PKI技术在IPSec系列协议中的应用*)

谭兴烈[1] 王天忠[2] 唐国栋[3] 周明天[4] 沈昌祥[5]

(四川大学数学学院 成都卫士通信息产业股份有限公司 成都610041)[1]

(成都卫士通信息产业股份有限公司 成都610041)[2] (信息产业部电子第三十研究所 成都610041)[3]

(电子科大卫士通信息安全实验室 成都610054)[4] (海军计算技术研究所 北京100841)[5]

Using PKI in IPSec Protocol Suite

TAN Xing-Lie[1] WANG Tian-Zhong[2] TANG Guo-Dong[3] ZHOU Ming-Tina[4] SHEN Chang-Xiang[5]

(Mathematics College of Sichuan University, Chengdu Westone Info Co,Ltd, Chengdu 610041)[1]

(Westone Information Industry INC,Chengdu 610041)[2] (No30 Electronic Institute,Ministry of Information Industry,Chengdu 610041)[3]

(Westone Information Secutity Lab,UESTC,Chengdu 610054)[4] (Navy Institute of Computing Technology,Beijing 100841)[5]

Abstract PKI and IPSec are the widely used technologies in today's information security area. In this paper,PKI and IPSec are discussed briefly at first. Then two methods of combining PKI with IPSec are proposed with details,and how to use PKI in IPSec configuration management is also discussed. Finally,it points out that identity of IPSec communication entity may be the special user but not limited to IP address with PKI. It also points out that PKI makes athentication of IPSec entity more secure and reliable,and makes IPSec configurations more flexible.

Keywords Public key infrastructure, IPSec protocol, Security association ,Internet key exchange protocol

1 引言

PKI(Public Key Infrastructure)即"公共密钥基础设施",是一个用公钥的概念和技术实施和提供安全服务的具有普遍适应性的安全基础设施,也是一个利用现代密码学中的公钥密码技术在开放的Internet网络环境中提供数据加密以及数字签名服务的统一的技术框架。IPSec是网络层安全的事实上的标准,尽管IPSec协议在处理多播协议以及在B2B环境中使用保留地址组建VPN等方面还存在这样那样的问题,但它目前还是得到了广泛的应用,是IP层安全公认的标准,同时它也是目前广泛利用的VPN技术。

本文首先简要介绍了PKI技术、IPSec技术,之后具体讨论了PKI技术与IPSec系列协议结合的方式,并分析了结合后带来的好处。

2 PKI技术及IPSec技术简介

2.1 PKI技术

2.1.1 *公开密码算法和证书体系* 区别于对称密码算法使用同一个密钥来加密/解密,公开密钥使用一个密钥对(公钥私钥对)来进行加密/解密,其中一个密钥加密的数据,只有使用另一个密钥来进行解密。用公钥加密,只能用对应私钥解密,这样就可以用来实现数据加密传送,也可以用来实现密钥的交换;用私钥来加密整个文档或文档的一个摘要,任何人都可以用公钥来解密检验其完整性。

公钥/私钥对的产生可以在可信的机构如CA中产生,此时私钥的分发通过安全的方式进行,公钥以证书的方式存放。公钥/私钥对也可以在CPU卡或USB令牌中产生,私钥产生后从不导出到CPU卡或USB令牌外,私钥运算只在设备内进行。

*)本文受国家863宽带VPN项目863-104-03-01课题资助。谭兴烈 博士,高工,主要研究方向为宽带VPN安全、应用系统安全及信息安全系统设计。

参考文献

1 徐秋亮.改进门限RSA数字签名体制.计算机学报,2000,23(5)

2 Desmedt Y, Frankel Y. Threshold Cryptosystem. In: Proc. of Crypto'89, Lecture Notes in Computer Science, LNCS 435, Springer Verlag,1990. 307～315

3 Hwang T. Cryptosystem for group oriented cryptography. In: Proc. of Eurocrypt'90, Lecture Notes in Computer Science, LNCS 473, Springer Verlag,1991. 352～360

