用自定义的高强度加密模块，能够满足对安全性和机密性要求较高领域的需求。

2　基于 SSL 协议的 VPN 技术研究

2.1　VPN 技术及其关键技术

VPN 技术通过在复杂的网络环境中建立一条虚拟通道，将位于通道两边的网络或节点连接起来，保证通道内数据的安全通信。它是利用隧道技术完成不同网络间共享数据的封装，采用加解密技术和客户端与服务器间的认证技术来达到实现专用网络的扩展。VPN 的关键技术包括数据加密技术、身份认证技术、隧道技术和密钥管理技术。其中隧道技术是通过一个网络为另一网络传输数据，实现不同网络间共享数据的一种技术。密钥的分发有手工配置和采用密钥交换协议动态分发这两种方式。

2.2　基于 SSL 协议的 VPN 技术

为提高 VPN 通信数据的安全性，SSL 协议被引入到 VPN 技术中。SSL 协议是计算机设备间利用 Internet 网络进行通信的加密协议，其本质上是在 VPN 虚拟隧道上对客户端与服务器间的通信内容使用公共密钥和私有密钥进行加密的技术，防止在网络传输过程中数据遭到截取或者窃听。SSL 协议由用于数据加密的对称算法和用于身份认证，密钥交互的非对称算法组成。

采用基于 SSL 协议的 VPN 技术实现客户端与服务器通信可分为两个阶段。第 1 阶段是客户端与服务器的握手阶段，该阶段要实现双方身份认证和密钥交互；第 2 阶段是客户端与服务器互发数据阶段，该阶段要实现数据的加密。SSLVPN 通信时通信双方的身份是通过数字签名技术验证的，私钥加密后的密文只能使用对应的公钥解密，因此，根据解密的结果是否成功来判断发送端与接收端的身份，就像双方对数据进行签名。为了防止非法用户冒充双方通信者中的某一方，双方在用数字签名技术验证身份时必须要确保双方的公钥是真实可靠的，这是握手阶段很关键的一个部分。SSL 协议中包含对称算法非对称算法和 HMAC 算法，其中 HMAC 主要用来对明文数据进行摘要操作。SSL 通信双方是在握手阶段完成密钥交互过程，包括预主密钥、主密钥两个部分。其中，预主密钥采用基于非对称的密钥协商算法、HMAC 和对称算法生成；生成预主密钥后，采用预主密钥生成主密钥；通信双方的对称密钥和 HMAC 密钥由主密钥所派生，该阶段生成的对称密钥和 HMAC 密钥将用于第 2 阶段的数据加密时的密钥。

基于 SSL 协议实现的 VPN 技术，其通信信道由 SSL 协议提供安全保障。在一般的应用场合，作为一个实用协议，SSL 协议保障信道的安全是通过协议本身的设计，谨慎的实现和使用来实现。但在信息安全性要求高的领域，受美国管制出口密码产品的限制，存在着密码算法弱强度的问题，这导致其加密性能大大降低，非常容易受到穷尽搜索密钥方法的攻击，对数据安全构成威胁。正因为此，很多学者已开始在 SSL 协议中采用替代算法的研究，如采用我国自主研发的同步流密码算法等。

