第32卷 第21期 计 算 机 工 程 2006年11月
Vol.32 No.21 Computer Engineering November 2006
·安全技术· 文章编号：1000—3428(2006)21—0170—03 文献标识码：A 中图分类号：TP393

支持交叉认证与状态检测的IPsec-VPN设计

杜春燕，杨绚渊，陆建德
(苏州大学计算机学院江苏省计算机信息处理技术重点实验室，苏州 215006)

摘 要：IPsec是为VPN制定的一组IP层安全协议，但随着应用的扩展和深入也出现了一些新的问题。文章将公钥基础设施PKI引入其中，结合ECC公钥技术，并增加了交叉认证接口设计，提出了一个基于改进的PKI体系的增强型IPsec VPN安全网关原型系统；同时对DPD协议进行了研究，设计并实现了对DPD的支持，从而有效弥补了现有IPsec VPN在身份认证和状态检测方面的缺陷，提高了VPN的安全性、可扩展性和健壮性。最后给出了一个基于Linux2.6内核的设计方案。

关键词：VPN；IKE；PKI；ECC；交叉认证；DPD

Design of Enhanced IPsec-VPN Supporting Cross-certification and Status-detection

DU Chunyan, YANG Xuanyuan, LU Jiande
(Jiangsu Province Computer IT Key Lab, School of Computer of Soochow University, Suzhou 215006)

【Abstract】IPsec is a set of security protocols in IP layer used for VPN. However, with its extensive and deep applications, some new problems have occurred. This paper introduces PKI and combines it with ECC technique and the design of cross certification interface, proposing an enhanced IPsec VPN security gateway prototype. Meanwhile, Dead peer detection (DPD) protocol is studied and implemented, so as to effectively improve on authentication and status detection to current IPsec VPN, assuring the security, extensibility and robustness of the VPN system. It gives out an implementing scheme based on Linux 2.6.

【Key words】VPN; IKE; PKI; ECC; Cross-certification; Dead peer detection(DPD)

IPsec是为VPN进行加密、隧道传送、认证的一系列IP层安全协议，主要包括认证头AH、封装安全载荷ESP、Internet密钥交换IKE等协议。虽然IPsec协议已较为丰富，但随着应用的扩展和深入，仍有一些需要解决和完善的问题。例如，当网络规模急剧增长或在远程终端用户访问网关(road warrior)的情况下，如何有效地解决身份认证和访问控制问题；当进行IPsec通信突然出现某些异常时，由于不能及时检测对方状态导致“黑洞”现象的产生，即数据包持续通过隧道发送但不能到达目的地，这在实际应用中是不允许的，而IPsec协议本身对这两种情况都无能为力。

PKI技术是一种遵循标准的密钥管理平台，能够为网络应用提供加密和数字签名等服务及所需的密钥和证书管理体系；DPD协议能有效探测对方状态，若对方处于不正常状态时则进行相应处理，从而解除了通信潜在的安全隐患，而这些正是目前IPsec所缺乏的。本文借助公钥基础设施PKI和DPD协议，在此基础上改进IKE协议，提出了一个增强的IPsec VPN安全网关原型系统。

1 基于PKI体系的IPsec身份认证

基于PKI的系统中，通信双方的信任关系和安全信道通过公钥证书建立，公钥证书是用户身份与其持有公钥间的相互绑定，绑定的有效性通过可信的第三方权威机构CA对数字证书进行签名实现，为系统的信息传递提供了机密性、真实性、完整性、不可否认性4大技术支持。遵循X.509证书标准的PKI称为PKIX[1]。

