设计研究与应用

商用 IPSec VPN 密码检测技术研究

鹿洲 韩金波
（中国科学院长春光学精密机械与物理研究所，吉林长春 130033）

摘 要：商用 IPSec VPN 作为当前 VPN 市场中的主流产品，其应用的密码技术直接决定其加密效率和安全性。本文通过对商用 IPSec VPN 使用的加密算法、密钥交换协议阶段进行详细阐述，分析了商用 IPSec VPN 常用的密码检测技术，能够使网络技术人员掌握其加密过程和密码检测方法，并确保其安全性。

关键词：虚拟专用网络；密码检测；报文侦听；加密算法；随机性测试
中图分类号：TP393.08 **文献标识码：**A **DOI：**10.3969/j.issn.1003-6970.2023.05.029
本文著录格式：鹿洲,韩金波.商用IPSec VPN密码检测技术研究[J].软件,2023,44(05):114-117

Research on Commercial IPSec VPN Password Detection Technology

LU Zhou, HAN Jinbo
(Changchun Institute of Optics, Fine Mechanics and Physics, CAS, Changchun Jilin 130033)

【Abstract】：Commercial IPSec VPN is the mainstream product in the current VPN market, and its encryption efficiency and security are directly determined by the cryptographic technology it applies. This paper describes the encryption algorithm and key exchange protocol used by commercial IPSec VPN in details and analyzes the common password detection technology of commercial IPSec VPN, which can enable network technicians to master its encryption process and password detection method to ensure its security.

【Key words】：virtual private network;password detection;message interception;encryption algorithm; randomness test

0 引言

随着网络安全意识的普及，越来越多的企业开始重视安全通信技术，而在众多安全通信技术中，虚拟专用网络（Virtual Private Network 简称 VPN）因其投入小、使用便捷及应用场景广泛等优点得到广泛应用。

IPSec（Internet Protocol Security）是一组基于网络层的、应用密码学技术的安全通信协议族，而 IPSec VPN 则是基于 IPSec 协议族所构建的在 IP 层实现的安全虚拟专用网络。通过在数据包中插入一个预定义头部的方式，来保障 OSI 上层协议数据的安全，主要用于保护 TCP、UDP、ICMP 和隧道的 IP 数据包。通过将 IPSec 协议应用到 VPN 上，能够更好地保证通信数据的机密性、完整性和不可抵赖性 [1]。

IPSec VPN 虽具备数据加密、身份识别、完整性检查等技术手段，但世界各地依然出现了很多产生重大影响的 IPSec VPN 攻击事件，因而对 IPSec VPN 的密码检测技术就变得至关重要。下面将对商用 IPSec VPN 的加密算法和密码检测技术进行详细研究。

1 加密算法

商用 IPSec VPN 中同时用到了对称加密算法、非对称加密算法与 Hash 算法，故此处对三者分别进行阐述。

1.1 对称加密算法

对称加密算法是指发送方与接收方使用同一个密钥，发送方用此密钥将明文加密为密文，接收方再用此密钥将密文解密为明文。对称加密算法可理解为机械锁与钥匙的关系。数据加密即把需要保护的东西用机械锁锁起来，密钥即机械锁的钥匙，可见同一个机械锁可以有多把相同的钥匙，任何人拥有这把钥匙都可以加锁或者解锁。对称加密算法如图 1 所示。

商用 IPSec VPN 常用的对称加密算法有 DES、3DES、AES 等。在国密 IPSec VPN 中，根据 GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》中的要求 [2]，规定

作者简介：鹿洲（1991—），男，黑龙江哈尔滨人，硕士研究生，工程师，研究方向：信息化建设与网络安全。

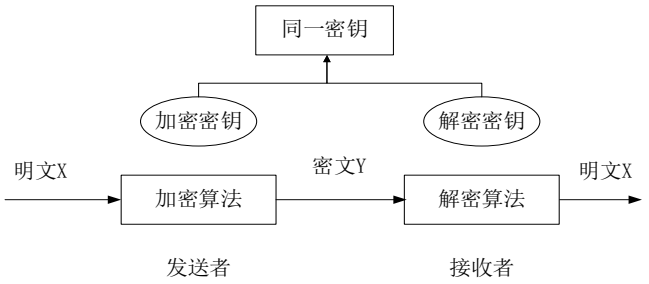

图 1 对称加密算法

Fig.1 Symmetric encryption algorithm

其在对称密码算法方面应当支持 SM4 分组密码算法。

1.2 非对称加密算法

在非对称加密算法中，发送方与接收方各有两个密钥，分别为公钥与私钥，且无法由其中一个密钥算出另一个密钥。在通信之前，发送方与接收方都将自己的公钥公开，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，所以非对称加密算法又名公开密钥加密算法。这样，信息就可以安全无误地到达目的地了，即使被第三方截获，由于没有相应的私钥，也无法进行解密，保证了加密过程是一个不可逆过程，即只有用私有密钥才能解密。非对称加密算法如图 2 所示。