3　ZUC 算法及其原理

算法(ZUC)，是由中国自主设计的同步流密码算法，是用于加密数据的 128-EEA3 (3GPP confidentiality algorithm)算法和用于保证数据完整性的 128-EIA3(3GPP integrity algorithm)算法的核心内容[7-8]。ZUC 算法在逻辑上采用 3 层结构设计，上层是一个线性反馈移位寄存器(linear feedback shift register，LFSR)，中层是比特重组(bit restructuring，BR)层，下层是一个非线性函数 F。该算法利用素域 GF($2^{31}-1$) 的 m 序列进行 LFSR 设计，该类序列具有周期长和统计特性好的特点，在特征为 2 的有限区域上不是线性的，且线性结构弱和比特关系符合率低，这导致该序列对于二元域等密码攻击具有天然的强抵抗能力。ZUC 算法的比特重组的作用是破坏 LFSR 在素域 GF($2^{31}-1$) 上的线性结构，结合底层的非线性函数 F 可使得一些在素域 GF($2^{31}-1$)上的密码攻击变得非常困难。ZUC 算法在设计非线性函数 F 时借鉴了分组密码设计的技巧，采用了 S 盒与具有高扩散特性的线性变换 L，非线性函数 F 有强的抵抗区分分析和快速相关攻击等方法的能力。上述 3 层结构的综合运用使得 ZUC 算法具有非常高的安全强度和抵抗目前常见的绝大部分流密码攻击的能力[7]。介于上述研究发现的 SSLVPN 技术存在的缺陷及 ZUC 算法的优越性，下面提出了一种用 ZUC 算法替换 SSLVPN 中弱强度算法的实现方案。

4　基于 OpenVPN 技术的实现方案

4.1　OpenVPN 技术

OpenVPN 技术作为隧道型 SSLVPN 技术的一个典型应用提供了实现 SSLVPN 全部功能的解决方案，OpenSSL 加密库和 SSLv3/TLSv1 协议在 OpenVPN 中得到了广泛的使用。OpenSSL 是一个强大的安全套接字层密码库，包括主要的密码算法、常用的密钥和证书封装管理功能及 SSL 协议，并提供丰富的应用程序供测试或其他目的使用[9]。

4.2　Engine 机制工作原理

Engine 机制目的是使 OpenSSL 可以透明地使用第三方提供的软件加密库或硬件加密设备来加密[10]。OpenSSL 了采用这种机制，并且使得 OpenSSL 提供了一个通用的加密接口，这样 OpenSSL 能够与很大部分加密库或加密设备协调工作。

OpenSSL 的 Engine 机制可实现 OpenSSL 加密模块的扩展。图 1 介绍了 Engine 机制的原理，从图中可看出应用程序调用密码库的方式有 3 种。1)应用程序直接通过

OpenSSL 自身提供的 Engine 来调用原本就封装在 SSLeay 密码库中的加解密算法。2)应用程序通过调用 OpenSSL 内部支持的 Engine(如图 1 的 nCipher Engine、Atalla Engine)加载和调用其支持的硬件加密设备,前两种方式都是对 OpenSSL 内部有对应接口的算法的调用。3)对 OpenSSL 内部没有对应接口的第三方自定义的密码模块(如图 1 的 XX 软硬件模块)的调用,如图 1 所示调用方法有两种,第一种是由其开发商提供或用户自行编写其 Engine,即图 1 中的 XX Engine,通过该 Engine 机制访问 XX 加密模块,另一种方式是为 XX 加密模块编写供 OpenSSL 内部的动态 Engine 调用的动态库,通过动态 Engine 调用 XX 动态库,进而访问 XX 加密模块,前一种方式需要将 XX Engine 添加进 OpenSSL 的源代码再对新的 OpenSSL 进行重新编译,而后一种方式只需提供供动态 Engine 调用的 XX Engine 动态库,而不需要对 OpenSSL 重新编译,这能够减小编译 OpenSSL 带来的代码开销。本文采用后一种方法来实现算法的添加。

