一种用于移动 IPv6 的混合认证方法*

陈 炜+, 龙 翔, 高小鹏

(北京航空航天大学 计算机学院,北京 100083)

A Hybrid Authentication Method Used for Mobile IPv6

CHEN Wei+, LONG Xiang, GAO Xiao-Peng

(School of Computer Science, BeiHang University, Beijing 100083, China)

+ Corresponding author: Phn: +86-10-82338059, E-mail: buaa_chen@yahoo.com.cn, http://www.buaa.edu.cn

Received 2004-04-09; Accepted 2004-07-06

Chen W, Long X, Gao XP. A hybrid authentication method used for mobile IPv6. *Journal of Software*, 2005,16(9):1617−1624. DOI: 10.1360/jos161617

Abstract: In the rapidly expanding mobile environment, authenticity of communicating parties is one of the big research challenges and is receiving increasing attention. In the Mobile IPv6 defined by IETF (Internet engineering task force), IPSec (IP security) protocols and RR (return routability) mechanism are used to protect signaling between related communicating nodes, however, how to realize identity authentication has not been efficiently solved. In this paper, the advantages and disadvantages of two authentication techniques—certificate-based authentication and identity-based authentication are analyzed. The scalability of certificate-based means is excellent, but the deployment of PKI (public key infrastructure) and the distribution of certificates make this method costly. On the contrary, identity-based method hurdles the deficiency of certificate-based means, nevertheless the scalability suffers from the share of parameters among related nodes. Then an approach of integrating the two methods mentioned above is proposed to realize a secure and fast authentication with low cost and high scalability. Finally, this hybrid technique is applied in Mobile IPv6 to improve the negotiation of SA (security association), and the security issues are discussed.

Key words: mobile IPv6; IPSec (IP security); CA (certificate authority); PKI (public key infrastructure); identity-based cryptography

摘 要: 随着移动通信的快速发展,通信实体的身份认证日益成为研究人员面临的巨大挑战.在 IETF(Internet engineering task force)的移动IPv6草案中,IPSec(IP security)协议和RR(return routability)机制被用于保护相关通信节点之间的通信信令,但解决通信实体身份认证问题的方法存在一定的不足.首先分析了基于证书和基于身份的认证技术的优点和不足.基于证书的认证方法有很好的可扩展性,但 PKI(public key infrastructure)的部署和证书的分发代价较高.反之,由于相关节点需要共享一组系统参数,基于身份的认证方法可扩展性差,但克服了基于证书的认证方法的不足.然后,提出一种同时使用上述两种认证方法的混合认证方法.该混合认证方法为实现安全、快速、低成本和可扩展性好的身份认证提供了一种新的思路.最后,将这种混合技术用于改进移动 IPv6 安全关联的协商过程,并讨论了该技术的安全性.

* 作者简介: 陈炜(1977－),男,四川自贡人,博士生,主要研究领域为计算机网络安全;龙翔(1963－),男,博士,教授,博士生导师,主要研究领域为计算机体系结构,计算机网络安全;高小鹏(1970－),男,博士,讲师,主要研究领域为计算机体系结构,计算机网络安全.

关键词: 移动 IPv6;IPSec(IP security);CA(certificate authority);PKI(public key infrastructure);基于身份的密码学
中图法分类号: TP393 文献标识码: A

随着移动通信的快速发展和广泛应用,移动环境下的网络安全问题已经成为一个十分重要和复杂的问题.MIPv6(mobile IPv6)[1]是 IETF(Internet engineering task force)提出的解决 IPv6 环境下移动问题的指导性文档.MIPv6 使用 IPSec(IP security)协议保护 MN(mobile node)和 HA(home Agent)之间的通信信令,使用 RR(return routability)机制保护 MN 和 CN(correspondent node)之间的通信信令[1−3].IPSec 协议可以提供访问控制、无连接完整性、数据源认证、拒绝重放包、保密性和限制流量保密性等安全服务[4],但该协议中基于预共享密钥或证书的认证方法有一定的局限性;而 RR 机制则不提供认证服务.

本文首先讨论 MIPv6 相关协议和各种认证方法;然后提出综合运用基于证书的认证方法和基于身份的认证方法,实现通信实体之间的认证.本文第 1 节讨论 MIPv6 相关协议、基于证书的认证方法和 RR 机制.第 2 节分析基于身份的认证方法.第 3 节论述本文提出的混合认证方法.第 4 节对全文进行总结.