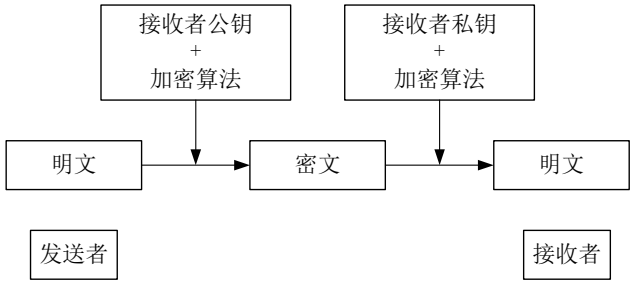

图 2 非对称加密算法

Fig.2 Asymmetric encryption algorithm

商用 IPSec VPN 常用的非对称加密算法有 RSA 等，在国密 IPSec VPN 中，根据 GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》中的要求，规定其对称密码算法应当支持 SM2 加密算法。对比对称加密算法与非对称加密算法后发现：对称加密算法的优点是加密速度快、效率高，能够对体量大的数据进行加密；但是其缺点也很明显，由于加解密都用同一个密钥，使其安全性完全依赖于密钥的安全性，密钥在传递过程中被任何人截获都可能将密文破解；非对称加密算法的优点是不公开不传递私钥，避免了密钥泄露问题，发送方与接收方只需要管理自己的私钥，降低了密钥管理复杂度，其缺点是非对称加密算法计算复杂度高、加密速度慢，一般情况下 RSA 算法要比 DES 算法加密速度慢 1000 倍。可见在传输数据量较大的情况下，非对称加密算法是不适用的。

商用 IPSec VPN 综合考虑了两类算法的优缺点，其整体流程可简述为：使用对称加密算法对报文进行加密，然后通过非对称算法 Diffie-Hellman（D-H）来保护对称加密算法的密钥 [3]，再进行密钥传递，这样既提高了加密效率，又保证了数据安全性。

1.3 Hash 算法

Hash 算法（哈希函数）是指任意长度的数据经过该算法运算，均输出为固定长度的数据，此数据称之为哈希值。Hash 算法必须具有以下 3 个特点：（1）无论输入多长的消息，输出都是固定长度，一般认为输出越长越安全；（2）输入消息不同，消息摘要不同，输入相同，消息摘要一定相同；（3）消息摘要的生成是单向不可逆的。

由以上特点可知，Hash 算法可用来保证传输消息的完整性和验证传输的消息是否被篡改，商用 IPSec VPN 常用的 Hash 算法有 SHA1、MD5 及国产算法中的 SM3 等。

2 IPSec VPN 加密检测

通过比较主流的 VPN 产品发现，IPSec VPN 的安全机制相较于 SSL VPN 更为健壮，目前能够对其加密方式进行检测的手段主要为报文侦听（即报文抓取后的格式分析）与随机性测试。

2.1 报文侦听

商用 IPSec VPN 的报文侦听需要对 IPSec 协议族的组成、协议内的载荷结构等进行研究，根据协议组成与结构来对协议报文抓取后进行分析，从中得到 IPSec VPN 加密的相关密码参数。而与 IPSec VPN 协议族和密码参数直接相关的，即是密钥交换协议（IKE）的两个阶段：第一阶段称为主模式，第二阶段称为快速模式。对实际 IPSec 报文加密采用何种加密算法（对称加密算法）在第一阶段协商确定；对 IPSec 报文加密使用的密钥（又称会话密钥）在第二阶段生成 [4]，会话密钥生成时需要利用第一阶段产生的其他密钥信息。第一阶段还需完成通信双方的身份验证与密钥协商，其中密钥协商是指非对称算法（D-H 算法）的密钥信息（又称工作密钥）。

主模式通过 3 次“握手”，共计 6 条消息，完成安全参数协商、密钥素材交换和身份认证。主模式 3 次“握手”如图 3 所示。

第一次“握手”的两条消息完成安全参数协商。协商出 IKE 5 元组：加密算法、Hash 算法、身份鉴别方式、DH 交换和 SA 生命周期，5 元组信息为明文信息。