4 Pedersen T P. Distributed Provers with Applications to Undeniable Signatures. In:Proc. of Eurocrypt'91, Lecture Note in Computer Science, LNCS 547, Springer Verlag,1991. 221～238

5 Pedersen T P. A Threshold Cryptosystem without a Trusted Party. In:Proc. of Eurocrypt'91,Lecture Notes in Computer Science, LNCS 547, Springer Verlag,1991. 522～526

6 Feldman. A Practical Scheme for Non-Interactive Verifiable Secret Sharing. In: Proc. of 28th IEEE symposium on Foundations of Computer Science,1987. 427～437

7 Park C,Kurosawa K. New ElGamal Type Threshold Digital Signature Scheme. IEICE Trans. Fundamentals, 1996,E79-A(1):86～93

8 王育民,刘建伟.通信网的安全-理论与技术.西安电子科技大学,1999

9 Shamir A. How to Share a Secret. Communications of the ACM, 1979,22(11):612～613

10 刘木兰,周展飞,陈小明.密钥共享体制.科学通报,2000.45(9)

11 http://grouper.ieee.org/groups/1363/StudyGroup/contributions/th-sche.pdf

2.1.2 CA、RA 及 CA 体系结构 CA 是签发和管理证书的实体。RA 负责核查申请证书实体的身份，并完成提交数据正确性验证。

根 CA 的证书是一个自签名的证书，所以根 CA 是一个自治的 CA，它位于 CA 体系的顶部，在该体系内，根 CA 是受信任的源头。

CA 有多种体系结构，如层次式的 CA 系统、平级的交叉认证(在不同 PKI 的 CA 间拓展了信任)、桥 CA 方式等。

2.2 IPSec 系列协议

2.2.1 IP 包的安全封装 IPSec 协议是公认的 IP 层安全标准，不仅能在目前通行的 IPv4下工作，也能在 IPv6下工作，主要包括封装的安全载荷 ESP(Encapsulating Security Payload)协议、鉴别头 AH(Authentication Header)协议以及 IPSec 密钥管理协议。

ESP 主要保护 IP 数据包的机密性、数据的完整性以及对数据源的身份验证，并且可抗重播攻击。可以保护整个 IP 包(隧道模式)，也可以只保护 IP 包内的数据(传输模式)，如图1所示，此时图中 IPSec 头为 ESP 头，阴影部分是被加密保护部分。

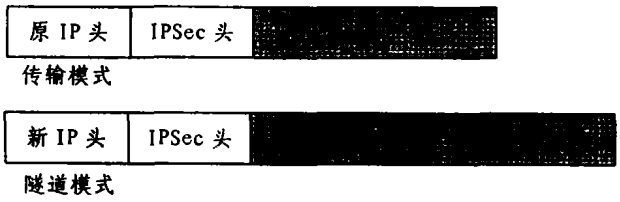

图1 IPSec 的两种工作模式

AH 提供了数据完整性、数据源鉴别以及抗重播攻击的能力。可以对整个 IP 包的数据进行封装(隧道模式)，也可以只对 IP 包内的上层数据进行封装(传输模式)，如图1所示，此时其中 IPSec 头在此为 AH 头，注意两种模式的被验证保护部分是整个新封装的 IP 包。

IPSec 的 ESP 处理和 AH 处理包括传输模式与隧道模式，隧道模式用于网关与网关之间的安全，传输模式用于保护主机与主机之间的安全。AH 与 ESP 协议可以单独使用，也可以结合使用。

2.2.2 IPSec 密钥管理协议 IKE 指 IKE(Internet Key Exchange)[1]系列协议，它用来实现 IPSec 协议所需要的算法、密钥、通信的保护方式(隧道/传输模式)、密钥的生命期等参数的协商等处理。IPSec 密钥管理协议是建立在由 Internet 安全关联和密钥管理协议(ISAKMP)[2]定义的一个框架之上并结合了 Oakley[3]和 SKEME 协议的混合型协议。ISAKMP 定义了包格式、重发计数器、消息构建要求以及安全关联 SA 的内容等。Oakley 协议的基本思想是对每一个会话密钥都采用 Diffie-Hellman 密钥交换机制，随后采用签名交换来确认 Diffie-Hellman 参数，确保没有"中间人"进行攻击，IKE 并没有完全实现 Oakley 协议，只实现了满足 Oakley 协议目标的必要的子集。IKE 还引入了 SKEME 中公钥加密认证的方法和通过 nonce 载荷交换必要的随机数来实现快速的密钥交换。