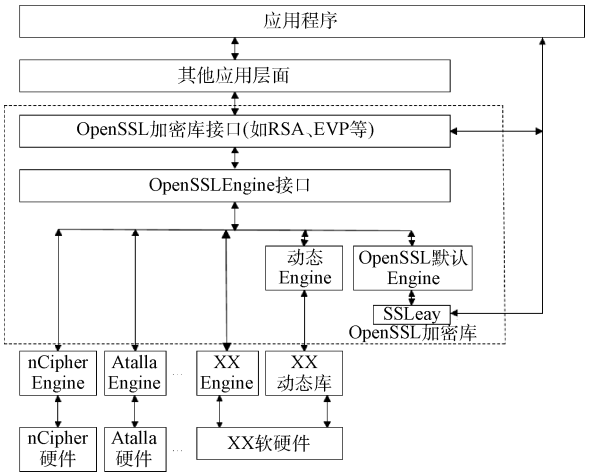

图 1 Engine 机制的原理

4.3 方案设计

用 ZUC 算法替换 OpenSSL 中的弱强度算法的方案流程如图 2 所示。

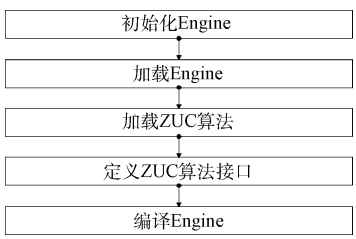

图 2 ZUC 算法替换流程

1)初始化 Engine

初始化 Engine 操作包括在 bind_helper(ENGINE * e)函数中使用 ENGINE_set_id()设置 Engine id 对 Engine 进行编号和 ENGINE_set_name()设置 Engine name 对 Engine 进行命名,还包括完成对 Engine 进行初始化的 Engine_init()函数,关闭 Engine 机制的 Engine_finish()函数和对 Engine 中函数进行痕迹清理的 Engine_destroy()函数(该函数是对调用完的函数进行痕迹清理,可以避免加载同一个 Engine 不同算法出现函数调用错误的情况)。

2)加载 Engine

加载 Engine 是通过调用 Engine_load_XX()函数实现把 Engine 对象加载到系统中的,然后调用 Engine * e=Engine_by_id()或者 Engine_by_name()完成 Engine 的调用。

3)加载 ZUC 算法

该方案在 CBC、CFB、OFB、ECB 四种模式中选择的是较普遍的 CBC 模式,因此加载 ZUC 算法需要完成 ZUC 算法的 EVP_CIPHER 结构体的设置。该方案可以减小一部分的代码开销体现在结构体成员 NID(算法的识别符)的设置上,以 OpenSSL 中原本存在的 Camellia 算法的 NID 号来命名 ZUC 算法,如此,ZUC 算法就不需要重新注册,也不需要对 OpenSSL 源代码做任何修改。EVP_CIPHER 结构体中其他元素的设置可根据 ZUC 算法的具体情况进行设置,内部的初始化,加解密函数都指向 ZUC 算法的接口。

4)定义 ZUC 算法接口

该方案采用的是 NID 替换的方法,表面是 Camellia 算法,实际上运行的是 ZUC 算法,调用的时候只需按照调用 Camellia 算法同样的方法就可以完成 ZUC 算法的调用。这样可以进一步减少注册算法,重新定义接口带来的代码开销。

5)编译 Engine

上述步骤全部完成即可完成该自定义 Engine 的编写,可实现将 ZUC 算法添加到 Engine 中,但实现 ZUC 算法的调用还需要将该 Engine 编译生成的 DLL 和 LIB 文件添加到 OpenVPN 中,供动态引擎调用,该动态引擎的调用函数是 ENGINE_load_dynamic(),之后再调用 ENGINE_by_id(id)对 Engine 进行搜索,有多个 Engine 时动态引擎的优势就可以体现出来,系统每次只需调用动态引擎即可,不需要将每个引擎都加载到 OpenVPN 中,节省了空间,也给替换算法增加了灵活性。Engine 的调用和加载均完成之后,再将 Camellia 算法添加进配置文件,即可完成方案中替换算法的要求。

4.4 测试结果及讨论

上文的实验方案可以完成该系统新加密算法的添加,完成算法的添加之后即要进行测试。在测试之前需要在两台电脑上搭建客户端与服务器的 OpenVPN 平台,双方均选择新添加的算法,完成搭建之后该系统的测试分为两个部分,一部分是进行 Sniffer Pro 嗅探器的抓包测试以确定算法被成功加密以密文的形式传输,另一部分是进行 TCP/UDP 调试助手的数据通信测试以确定服务器客户端