1 MIPv6 相关协议

MIPv6 协议使用了 IPSec 协议和 RR 机制保护通信信令[1−3].IPSec 协议基于预共享密钥或证书认证实现通信实体之间的认证;RR 机制通过请求/响应/验证的方式保护通信信令.下面分别简要讨论 MIPv6 的相关协议、IPSec 协议认证方法和 RR 机制.

1.1 MIPv6相关协议概述

在文献[1]中,MIPv6 由 3 个实体组成:CN,HA 和 MN.每个 MN 有一个永久性的 IP 地址 HoA(home of Address).当 MN 移动到一个新的网络后,它将获得一个临时的 IP 地址 CoA(care-of address).MN 获得 CoA 后,通过 BU(binding update)消息,把这个 CoA 通知给 HA;HA 通过 BA(binding acknowledge)消息响应 BU.CN 发送消息给 MN 时,有两种情况:① CN 只知道 MN 的 HoA.CN 把 MN 的 HoA 作为目标地址,把数据包发送给 MN.如果 MN 发生了移动,HA 将根据 MN 注册的 CoA,通过隧道把数据包转发给 MN.MN 发现数据包来自 CN,通过 BU 消息告诉 CN 自己的 CoA,CN 通过 BA 消息进行响应;② CN 知道 MN 的 CoA.CN 把 MN 的 CoA 作为目标地址,直接把数据包发给 MN.MN 向 CN 发送数据包时,是直接把数据包发送给 CN(不经过 HA).

IPSec 协议是 IETF 提出的解决网络安全通信的标准协议,该协议主要由体系结构[5]、封装安全载荷(ESP)[6]、认证头(AH)[7]、加密算法、认证算法、密钥管理和解释域(DOI)这 7 个部分组成[4].IPSec 协议的基本思想是:首先通过密钥管理协议协商用于保护数据包的安全关联(security association,简称 SA),然后使用协商好的 SA 对数据包进行 AH 协议或 ESP 协议封装.IKE 协议是产生和维护 IPSec 安全关联的主要协议[8].SA 是通信实体之间对 IPSec 协议(AH 协议或 ESP 协议)、协议操作模式(传输模式或隧道模式)、密码算法、密钥等安全参数的一种协定.

目前 IKE 有两个版本,IKEv1 和 IKEv2[9].IKEv1 主要由 RFC2407[10],RFC2408[11]和 RFC2409[12]组成[9].IKEv2 对 IKEv1 中的消息数目和消息格式进行了修改,但基本思想不变.IKEv2 的基本思想是首先验证通信双方的身份,然后协商用于保护通信的 SA.为了加快保护数据通信的 SA 的更新过程,IKEv2 将密钥协商的过程分成两个阶段:① 阶段 1 完成通信实体间身份的认证,并建立用于保护阶段 2 协商的 IKE_SA;② 阶段 2 在阶段 1 建立的 IKE_SA 的保护下,协商用于保护通信实体间数据通信的 CHILD_SA.一个在阶段 1 建立的 IKE_SA 可用于保护多个阶段 2 的 CHILD_SA 的协商,从而加快 CHILD_SA 的更新过程.

AH 协议和 ESP 协议通过对数据包进行传输模式或隧道模式封装,实现对数据包的安全处理.AH 协议和 ESP 协议对外出数据包进行 IPSec 协议处理的过程叙述如下:首先根据 IP 包的某些域,查询安全策略数据库(SPD);然后根据 SPD 查询安全关联数据库(SAD);最后根据查到的 SA 对数据包进行认证、加密和封装.AH 协议和 ESP 协议对进入数据包进行 IPSec 协议处理的过程叙述如下:首先根据数据包的某些域,查询 SAD,并根据查到的 SA 对数据包进行认证、解密和解封装;然后根据解封装后得到的 IP 包,查询 SPD,并由此得到相应的 SA;

最后把先前使用的 SA 和查询 SPD 得到的 SA 进行对比,如果相同,则接受该数据包.否则,丢弃该数据包.