3 PKI 技术在 IPSec 中的应用

3.1 概述

IPSec 密钥管理协议的密钥协商分为两个阶段，第一阶段主要完成 ISAKMP SA 的协商；第二阶段用第一阶段协商得到的 ISAKMP SA 形成安全通道保护 IPSec SA 的建立，所以整个安全体系建立在 ISAKMP SA 安全的基础之上，而 IPSec 采用 ISAKMP 框架下的 Oakley 密钥协商管理。Oakley 协议的基本思想，正如上面所述的是签名验证的 DH 交换。IKE 扩展了验证的方式，新加入了预共享密钥和公钥验证两种方式，此时采用加密方法对 DH 交换数据提供了机密性保护。预共享密钥方式在具体实现时又可以采用有多种方式，比如另外建立一个密钥管理中心，它与通信各方都共享一个主密钥，在此主密钥的保护下为通信双方临时分发预共享密钥；公钥加密的实现方式主要用公钥加密个人身份数据和密钥素材，只有对应的私钥正确解密了这些个人身份数据和密钥素材后才能让密钥交换继续下去；签名验证是在第一阶段的最后两个消息的末尾各自附上签名，签名保护的对象是参与 DH 交换的消息，对方就能确认 DH 交换的消息确实来自能验证签名的私钥持有者。这几种方法都需要通信双方预先拥有共享密钥或公钥并配置妥当，当有用户加入或离开时，就会导致新一次的密钥分发和配置，当用户数较多且变化较频繁时，其缺点是显而易见的。

综上可以看出 IPSec 采用 Oakley 作为 ISAKMP 框架下强制推行的密钥管理手段，而 ISAKMP 协议定义了 SA 以及密钥交换步骤，但不对交换的内容作具体解释，以 Oakley 协议定义的密钥交换机制来完成密钥交换，而 Oakley 运用 DH 算法完成密钥协商。在 ISAKMP SA 建立阶段，把证书作为 Oakley 属性值之一发送到通信对方，由对方验证证书有效后取出证书的公钥，然后进行标准的 RSA 签名认证以及公私钥加密解密运算来实现身份鉴别和数据保护，证书以这种方式与 IPSec 密钥交换相结合，弥补 DH 算法的缺陷，增强了密钥交换的安全强度。因此，面对大规模不断变换的网络用户环境，使用 PKI 技术来实现通信双方的身份验证、密钥交换等保护恰是十分方便的。

3.2 PKI 技术在 IPSec 密钥管理协议中的应用

3.2.1 基本思想及术语说明 IKE 中定义了三个与公钥有关的认证方式：签名认证、公钥加解密认证和改进的公钥加解密认证[1]。这三种方式中只有签名认证中有可选的证书载荷，我们将此可选项变为必选项，同时要求证书作进一步处理，比如验证证书合法性等；另外两种方式没有涉及到证书，我们需要在适当的地方交换证书信息并做必要的处理。下面我们详细讨论 PKI 技术与三种方式的结合。