1.1 基于ECC的PKI的优越性

RSA是目前PKI较为流行的公钥算法，但ECC有着许多让人无法抗拒的相对于RSA的优越性，在信息安全领域中的应用正开始崭露头角。

ECC的安全性是基于椭圆曲线上的离散点分离问题。与RSA相比，ECC在相同加密强度下所需的密钥长度要短很多。以160位ECC和1 024位RSA为例，二者具有相同的安全强度，并且随着加密强度的提高，ECC密钥长度变化远远小于RSA密钥长度的增长速度。在相同安全强度下，ECC公钥和签名大小也比RSA小许多。ECC公钥由椭圆曲线上的某个点组成，一个160位ECC产生的公钥为40B大小，若采用点压缩技术(point compression)，则可减少到21B；160位ECC生成的签名为40B。1 024位RSA系统产生的公钥大小为131B，生成的签名大小为128B[2]。而且随着安全有效位数的增加，二者的差别更为明显。

当安全有效位数从80位增加到256位，即相应ECC组大小从160位增加到512位、RSA密钥大小从1 024位增加到15 360位时，ECC密钥生成时间和ECDSA签名生成时间大约增长了33倍；而RSA则分别超过了50 000和3 000倍[2]。因此，在既要获得较高的安全性，同时又要计算量小、效率高的情况下，ECC比RSA具有更大的优势，这也是本设计采用ECC的原因之一。

1.2 基于X.509证书主体信息的IKE身份载荷设计

X.509证书中主体(subject name)是证书拥有者的可识别

基金项目：江苏省自然科学基金资助项目(BK2004039)
作者简介：杜春燕(1981－)，女，硕士生，主研方向：计算机网络，信息安全；杨绚渊，硕士生；陆建德，教授
收稿日期：2006-02-15 **E-mail：**210313041@suda.edu.cn

名，在X.509v3 证书中增加了扩展项，其中的主体别名可以包括电子邮件地址、IP地址、URI等。根据IKE和IPsec PKI profile[3]中的相关说明，在基于X.509 证书的IKE主模式交换过程中使用这些数字证书中的身份标记信息供访问控制 使用。

当通信双方都是 VPN 网关时可以选择 IP 地址作为身份载荷 ID。但是对于远程登录用户来说，由于其 IP 地址不固定，因此 IP 地址作为 ID 是不适合的。这种情况下 IKE 交互第 1 阶段主模式中第 5 条和第 6 条消息发送的身份 ID，须与证书中的相关字段关联。如果使用 ID_DER_ASN1_DN(X.500 唯一名)作为 ID 则必须与该实体证书中的主题唯一名相同，而对 ID_FQDN(正式域名)或者 ID_USER_FQDN (用户 email 地址)来说则必须包含在 X.509 证书扩展项中的别名中。

1.3 基于证书的身份认证设计

IPsec VPN中常用的验证方法有预共享密钥(PSK)、数字签名、公钥加密、改进的公钥加密 4 种方式[4]。用PSK实现的身份认证，密钥只能通过双方IP地址来进行标识，这是PSK的一个致命缺陷，尤其对于远程登录的拨号用户，由于其没有固定IP地址，无法对其进行有效的身份认证，因此无法完成IKE协商。公钥加密和改进公钥加密方式的复杂性，以及公钥操作对象数据块较之数字签名有较大差别，使得后两种身份认证方法并未成为主流身份认证方式。基于X.509 证书的身份认证，用户身份同用户IP没有直接的关系，因而可以有多种选择，具有良好的可扩展性和安全性，提供了强身份认证。

使用 PKI 身份认证的 IKE 主模式第 1 阶段第 2 次、第 3 次交互可设计如下，通信双方完成身份认证信息的交互，以及对前两次交互的消息验证：

③ I→R：HDR；KEi；Ni

④ R→I：HDR；KEr；Nr；CR

⑤ I→R：HDR*；IDi；CERTi；SIGi

⑥ R→I：HDR*；IDr；CERTr；SIGr

其中，“ HDR* ”表示 ISAKMP 头之后的载荷是加密的。ID 可以是 1.2 节中所述的 X.509 证书主体身份信息。SIGi 和 SIGr 是协商的数字签名算法分别应用到 HASH_I 和 HASH_R 所产生的结果。