1.2 IPSec协议的认证方法

IPSec 协议现有 4 种认证方法:预共享密钥、公钥签名、公钥加密和改进的公钥加密[8].其中基于预共享密钥的认证方法可扩展性差.任何两个通信实体之间都要共享一个密钥的要求不仅导致密钥数量剧增,而且在通信实体之间没有共享密钥时不能实现认证.基于证书的认证方法的局限性如下:① 成本高.基于证书实现安全认证,客观上要求通信实体必须首先公开自己的公钥,然后才能进行认证.这种要求导致了证书目录(public key infrastructure,简称 PKI)的部署.认证中心(certificate authority,简称 CA)不仅要为通信实体签发证书,还要在网络中维护 PKI;② 带宽需求大.通信实体进行认证时,需要传输证书,这将导致网络带宽需求增大;③ 存储空间的需求较大.通信实体需要存储每一个通信伙伴的证书,当通信伙伴很多时,对通信实体存储空间的需求较大.但是证书认证具有很好的可扩展性,通信实体之间不必预先共享任何信息,只要拥有合法的证书,就可以实现安全的相互认证.

1.3 RR机制

在 IETF 的 MIPv6 草案[1,3]中,讨论了 MN 和 CN 之间的绑定更新问题.MN 和 CN 之间的绑定更新采用了无须证书的无认证框架的 RR 机制.RR 机制由 4 条消息组成:HoTI(home test Init),CoTI(care-of test Init),HoT(home test)和 CoT(care-of test).其中 HoTI 和 HoT 构成一对请求/响应,CoTI 和 CoT 构成另一对请求/响应.

RR 机制的工作原理如下:① MN 首先向 CN 发送 HoTI 和 CoTI.HoTI 经由 HA 到达 CN;CoTI 则直接发往 CN;② CN 在收到这两个消息后,根据一个只有 CN 知道的秘密(Kcn),分别产生 home keygen token 和 care-of keygen token;③ CN 在消息 HoT 中,把 home keygen token 经由 HA 发送给 MN;在消息 CoT 中,把 Care-of keygen token 直接发送给 MN;④ MN 在收到 HoT 和 CoT 之后,通过对 home keygen token 和 care-of keygen token 进行运算,产生一个只有 MN 和 CN 知道的秘密(Kbm);⑤ MN 给 CN 发送一个 BU 消息,该消息使用 Kbm 进行认证;⑥ CN 在收到 BU 后,首先计算 Kbm,然后用该 Kbm 对 BU 进行认证.如果认证通过,则接受这个 BU,否则拒绝绑定更新.

通过对文献[3]的研究可知,RR 的安全性基于以下两个假设:① 消息在公共网络中传输,分别在两条路径上传输的两条消息,不会同时被截获(这里指的是 CN 和 HA 之间以及 CN 和 MN 之间的两条路径.文献[3]特别强调,MN 和 HA 之间的消息有 IPSec 协议的保护,因而安全性是有保障的);② 在有线网网络窃取消息的难度比在无线网网络窃取消息的难度要大.仔细研究 RR 机制可以看到,RR 机制实际上并没有提供身份认证服务(只提供了所谓的可达性服务),而且其提供的防止消息伪造的服务也是比较脆弱的.例如,如果攻击者可以在 CN 附近成功地截获 HoT 和 CoT,就可以向 CN 发送伪造的 BU,并成功实现对 CN 的欺骗.由于缺乏全局的信任框架的支持,CN 和 MN 之间无法实现安全的认证,这使得 RR 机制容易受到攻击.

2 基于身份的加密签名算法

2001 年,在 CRYPTO 会议上,Boneh 和 Franklin 提出了基于身份和 bilinear pairings 的加密算法.该算法的最初目标是简化 E-mail 系统中证书的管理[13].不久,基于身份进行认证的方法也提了出来.在基于身份实现加密和认证的系统中,每个通信实体拥有一个〈公钥,私钥〉对:公钥是通信实体的身份,私钥由通信双方都信任的第三方生成,即由 PKG 生成.下面首先简要介绍文献[14]中提出的基于身份的认证算法,然后讨论该算法的优、缺点.

2.1 算法介绍

随机选择素数 q,求出满足下列条件的最小素数 p:① $p>3$;② $p=2 \bmod 3$;③ $q|(p+1)$;④ q^2 不能被$(p+1)$整除.椭圆曲线 $E: y^2=x^3+1$ 定义在有限域 F_p 上;群 G_1 是 E/F_p 上阶为 q 的子群;群 G_2 是 $F_{p^2}^*$ 上阶为 q 的子群;$\hat{e}$ 是 G_1*G_1 到 G_2 的满足下面要求的映射:① Bilinear: $\forall P,Q\in G_1$,以及所有的 $a,b\in F_p$,有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$;② 非退化:若 P 是 G_1 的生成元,则 $\hat{e}(P,P)\in G_2$ 是 G_2 的生成元;③ 可计算性:给定 $P,Q\in G_1$,存在有效算法,计算 $\hat{e}(P,Q)\in G_2$.