能调用 ZUC 算法进行加密解密传输。

以上的两部分测试的结果表明，上文的方案能够实现 ZUC 算法的添加，并且可以用同样的方法实现其他加密算法的添加。文献[6]中的添加方法采用的是程序开发者编写一个 Engine，将该 Engine 加载到 OpenSSL 中，然后对 OpenSSL 进行重新编译，且需要对新添加的算法进行注册，这种方法添加的自定义算法如果发生改变则需要重新注册该算法，这导致添加算法的灵活性较低，并且需要对 OpenSSL 源代码进行修改。本文所提出的方法不需要将编写好的 Engine 添加到 Openssl 中进行重编译，亦不需要对新添加的算法进行注册，而是将 Engine 库直接添加到 OpenVPN 中，通过加载代码直接加载该 Engine，实现对算法的调用，并且若添加的自定义算法发生改变，只需修改 engine 中该算法的实现过程，将 SSLeay 底层加密算法与该算法绑定以实现替换，不需要对 OpenSSl 源代码进行修改。本文提出的方法相对于注册算法的方法在提高安全性的同时减小了代码的开销。

5　结　　论

针对基于 SSL 协议的 VPN 技术存在的加密算法弱强度导致的安全问题，本文提出并实现了一种替换算法的解决方案。经上文的两部分测试结果表明：该方案能实现对弱强度算法的替换保证安全性，并且能够减小一定程度上的代码开销。从安全性能与代码开销上看，具有一定的实用意义，从应用的角度看，随着人们对安全性的要求越来越高，该系统的应用方面会越来越广，而不仅仅应用到银行，军事等传统高安全领域。

参考文献

[1] 李湘锋，赵有健，全成斌. 对称密钥加密算法在 IPsec 协议中的应用[J]. 电子测量与仪表学报，2014，28(1)：75-83.

[2] 陈晨，杨中岳，陈启美. 指纹远程登录的 SSL 安全通信系统[J]. 电子测量技术，2010，33(6)：123-129.

[3] 王凤领. 基于 IPSec 的 VPN 技术的应用研究实现[J]. 计算机技术与发展，2012，22(9)：250-253.

[4] 朱意秋. 基于 SSL 协议的 VPN 技术研究和实现[J]. 轻工科技，2015(5)：55-56.

[5] 周勇. VPN 技术 IPSec 和 SSL 的对比研究[J]. 信息通信，2012(3)：126-127.

[6] 诸晔，桂祚勤. 基于 OpenVPN 的虚拟专用网关键技术研究与实现[J]. 计算机安全，2014(1)：20-24.

[7] 周威，王博，潘伟涛. 祖冲之算法硬件实现与研究[J]. 国外电子测量技术，2015，34(7)：66-71.

[8] 任高峰，乔树山，黑勇. 祖冲之算法在数字图像加密中的应用与实现[J]. 科学技术与工程，2013，13(3)：766-770.

[9] 王玮，龙毅宏，唐志红，等. OpenSSL 引擎机制的研究[J]. 信息安全与通信保密，2011(10)：60-62.

[10] 董海韬，田静，陈君. OpenSSL 引擎机制与加密套件协商的应用研究[J]. 网络新媒体技术，2013，2(4)：13-17.

作者简介

吴建斌，1972 年出生，工学博士，副教授，硕士生导师主要研究方向为信息隐藏、探地雷达信号处理等。

费潇潇，1992 年出生，工学硕士，主要研究方向为信息隐藏。

E-mail：xiaoxiaofei@mails. ccnu. edu. cn

王年丰，1989 年出生，工学硕士，主要研究方向为信息隐藏。

(上接第 63 页)

作者简介

范振峰，工学硕士，主要研究方向为电磁场与电磁波、信号与信息处理。

E-mail：fanzhenfeng13@mails. ucas. ac. cn

黄玲(通讯作者)，工学博士，副研究员，主要研究方向为探地雷达方法、地球物理勘探方法等。

E-mail：lhuang@mail. ie. ac. cn