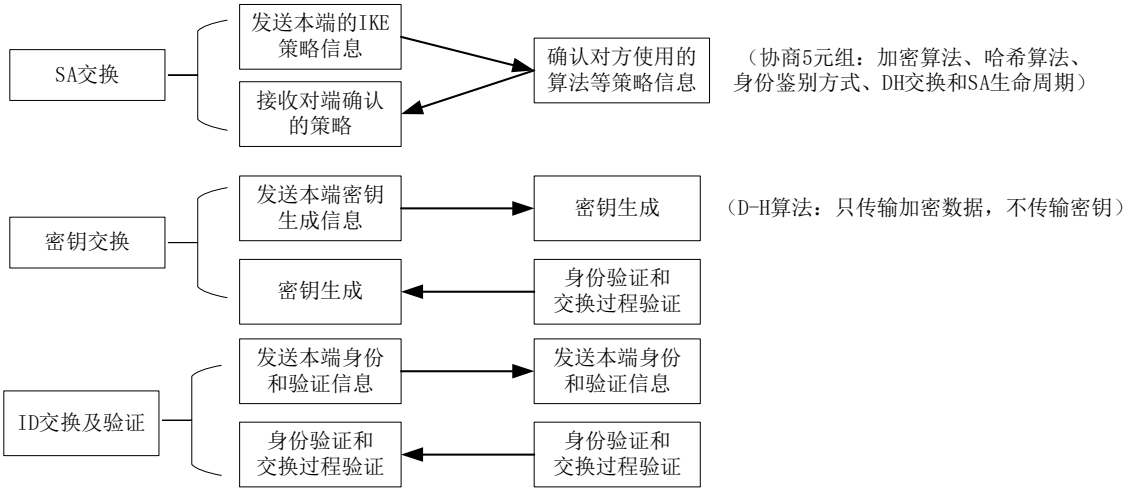

图 3 主模式三次“握手”

Fig. 3 Three "handshakes" in main mode

第二次“握手”的两条消息完成密钥素材交换。这一阶段的目的是确定基本密钥参数 SKEYID，以便用其生成 3 个密钥参数：SKEYID_e、SKEYID_a、SKEYID_d。3 个参数的作用是：SKEYID_e 对载荷主体进行加密处理，SKEYID_a 对指定报文字段进行完整性校验，SKEYID_d 则用于生成最终在 IPSec 报文加密使用的对称密钥。

第三次“握手”的两条消息完成全局身份验证。快速模式是通过 3 条消息协商出会话密钥，但 3 条消息都被加密保护。分析后发现，在 IPSec VPN 两个阶段中，只有主模式的部分明文信息可作为密码检测的参数。以某品牌 IPSec VPN 为例，经抓包分析后，主模式中 5 元组的结果部分为：加密算法：3DES-CBC；Hash 算法：MD5；身份鉴别方式：共享密钥（PSK）；SA 生命周期：1h；D-H 组密钥交换：1024 bit。此处加密算法即 IPSec 报文加密所用的对称加密算法，这些参数就是 IPSec VPN 的相关检测项中的部分指标，除此之外还包括 IP、端口、Nonce 随机数等密码参数 [5]。

2.2 随机性测试

商用 IPSec VPN 的安全联盟协商或会话建立过程中涉及的密码安全参数中，一部分重要参数是非描述性的（主要包括会话协商时相互交换的密钥素材、加解密时用来填充的初始化向量），从密码学安全角度出发，这些密码参数在编码形式上应满足随机性的要求。故需要在密码参数提取分析基础上，对这些密码参数的随机性进行测试，并给出定量评估。

从数学的角度分析其随机性，即对这些参数进行显著性检验，通过显著性水平 α 与检验 p 值的关系，判断其是否符合安全要求。

目前国际比较知名的随机性测试标准为 NIST 标准，具体包括以下检测项：单比特频数测试、块内频数测试、游程测试、块内最长游程测试、二进制矩阵秩测试、离散傅里叶变换测试、非重叠模板匹配测试、重叠模板匹配测试、通用统计测试、线性复杂度测试、序列测试、近似熵测试、累加和测试、随机游走测试、随机游走变量测试。

国密随机性检测的标准是在国际标准的基础上进行了调整，包含了国际标准大部分检测项的同时又增加了部分检测项，具体为：单比特频数检测、块内频数检测、扑克检测、重叠子序列检测、游程总数检测、游程分布检测、块内最大“1”游程检测、二元推导检测、自相关检测、矩阵秩检测、累加和检测、近似熵检测、线性复杂度检测、Maurer 通用统计检测、离散傅里叶检测。