基于身份实现认证的签名算法如下:

① Setup:选 G_1 的生成元 P,选随机数 $s \in F_p$,令 $P_{pub} = sP$.定义两个密码学哈希函数: $H_1: \{0,1\}^* * G_1 \to F_p$ 和 $H_2: \{0,1\}^* \to G_1$.该系统的系统参数是 (P, P_{pub}, H_1, H_2),主密钥是 s.

② Extract:给定身份标识符 ID(也就是公钥),计算 $D_{ID} = s H_2(ID)$.D_{ID} 就是 ID 的私钥.定义 $Q_{ID} = H_2(ID)$.

③ Sign:给定准备签名的消息 m,取随机数 $r \in F_p$,计算签名 $\sigma = (U,V)$.其中 $U = r Q_{ID}$, $h = H_1(m,U)$, $V = (r+h) D_{ID}$.

④ Verify:如果 $\hat{e}(P,V) = \hat{e}(P_{pub}, U + hQ_{ID})$,则通过认证.否则,拒绝认证.

2.2 算法讨论

基于身份的认证方法有如下优点:① 通信实体拥有〈公钥,私钥〉两个密钥,且系统中不必部署 PKI.在基于身份的认证方法中,每个通信实体有一个不公开的私钥,消息的发送方用私钥签名,接收方用发送方的身份(即公钥)进行验证.② 网络带宽需求小.基于证书的认证方法要求传送证书,而基于身份的认证方法则不需要这些操作,因而节约了带宽.例如,根据现在计算机的处理能力,使用 1 024 比特~2 048 比特公钥的 RSA 签名算法是安全的[4].这样,为传送证书,基于证书的 RSA 签名算法至少需要 1 024 比特~2 048 比特的带宽,而基于身份的认证方法则不需要这些带宽.③ 通信实体进行认证计算的负担小.通信实体不需要验证 CA 对证书的签名,节约了通信实体的计算能力.④ 存储空间需求小.通信实体不必为每一个通信伙伴存储证书,只需存储 AS 的系统参数就可以了.但是,基于身份的认证方法需要通信双方共享一组系统参数,这在一定程度上限制了该方法的可扩展性.

3 基于混合认证协商 SA

从第 1 节和第 2 节的讨论可知,证书认证可扩展性好,但成本高;身份认证成本低,但需要预先共享一组系统参数.本文提出一种可用于 MIPv6 的混合认证方法.该方法综合了证书认证和身份认证两种认证方法的优点,可以实现安全、快速、低成本和可扩展性好的认证.

身份认证要求通信实体之间共享一组用于认证的参数,从逻辑上看,这等价于要求通信实体处于同一个自治系统(AS)中.因特网是由大量的 AS 组成的,因此,因特网的网络拓扑结构为采用身份认证提供了网络基础.在 MIPv6 中,MN 与 HA 必然属于同一个 AS,从而它们可以共享同一组系统参数.无论 MN 移动与否,MN 与 HA 之间总是可以基于身份认证协商 IKE_SA;然而 CN 与 MN 却可能属于不同的 AS(注意,CN 与 MN 是否属于同一个 AS 不会由于 MN 的移动而改变),从而可能具有不同的系统参数.当 CN 和 MN 具有不同的系统参数时,CN 和 MN 之间不能实现基于身份的认证.为了使 CN 与 MN 可以基于身份认证协商 IKE_SA,必须且只需考虑两种情况:① CN 与 MN 处于同一个 AS 中.这时,通信实体共享同一组系统参数,可以直接基于身份认证协商 IKE_SA;② CN 与 MN 处于不同的 AS 中.这时,两个 AS 必须首先以安全的方式交换系统参数.在交换了系统参数以后,CN 和 MN 就可以基于身份认证协商 IKE_SA 了.以上关于 CN 和 MN 之间协商 SA 的讨论,同样适用于 CN 和 HA 之间 SA 的协商.