下文描述中用到的符号的含义说明如下：

Initiator/Responder：ISAKMP 协议中的发起者/响应者；

HDR：ISAKMP 消息头，HDR * 指 ISAKMP 头之后紧跟的是加密载荷；

SA：安全关联协商载荷，发起者的安全关联协商载荷中可以提供多个提议载荷，而响应者的安全关联协商载荷中只能有一个提议载荷，该提议载荷是从发起者的提议载荷中选择的；

b：指整个载荷体，它不包括 ISAKMP 消息头；

SAi_b，由发起者提供的除了 ISAKMP 通用头的整个 SA 载荷体，即发起者提供的 DOI、所有提议载荷和转码载荷；

CKY-I /CKY-R：发起者/响应者的 cookie；

g ^ xi / g ^ xr：发起者/响应者的 Diffie-Hellman 共享值；

g ^ xy：Diffie-Hellman 共享秘密；

KE：密钥交换载荷，其中包含 Diffie-Hellman 交换的公

共信息；

Nx：nonce 载荷，x 可能是 i 或者 r，各自表示是 ISAKMP 发起者或响应者；

Idx：指 x 的 ID 载荷，x 可以是：ii 或者 ir，表示第一阶段交换的发起者和响应者；

Cert/CERT：证书载荷，Cert-I_b 和 Cert-R_b 分别指发起者和响应者的证书载荷；

SIG_I/SIG_R：发起者/响应者的签名载荷；

prf(key，msg)：键控 Hash 函数，一般用于密钥衍生或消息验证；

PrivKey_i/PrivKey_r：发起者/响应者的私钥；

PubKey_i/PubKey_r：发起者/响应者的公钥；

〈x〉y：x 被密钥 y 加密；

X | Y：表示 X 与 Y 串联；

[x]：表示 x 可选。

→：表示通信方向为“从发起者到响应者”(请求)

←：表示通信方向为“从响应者到发起者”(应答)

3.2.2 *无需增加新载荷的结合方式* 这种结合方式对原协议的改动较少，但只适用于签名认证，不过可以用于其主模式和积极模式。

将原协议中定义的可选证书载荷变为必选载荷，并且要求对对方证书认证，即需要对 CA 的签名、时间有效、证书是否被撤销等验证，认证接受后再从该证书中取出身份信息和公钥对 SIG_I 或 SIG_R 作签名验证：

对于签名认证方式中的主模式，与 PKI 技术的结合方式如下：

Initiator		Responder
HDR, SA	→	
	←	HDR, SA
HDR, KE, Ni	→	
	←	HDR, KE, Nr
HDR*, IDii, Cert-I_b, SIG_I	→	
	←	HDR*, IDir, Cert-R_b, SIG_R

对于签名认证方式中的积极模式，与 PKI 技术的结合方式如下：

Initiator		Responder
HDR,SA,KE,Ni[,IDii]	→	
	←	HDR, SA, KE, Nr, [IDir,] Cert-R_b, SIG_R
HDR, Cert-I_b, SIG_I	→	

其中，

SIG_I=〈HASH_I〉PrivKey_i

HASH_I=prf(SKEYID,g^xi|g^xr|CKY-I|CKY-R|SAi_b|IDii_b)

SKEYID =prf(Ni_b|Nr_b, g^xy)

SIG_R=〈HASH_R〉PrivKey_r

HASH_R=prf(SKEYID,g^xr|g^xi|CKY-R|CKY-I|SAi_b|IDir_b)

所以，双方的 cookie(CKY-I,CKY-R)，DH 密钥交换数据(g^xi,g^xr)及双方的共享秘密(g^xy)，发起者安全关联载荷体(SAi_b)，现场数据(Ni_b,Nr_b)，以及双方的身份信息(IDii_b,IDir_b)都在签名保护之内。

另外需要注意的是，因为证书中有身份信息，所以 IDii_b 和 IDir_b 为可选项。如果没有选用 IDii_b 和 IDir_b，在需要用到 ID 信息的地方，用证书中的身份信息替换(以下类同)。

3.2.3 *需增加新载荷的结合方式* 这种结合方式主要是在第一、二条消息中加入证书载荷，实现证书交换，并且需要对证书进行验证，然后用证书中的公钥完成其余的交换步骤。此种方式适合于三种认证方式，现说明如下。

对于签名认证方式的阶段1，与 PKI 技术的结合方式如下：

Initiator		Responder
HDR, SA, Cert-I_b	→	
	←	HDR, SA, Cert-R_b
HDR, KE, Ni	→	
	←	HDR, KE, Nr
HDR*,[IDii,] SIG_I	→	
	←	HDR*,[IDir,] SIG_R