如果 IKE 初始化时双方没有提前载入对应的 ECC 公钥(或 RSA 公钥)，则响应方在第 4 条消息中需构造证书请求载荷 CR，请求发起方证书。相应发起方在第 5 条消息中传送本方 ECC 证书(考虑到兼容，也可以是 RSA 证书)，并构造签名 SIGi。如果本方没有则在载荷中标记本方证书存放的链接地址，对方可从该地址取得本方证书。相应地，在第 6 条消息中，响应方通过验证数字签名来检查通信对方实体的身份，这需要进行证书验证和解析处理从而获取对方的公钥，解密接收到的 ECC_SIG(或者是 RSA_SIG)，然后与计算所得的 HASH 值比较，若相同则验证通过。同时响应方还需发送身份载荷 ID、本方证书 CERTr 和签名 SIGr 供发起方进行验证。

1.4 IKE 协议中交叉认证接口设计

如果通信双方证书的CA相同或有从属关系，即是单CA模型或同信任域下属层次模型[5]时，双方可以通过证书链直接进行证书验证。但在实际应用中更多的情况是双方证书的CA属于不同的域，因此在VPN网关设计中就必须增加交叉认证接口设计，使得可以在之前无关的CA各自主体群间通信，提高系统的通用性和扩展性。

为了使系统能支持交叉认证，按照如下思路对 IKE 第 1 阶段的第 4、第 5、第 6 条进行改进。

首先通信双方需另外保存各自的本地信任列表，其中每一项对应一张本地证书，包括根信任锚 DN、证书、默认证书链等内容，其中根信任锚 DN 存放的是证书的根信任锚 CA 的唯一标识名，如果该证书由根 CA 签发，则该证书的签发者名与根信任锚 DN 一致，否则根信任锚 DN 与默认证书链的第 1 张证书的签发者一致。

确定本地信任列表后，在之后的 IKE 交互中，响应方取其所有的信任锚 DN 封装在证书请求载荷中，构造第 4 条消息发送给发起方。发起方收到该消息后，解析证书请求载荷取得请求的 DN 集合，然后在本地的信任列表中进行依次匹配(信任列表中证书的先后次序可以采用最近访问优先的方式排序)，如果匹配成功，则属于单 CA 模型或同信任域下属层次模型，只需直接把信任列表中的匹配到的第 1 张证书封装成第 5 条消息的证书载荷 CERTi，传给发起方；如果匹配不成功，即双方的信任锚无交集时，就需要进行交叉认证。

为了实现交叉认证，系统需另外添加一个路径构造与路径验证的代理服务器，完成路径构造、证书链的生成和验证以及交叉证书的生成和发布等功能。在此基础上发起方依次将信任列表中每个信任锚发送构造交叉证书链的请求，由代理服务器来帮助执行路径构造，并将构造好的交叉证书链后返回给发送方，然后发送方就可以把构造好的路径和所选信任锚对应的那张证书一起在消息 5 中发送给对方。如果信任列表都搜索完毕，也不能构造交叉路径，则发送通知载荷表明认证失败。同时，发起方也要构造证书请求载荷，取得响应方证书，过程同上。

响应方收到第 5 条消息后，解析出证书载荷和证书链，并依次对证书链中的每张证书进行检查，包括有效期、检查 CRL、验证签名等内容。然后解析发起方发送过来的证书请求载荷，根据证书请求载荷，进行类似于上述操作的处理，将自己的证书和相应的证书链给发起方。