本文采用网络访问标识(NAI)作为通信实体的身份标识,NAI 的格式为“user@realm”[15].NAI 作为一个字符串,不会随着 MN 的移动而变化,也就是说,MN 的身份始终保持不变(当然,随着 MN 的移动,MN 的 CoA 可能会发生变化).选择 NAI 作为身份标识的原因如下:在移动通信中,如果以通信实体的 IP 地址作为身份协商安全关联,随着通信实体 IP 地址的改变,不仅难于实现通信实体之间基于身份的认证(因为通信实体的身份可能发生变化),而且正在使用的 SA 也会受到影响.采用 NAI 作为身份标识就可以避免这些问题.

3.1 系统的构造

为了实现混合认证,系统必须具备一些基本组件.这些组件包括:① 可信的 CA.可信的 CA 负责为每个 AS 的 PKG 颁发证书.不同 AS 中的 PKG 之间通过证书实现安全的认证,并在此基础上,实现系统参数的安全交换.② 每个 AS 中有一个该 AS 中所有通信实体都信任的 PKG.该 PKG 不仅负责产生该 AS 中所有通信实体共享的系统参数,还负责为每个通信实体产生私钥.③ IPSec 协议的安全策略数据库使用 NAI 作为选择符.除了上述

组件以外,通信实体必须可以进行基于身份的签名运算.系统网络拓扑关系如图 1 所示.

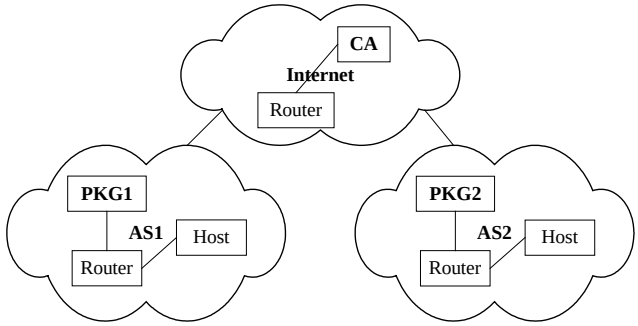

Fig.1 Network topology

图1 网络拓扑图

PKG 必须存储系统参数(为方便起见,本文要求所有通信实体的哈希函数 H_1,H_2 都相同,因此不再把它们作为必须公开的系统参数)和证书公钥.本文采用结构存储相关的参数,见表 1.在表 1 中,公钥用于记录不同 PKG 对应的证书公钥,系统参数用于记录不同 AS 的系统参数,身份标识用于识别 PKG 和自治系统,有效期指出公钥或系统参数的有效期.通信实体也有一个类似的表结构,只是没有公钥这一项.

Table 1 Data structure of PKG

表 **1** PKG 的数据结构

Public keys	System parameters	Identitys	Life time
–	–	–	–
Key_{pub}	–	$Identity_i$	$TIME_j$
–	P, P_{pub}	$Identity_j$	$TIME_i$
–	–	–	–

3.2 AS间系统参数的交换

本文中,通信实体之间基于身份认证协商 SA(不是基于证书认证),因此,在基于身份进行认证之前,需要判断是否需要进行 AS 间系统参数的交换.事实上,通信实体通过比较 NAI 的 realm 域,就可以知道自己和通信伙伴是否处于同一个 AS,从而决定是否需要进行 AS 间系统参数的交换.如果通信实体和通信伙伴处于同一个 AS,直接进行基于身份的认证;如果处于不同的 AS,首先进行 AS 间系统参数的交换,然后进行基于身份的认证.

通信实体之间交换 AS 系统参数的消息必须满足下列条件:① 确保消息的真实性和完整性;② 确保消息的及时性;③ 防止消息的重放.本文使用一次性随机数(nonce)来实现消息的及时性和防止消息的重放.nonce 是消息发送方选择的临时交互号,这个临时交互号必须是随机的和不可伪造的(只有发送方可以生成),且应该与当前时间有关.采用 nonce 验证的原因如下:① 避免 PKG 受到拒绝服务(DoS)攻击,频繁发起 AS 间系统参数的交换;② 防止 Client 频繁处理不需要的其他 AS 的系统参数.本文提出的 AS 之间交换系统参数的过程由如图 2 所示的 8 条消息组成.消息中的"||"表示载荷的链接.

(1) Client → PKG1: ID_{Client} || $NONCE_{Client}$ || REQUEST || $SIGN_{Client}$;

ID_{Client}=NAI || TIME || PROPERTY.