双方在收到证书后，立即进行证书验证，然后继续完成整个密钥交换。SIG_I 和 SIG_R 的计算方式与上一小节描述的相同。

对于公钥加密认证方式的阶段1，与 PKI 技术的结合方式如下：

Initiator		Responder
HDR,SA,Cert-I_b	→	
	←	HDR,SA,Cert-R_b
HDR,KE,[HASH(1),] [〈IDii_b〉PubKey_r,] 〈Ni_b〉PubKey_r	→	
		HDR, KE, [〈IDir_b〉PubKey_i,]
	←	〈Nr_b〉PubKey_i
HDR*, HASH_I	→	
	←	HDR*, HASH_R

双方在收到对方的证书时，也需要进行证书有效性的验证，验证通过后取出证书中的个人身份信息和相应的公钥。加密中所用公钥 PubKey_i 和 PubKey_r 来自于第一、二条消息中的证书载荷。需要注意的是，因为从证书中可以取用身份信息，所以我们将 IDii_b 和 IDir_b 载荷变为可选载荷。另外，HASH(1)是用 SA 中协商好的 HASH 算法对发起者的证书作 HASH 运算所得结果(从原协议沿袭而来，意义不大，建议不用，以下类同)。

对于改进的公钥加密认证方式的阶段1，与 PKI 技术的结合方式如下：

Initiator		Responder
HDR,SA,Cert-I_b	→	
	←	HDR,SA,Cert-R_b
HDR,[HASH(1),] 〈Ni_b〉Pubkey_r, 〈KE_b〉Ke_i, [〈IDii_b〉Ke_i]	→	
	←	HDR,〈Nr_b〉PubKey_i,

〈KE_b〉Ke_r,[〈IDir_b〉Ke_r,]
HDR*, HASH_I →
← HDR*,HASH_R

也是首先完成证书验证，然后再取用公钥，IDii_b 和 IDir_b 仍然为可选载荷。其中 Ke_i 由 Ni_b 和 CKY-I 演算而来，Ke_r 由 Nr_b 和 CKY-I 演算而来，作为 SA 中协商好的对称加密算法的密钥。Ke_i 和 Ke_r 的具体演算过程如下：

Ne_i = prf(Ni_b, CKY-I)

Ne_r = prf(Nr_b, CKY-I)

如果加密算法的密钥位数小于或等于 Ne_i/Ne_r 的位数，Ke_i/Ke_r 直接从 Ne_i/Ne-r 的高位开始取，取够为止；否则，将 prf 的运算结果反馈到 prf 中继续运算，并把结果串联起来，直到串联位数大于或等于密钥位数为止，密钥从串联结果的高位开始取，取够为止。例如密钥需要320位，而 prf 输出只有128位，则密钥 Ke_i 为如下计算的 K 的高320位：

K=K1|K2|K3，其中：

K1=prf(Ne_i,0)

K2=prf(Ne_i,K1)

K3=prf(Ne_i,K2)

3.2.4 PKI 技术与 IPSec 的配置管理相结合 IPSec 的主要目的是为通信双方建立安全的 IP 通道，其工作标识是 IP 或 IP 对，IP 并不固定对应于某个实体，时间地点的不同，同一个实体的 IP 往往也不同，而且还有很多因素会改变一个实体与 IP 的对应；证书主要包含个人身份信息和公钥，这些信息相对固定地对应于某个实体，而且不随时间地点及诸多因素的改变而改变。从工作层次上说，IP 工作在网络层，一般不与用户对应，而证书却要与用户对应，工作在应用层。IP 是平等开放的，证书却对应着身份和权限。所以我们不仅要对证书作验证，还要根据证书信息对 IPSec 用户进行分门别类的限制，满足不同应用要求。可以用证书中个人身份信息的部分或全部、源或目的 IP 地址、IPSec 的协议如 ESP 或 AH 及工作模式等信息形成配置项，检查 IPSec 通信的合法性。例如一个公司用一个网关与 Internet 相连，在网关处可以作如下配置：若目的地址为 Web 服务器，则个人身份信息的公司名与本公司名一致的为可接受者，而目的地址为公司内部的一台有机密数据的服务器则配置为不仅要求与公司名称一致，而且要求是指定的相关人员才可接受，参见图2。