发起方收到第 6 条消息后，要对证书进行解析验证操作。如果验证成功，则双方身份认证完成。否则发送通知载荷，告知身份认证失败，双方交互终止。

2 VPN 网关中应用状态检测 DPD 协议的设计

通信双方使用IPsec通信时，有可能出现异常情况，由于网络阻塞丢包或其它原因导致数据包不能正确到达对方；或者对方由于非正常原因删除了SA但没有发送删除消息(比如因故障重启)；或者本地网关因网络故障没有收到对方发来的删除消息，在上述情况下，本地主机因为未能及时了解对方状态，会继续使用原来的SA与对方进行通信直到手工删除SA或者SA超时，或者对方重新发起协商。这样就可能导致通信双方在相当长的一段时间内不能进行正确的安全通信，在实际应用中是不允许的。DPD[6] 协议设计的目的就在于及时探测通信双方可能存在的这种非正常状态，在探测到对方不能正常进行IPsec通信时能够主动删除本地IKE SA和IPsec SA，重新发起IKE协商，自动恢复安全通信，提高VPN网关的健壮性和效率。

在VPN网关软件设计中加入DPD协议后，DPD采用查询和应答机制，以IKE通知载荷[2]的形式发送查询和应答报文(R_U_THERE / R_U_THERE_ACK)来确定对方当前状态，如图 1 所示。双方采用已经建立的IKE SA对报文进行加密和认

证保护，如果IKE SA不存在或过期，则无法发送或响应DPD报文，也就意味着需要重新协商建立新的IKE SA和IPsec SA，恢复正常通信。

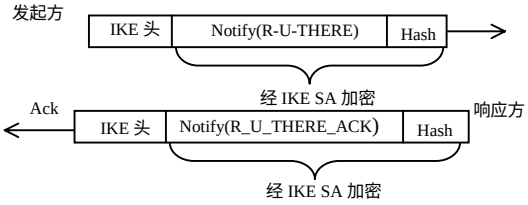

图 1 DPD 消息交换

在 IKE 主模式第 1 阶段 1、2 条消息中，通信双方发送 DPD 开发者 ID 载荷以支持 DPD 服务。在 IKE 第 2 阶段快速模式第 2 次交互中，双方根据配置的本地策略，为当前协商的连接初始化 DPD 服务参数，并在消息队列中插入该 DPD 事件，由时钟调度 DPD 事件。在设计中，VPN 网关指定如下策略来进行 DPD 相关设置：

```
conn netlab
dpddelay=1m //DPD 延时阈值
dpdtimeout=3m //DPD 超时阈值
dpdaction=clear //若超时，采取“clear” 或“hold”方式
```

双方各自维护一个定时器，发送查询报文的间隔或隧道空闲时间阈值可以根据紧急情况自行设置。以上述配置文件为例，发起方首先检查隧道是否有持续的 IPsec 数据流，如果有则无需发送查询报文。如果 IPsec 数据流空闲，且超过本地策略设定的空闲时间阈值，发起方每隔 1min 发送 R_U_THERE 消息，如果在 1min 内没有收到对应的 R_U_THERE_ACK 响应包，则重发，超过 3mn 若还没有收到应答，判定对方已不在线，可根据“clear”方式自动删除相关 SA 和路径流量信息，或“hold”方式清除包括 IKE SA、IPsec SA 内核相关数据结构，但保留路径流量信息，这样新信包到来时将迫使在原来连接上重新开始，并不会遗漏该路径上的流量信息。

3 IPsec VPN 安全网关总体设计

经作者所在课题组对最新 Linux2.6 内核的研究分析，2.6 新内核的设计已增加了 IPsec 基础处理框架，对 IPsec 协议提供了极大支持。因此设计了一个完整的 VPN 安全网关，其重点在于用户空间 IKE 子系统与用户管理子系统的设计。IKE 子系统按照功能分为 IKE 消息处理模块、IKE 状态库、证书处理模块、网络消息处理模块、DPD 处理模块、用户接口和内核接口，如图 2 所示。