Client 向 PKG1 请求 PKG2 的系统参数.ID_{Client} 是 Client 的身份载荷,由 NAI(身份标识)、TIME(有效期)、PROPERTY(属性)这 3 个域组成.有关身份载荷的说明,在第 3.4 节有进一步的讨论.$NONCE_{Client}$ 是 nonce 载荷.REQUEST 是请求 PKG2 系统参数的载荷.$SIGN_{Client}$ 是签名载荷,Client 用自己的私钥对消息进行签名(基于身份认证),签名用于确保请求的真实性和完整性.

(2) PKG1 → Client: ID_{PKG1} || $NONCE_{Client}$ || $NONCE_{PKG1}$ || REQUEST || $SIGN_{PKG1}$.

PKG1 向 Client 发送验证请求.REQUEST 是 Client 发送的请求 PKG2 系统参数的载荷.$SIGN_{PKG1}$ 是 PKG1 对消息的签名(基于身份认证).

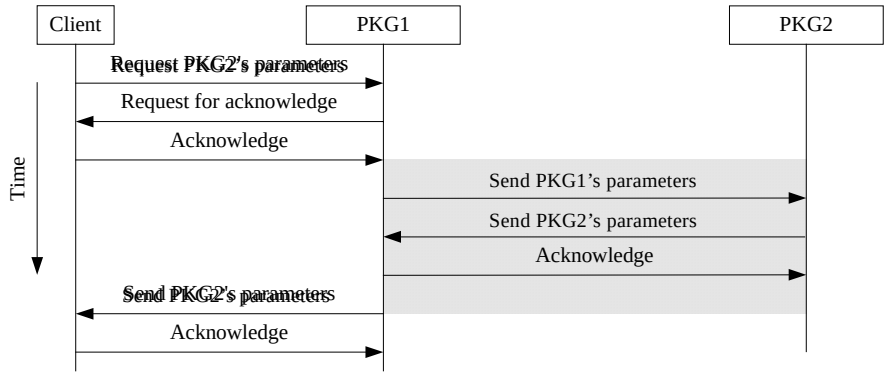

Fig.2 Exchange of system parameters between AS

图 2 AS 间交换系统参数

(3) Client → PKG1: $ID_{Client} || NONCE_{PKG1} || NONCE_{Client} || REQUEST || SIGN_{Client}$.

Client 回应 PKG1 的验证请求,请求 PKG1 提供 PKG2 的参数.SIGNclient 是 Client 对消息的签名(基于身份认证).此时,$NONCE_{Client}$ 载荷中的 nonce 是新的 nonce,该 nonce 和第 1 条消息中 $NONCE_{Client}$ 载荷中的 nonce 不同.

(4) PKG1 → PKG2: $ID_{PKG1} || NONCE_{PKG1} || PARAM_{PKG1} || REQUEST || CERT_{PKG1} || SIGN_{PKG1}$;

$PARAM_{PKG1}=P || P_{Pub} || TIME$.

PKG1 如果没有 PKG2 的系统参数,就发起与 PKG2 交换参数的过程.否则,直接跳至第 7 条消息(即图 2 中有阴影的 3 条消息不是每次都执行).$PARAM_{PKG1}$ 是 PKG1 的系统参数,由 P,P_{pub},TIME(PKG1 的系统参数的有效期)这 3 个域组成.PKG1 主动向 PKG2 发送自己的系统参数,可以避免 PKG2 在向 PKG1 发送 PKG2 的系统参数后,又向 PKG1 请求 PKG1 的系统参数.REQUEST 是 PKG1 发送的请求 PKG2 系统参数的载荷.$CERT_{PKG1}$ 是 PKG1 的证书;$SIGN_{PKG1}$ 是 PKG1 对消息的签名(基于证书认证).此时,$NONCE_{PKG1}$ 载荷中的 nonce 是新的 nonce,该 nonce 与第 2 条消息中 $NONCE_{PKG1}$ 载荷中的 nonce 不同.

(5) PKG2 → PKG1: $ID_{PKG2} || NONCE_{PKG1} || NONCE_{PKG2} || PARAM_{PKG2} || CERT_{PKG2} || SIGN_{PKG2}$;

$PARAM_{PKG2}=P || P_{Pub} || TIME$.

PKG2 向 PKG1 提供自己的参数.$SIGN_{PKG2}$ 是 PKG2 对消息的签名(基于证书认证).

(6) PKG1 → PKG2: $ID_{PKG1} || NONCE_{PKG2} || SIGN_{PKG1}$.

PKG1 通知 PKG2 已经收到了 PKG2 的参数.$SIGN_{PKG1}$ 是 PKG1 对消息的签名(基于证书认证).