[src=*,dst=Addr_Web,prot=tcp,
srcid=?CN/ST=Sichuan/L=Chengdu/O=Westone Information Industry Ltd"]→
IP see prot=esp mode=transport algorithm=WSTALG-SHAI
[src=*,dst=Addr_ConfInf,prot=tcp,
srcid="/C=CN/ST=Sichuan/L=Chengdu/O=Westone Information Industry Ltd/CN=CTO/Email=cto@westone.com.cn"]→
IPSec prot=esp mode=tunnel algorithm=WSTALG-SHAI

图2 证书身份信息参与 IPSec 策略配置的示意图

有的证书如 X.509 V3证书[4]含有扩展项，部分扩展项也可以用于配置项参数。利用证书身份信息和/或证书扩展项信息的部分或全部，可以形成不同的配置粒度，满足不同的需要。比如对于 X.509 V3 证书，它有一系列的标准扩展项，各扩展项都有其特殊用途，其中证书持有者可替换名(subjectAltName)主要用于扩充定义与证书持有者相关的信息，比如 Email 地址、统一资源识别符(URI)、职位等等。一个公司或部门可以定义一些独特标识放于内部人员证书的 subjectAltName 域中，配置文件指定这些标识与访问策略对应，实现群组与策略的对应。

配置项可以存放于数据库中，也可以形成配置文件存放于相对安全的区域。对于移动用户或配置项较少的用户，还可以把配置项存放于 IC 卡、USB 令牌等安全介质上。同时有了证书信息参与的 IPSec 配置，大大拓展了 IPSec 的应用范围。

3.2.5 PKI 技术与 IPSec 相结合的优势 没有与 PKI 技术结合的 IPSec 协议要求通信双方的身份信息以及公钥必须预先传送给对方，由对方配置好。有多少个通信用户，就需要配置有相应数量的身份信息和公钥，显然当用户量较大时，配置文件将变得过分庞大，对用户的检索也变得不是十分方便。另外，身份信息和公钥在传输过程中，难免会遭受窜改，从而破坏其完整性，再加之 IPSec 没有提供有效的方法去检测这些错误，其最终体现可能是通信不成功，导致服务被拒绝，也可能出现通信对方是一个恶意的冒充者，导致信息泄密等。

与 PKI 技术相结合后，在 IPSec 的密钥交换协议中，首先通过交换证书的方式交换了可以信赖的身份信息和公钥(可以通过验证对方证书的有效性来实现)，在密钥交换的后续过程中利用验证了的身份信息，可以大大增强信息来源的可信度，通信双方的身份以及双方的密钥等信息的完整性就得到了充分的保证。

通过与 PKI 技术的结合，IPSec 配置文件中只需要配置少数几个 CA 证书(它是指 CA 自身的证书，而非普通用户的证书，普通用户的证书通过在线交换获取)就可以实现与大量用户通信，只要这些用户的证书是由配置文件中配置有证书的 CA 所签发的。

随着 PKI 技术的进一步完善，我们还可以通过访问 PKI 的其他基础设施如 LDAP 服务器、OCSP 服务器等，去实时获取更多更有效的信息，来进一步提高 IPSec 通信的灵活性，确保它的安全可靠。

结束语 本文讨论了 PKI 技术在 IPSec 协议中的应用，特别指出由于使用了证书可以为 IPSec 通信实体提供数字 ID，从而为 IPSec 与具体的用户实体间的对应提供了事实依据，使 IPSec 通信更具有灵活性，扩展了 IPSec 的应用层次和范围，IPSec 协议与 CA 如何进行通讯等方面还有待于进一步研究。

参考文献

1 RFC2409, D. Harkins, D. Carrel cisco Systems. Nov. 1998

2 RFC2408, D. Maughan, National Security Agency M. Schertler, Security, Inc. M. Schneider, National Security Agency J. Turner, RABA Technologies, Inc. Nov. 1998

3 RFC2412, H. Orman, Department of Computer Science, University of Arizona. Nov. 1998

4 RFC2459, R. Housley SPYRUS, W. Ford VeriSign, W. Polk NIST, D. Solo Citicorp. Jan. 1999