然而，在实际检测过程中，待测数据的长度往往不能同时满足所有检测项中对长度的要求，即意味着如果直接进行检测，部分检测项会无法完成。故从安全角度考虑，为了完成所有检测项，对不符合其长度要求的检测项，可以采取补充扩展的方式，使其长度符合要求。取待测数据的一段待测序列，在开始测试前，先进行长度匹配，如果满足测试的长度要求，就进入测试模块进行判断，判定结果用“0”（非随机）或“1”（随机）表示，否则进行序列扩展处理，扩展后串接后的长度满足该标准测试模块的最低输入长度要求后，即可进行该项测试模块，如此循环往复，完成全部测试。具体流程如图 4 所示。

采用上述随机性测试方法，基本可以完成对非描述性密码参数的初步判定，参考此判定结果也可以决定是否还需要更进一步的大型测试，比如国家密码局的正式检测等。相比大型测试之下，这种初步判定方法在时间

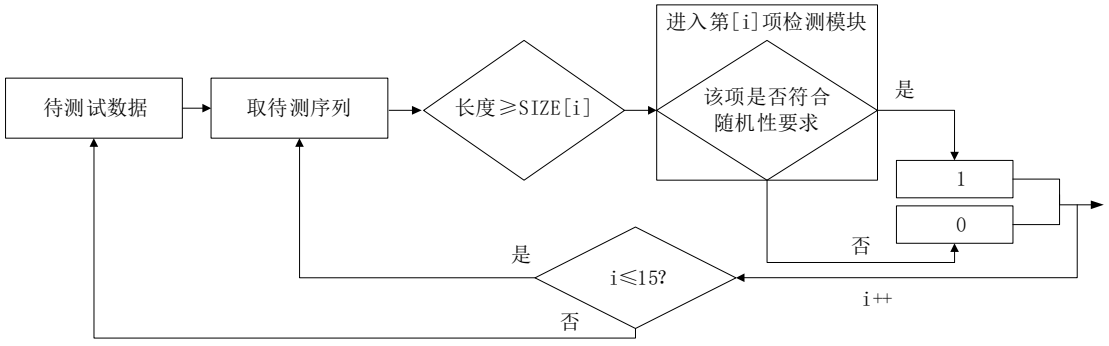

图 4 密码参数的随机性扩展测试

Fig.4 Randomness extension test of cryptographic parameters

成本、经济成本上更有优势，用户可以根据安全性要求自行选择测试方案。

3 结语

商用 IPSec VPN 利用对称加密算法对数据报文进行加密，利用非对称算法保护对称加密算法密钥的传递，并通过消息摘要算法来保证数据的完整性。其密码检测方法有报文侦听与随机性测试，其中报文侦听能够完成描述性密码安全参数的识别；随机性测试能够判定非描述性密码参数的随机性是否符合安全性要求。

参考文献

[1] 张越.国密IPSec VPN安全机制研究与实现[D].西安:西安电子科技大学,2018.

[2] GB/T 36968-2018.信息安全技术 IPSec VPN技术规范[S].

[3] 博兰普拉格德.IPSec VPN设计[M].北京:人民邮电出版社,2006.

[4] 王春海,宋涛.VPN网络组建案例实录(第2版)[M].北京:科学出版社,2011.

[5] 周益旻,刘方正,王勇.基于混合方法的IPSec VPN加密流量识别[J].计算机科学,2021,48(4):295-302.

…… 上接第94页

参考文献

[1] 全国信息与文献标准化技术委员会.信息与文献 信息交换格式:GB/T 2901—2012/ISO 2709:2008[S].北京:中国标准出版社,2012:4.

[2] BASSETT L.JSON必知必会[M].魏嘉汛,译.北京:人民邮电出版社,2016:1.

[3] 马尔斯.JSON实战[M].邵钏,译.北京:人民邮电出版社,2018:3.

[4] 福塔.正则表达式必知必会[M].门佳,杨涛,译.修订版.北京:人民邮电出版社,2019:4.

[5] FRIEDL J E F.精通正则表达式(3版)[M].余晟,译.北京:电子工业出版社,2012:1.

[6] NDJSON.ORG.Newline Delimited JSON[EB/OL].(2020-06-23)[2022-10-10].http://ndjson.org.

[7] MOUAT A.Docker开发指南[M].黄彦邦,译.北京:人民邮电出版社,2017:3.

[8] 浙江大学SEL实验室.Docker容器与容器云(2版)[M].北京:人民邮电出版社,2016:4.

[9] 杨保华,戴王剑,曹亚仑.Docker技术入门与实战(3版)[M].北京:机械工业出版社,2018:5.

[10] CARLSON J L.Redis实战[M].黄健宏,译.北京:人民邮电出版社,2015:4.

[11] Redis.RediSearch[EB/OL].(2022-07-27)[2022-10-10].https://redis.io/docs/stack/search/.

[12] Redis.RedisJSON[EB/OL].(2022-09-08)[2022-10-10].https://redis.io/docs/stack/json/.