(7) PKG1 → Client: $ID_{PKG1} || NONCE_{Client} || NONCE_{PKG1} || PARAM_{PKG2} || SING_{PKG1}$.

PKG1 把 PKG2 的系统参数提供给 Client.$SIGN_{PKG1}$ 是 PKG1 对消息的签名(基于身份认证).此时 $NONCE_{PKG1}$ 载荷中的 nonce 是新的 nonce,该 nonce 与第 2 条消息(或第 4 条消息)的 $NONCE_{PKG1}$ 载荷中的 nonce 不同.

(8) Client → PKG1: $ID_{client} || NONCE_{PKG1} || SIGN_{client}$.

Client 通知 PKG1 已经收到了 PKG2 的参数.$SIGN_{client}$ 是 Client 对消息的签名(基于身份认证).

3.3 通信实体之间安全关联的协商

本文提出基于身份认证改进 IKEv2 协议.基于身份认证实现 IKEv2 协议,在协商过程中不必传送证书,节约了网络带宽(当然,如果通信双方处于不同的 AS,可能需要进行 AS 系统参数的交换);通信实体只需存储 AS 的系统参数,而不必为每个通信伙伴存储证书,节约了存储空间;不必部署 PKI,节约了成本.

通信实体之间协商 SA 的过程由如图 3 所示的 4 条消息组成.图 3 中 I 代表消息的发送方,R 代表消息的接收方.因为通信实体之间基于身份进行认证,所以本文去除了 IKEv2 标准消息中的证书载荷和证书请求载荷.消息中的 ID 载荷采用第 3.2 节中的身份载荷格式.

(1) I → R: HDR || SAi1 || KEi || Ni.

这条消息是 IKEv2 的标准消息.HDR 包含 SPI(安全参数索引)、版本号等信息,SAi1 声明发起者支持的 IKE_SA 加密算法,KE 载荷发送 Diffie-Hellman 值,Ni 载荷是发起者的 nonce.

(2) R → I: HDR || SAr1 || KEr || Nr.

原来的消息是:HDR || SAr1 || KEr || Nr || [CERTREQ].

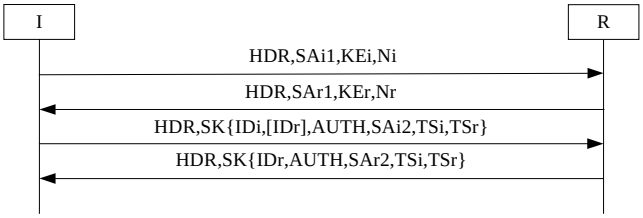

Fig.3 Negotiation of SA between nodes

图 3 节点间安全关联的协商

(3) I → R: HDR || SK{IDi || [IDr] || AUTH || SAi2 || TSi || TSr}.

原来的消息是:HDR || SK{IDi || [CERT] || [CERTREQ] || [IDr] || AUTH || SAi2 || TSi || TSr}.

ID 载荷是身份载荷.TS 载荷是流量选择载荷,用于选择安全策略.AUTH 是认证载荷,用于确保消息的真实性和完整性.SK 表示用通信双方共享的密钥加密载荷.注意,消息接收方根据通信伙伴 ID 载荷中的身份标识(NAI)域,可能需要首先发起一个第 3.2 节所描述的交换 AS 系统参数的过程,然后再继续进行通信实体间安全关联的协商.

(4) R → I: HDR || SK{IDr || AUTH || SAr2 || TSi || TSr}.

原来的消息是 HDR || SK{IDr || CERT || AUTH || SAr2 || TSi || TSr}.

上述 4 条消息完成以后,通信实体之间就有了 IKE_SA 和 CHILD_SA.随后 CREATE_CHILD_SA 的过程和 INFORMATIONAL 的过程都是标准的 IKEv2 过程,这里就不再讨论了.

3.4 密钥的更新

通过研究文献[13,14]可以知道,基于身份的认证方法,其核心是:私钥由 PKG 根据通信实体提交的公钥产生,而公钥是一个任意的字符串.本文采用“NAI || Time || Property”形式的字符串作为通信实体的公钥[13],用一个身份载荷来承载.其中的“||”代表字符串的链接.公钥由身份标识(NAI)、有效期(Time,如某年,某月)和通信实体的属性(Property,如拥有公钥的部门)这 3 个域组成.