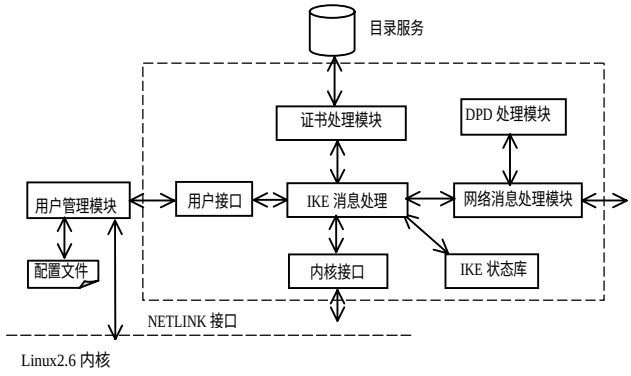

图 2 IPsec VPN 安全网关原型

其中，IKE 子系统中的证书处理模块负责从 LDAP 服务器查询并获取证书及 CRL，或者按本地策略在本地硬盘上读取证书，并对不同格式的数字证书进行解析、验证工作，其中路径构造与路径验证的代理服务器，完成路径构造、证书链的生成和验证以及交叉证书的生成和发布等功能。DPD 处理模块根据本地指定的策略，为参与通信的双方进行 DPD 交互提供统一的处理。内核接口模块通过 NETLINK 套接字与内核 IPSec 模块交互，实现 IKE 与内核 SADB 之间的消息传递。日志模块记录系统运行和 IKE 过程中的异常和错误信息以及用户指定记录的信息，供各个模块统一调用。

用户管理子系统接收用户控制台传来的配置和查询命令，通过 AF_UNIX 套接字与 IKE 消息处理模块进行交互，或者通过 NETLINK 接口调用内核中的 SA 与 SP 的各种处理，并相应调整、更新配置文件与日志。

根据图 2 设计的 IPsec VPN 网关工作过程如下：通信双方获得 CA 签发的 ECC 或 RSA 证书后，进行 IKE 协商，并在其过程中交换数字证书，根据实际情况确定是否需进行交叉认证，从而验证对方证书是否有效。然后通信双方在 IKE 协商建立阶段得到的 SA 基础上建立安全隧道连接，使用 ESP、AH 协议封装并传送信包。VPN 网关接收并解封信包，并结合具体策略进行访问控制。

IPsec 在需要与对方通信时，如发送数据包前，或已发送了数据包但还未收到响应的情况下，需要探测对方是否处于活动状态，检查对方是否有持续的 IPsec 数据报发送，如果有则说明对方处在活跃状态，无需发送查询报文；如果 IPsec 数据流空闲超过本地策略设定的时间间隔，则开始 DPD 交互，发送查询报文检查对方状态，并在预定义的时间段内等待 ACK 响应，若超过 DPD 超时阈值，则认为对方不可达，根据设置的“dpdaction”进行处理。

4 结束语

IPsec VPN 技术目前仍处于一个不断发展和完善的过程。针对现有 VPN 系统对大型网络及远程访问情况下身份认证和访问控制的局限性，本文将公钥基础设施 PKI 引入 IPsec 协议中，对基于 ECC 的密钥交换、数字签名及在 IKE 中设计交叉认证接口进行研究，提高了系统的安全性、可扩展性和完善性；鉴于网络通信过程中可能随时产生的不稳定因素，系统支持 DPD 状态检测机制，有效解决了对方不在线的发现机制并发起重新协商，提高了系统的健壮性和效率。最后提出了一个基于 Linux2.6 内核的 IPsec-VPN 安全网关的基本框架。其中，证书模块中相关部分、路径构造与路径验证的代理服务器等有待进一步完善，以期达到与 IPsec-VPN 安全网关有机结合目的。

参考文献

1 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京: 电子工业出版社, 2002.

2 Zuccherato R. Using A PKI Based Upon Elliptic Curve Cryptography[Z]. http://www.entrust.com, 2003.

3 Korver B. The Internet IP Security PKI Profile of IKE/ISAKMP and PKIX[Z]. draft-ietf-IPsec-pki-profile-04.txt, IETF Internet Draft:pki4 IPsec, 2004.

4 The Internet Key Exchange (IKE)[S]. RFC 2409, 1999.

5 A Traffic-based Method of Detecting Dead Internet Key Exchange (IKE)Peers[S]. RFC 3706, 2004.