公钥中 3 个域的作用叙述如下:通信伙伴根据身份标识域判断通信的双方是否同处一个 AS;有效期域和属性域有两个作用:① 消息接收方根据这两个域判断该公钥的有效性.如是否过期、消息发送方是否可以使用这个公钥等;② PKG 根据公钥的这两个域,限定相应私钥的有效期和使用范围.也就是说,PKG 在严格审查公钥的申请后,才签发相应的私钥,从而使得签名者不能在有效期和有效范围之外使用该私钥,也即实现了密钥的撤销.通信实体的〈公钥,私钥〉过期后,需要向 PKG 申请新的〈公钥,私钥〉对.

为了更加有效地实现密钥的更新,PKG 可以仿照 CRL(certificate revocation list),在自己的机器上建立一个〈公钥,私钥〉撤销列表,以便及时发布因为意外原因导致的必须撤销的未过期的〈公钥,私钥〉对.

3.5 安全性分析

本文提出的混合认证方法的安全性来自 4 个方面:① 通信实体之间基于身份实现认证.该认证算法具有良好的安全性,可以有效防止安全攻击[13,14].② AS 间系统参数的交换.本文利用了证书体制所提供的安全性,可以有效地保证消息的完整性和真实性.通过使用 nonce,可以有效地实现消息的及时性和防止消息的重放;③ 通信实体之间 SA 的建立.基于 IKEv2 协商 SA,可以有效地确保消息的真实性、完整性和保密性,防止重放、拒绝服务等攻击.④ PKG 作为可信任的第三方,作用和 CA 相同.因此,虽然 PKG 知道通信实体的私钥,也不会降低系统的安全性.

3.6 结 论

基于混合认证协商 IPSec 安全关联有以下特点:① 可扩展性好.通过证书认证,不同的 AS 之间可以安全实现系统参数的交换.② 安全有保障.通信实体之间基于身份实现认证的认证方法有良好的安全性.③ 只需要部署少量的基于证书的 PKI.证书认证仅限于 AS 之间,而不是单个的通信节点之间,可以极大地减轻部署 CA 和 PKI 的工作量.④ 可操作性强.通信节点在自己的 AS 中,向 PKG(由 AS 的网管管理)提供自己的公钥,并从 PKG 获得自己的私钥.显然,这种注册方式在组织或企业中是可行的.对于无组织的通信节点,必须首先在 CA 处注册,以获得合法的证书并形成一个 AS,然后就可以基于身份认证实现认证了.⑤ 网络带宽占用小.AS 之间系统参数的一次交换,可以供多对通信实体多次使用.⑥ 存储空间占用少.通信实体只需存储不同 AS 的系统参数,而不必为相同 AS 中的每一个通信伙伴存储系统参数,节约了存储空间.⑦ 某个 AS 内部系统参数的更新不必通知 CA,增强了认证系统的灵活性.⑧ 解决了 MIPv6 中 CN 和 MN 的认证问题,从而可以有效地避免 RR 机制存在的不足.当然,这种混合认证方法必须要有少量 CA,PKI 和 PKG 的支持,而这些设施是 RR 机制所不需要的.

4 结束语

当前有两种主要的认证方法:基于证书实现认证和基于身份实现认证.本文总结了这两种认证方法的优缺点,指出单纯使用一种方法实现通信实体的认证都存在一定的局限性.本文在深入研究移动 IPv6 草案的基础上,将基于身份的认证方法引入 IPSec 的密钥协商过程,提出一种同时使用这两种认证方法的混合认证方法,并详细讨论了该混合认证方法的技术细节和安全性.该混合认证方法为实现安全、快速、低成本和可扩展性好的身份认证,提供了一种可操作性强的新思路.

References:

[1] Johnson D, Perkins C, Arkko J. Mobility support in IPv6. draft-ietf-mobileip-ipv6-24.txt, 2003.

[2] Arkko J, Devarapalli V, Dupont F. Using IPSec to protect mobile IPv6 signaling between mobile nodes and home Agents. draft-ietf-mobileip-mipv6-ha-IPSec-06.txt, 2003.

[3] Nikander P, Aura T, Arkko J, Montenegro G. Mobile IP version 6 route optimization security design background. draft-nikander-mobileip-v6-ro-sec-00, 2003.

[4] Stallings W. Cryptography and Network Security: Principles And Practice. 3rd ed., Upper Saddle River: Prentice Hall, 2003.

[5] Kent S, Atkinson R. Security architecture for the Internet protocol. RFC2401, 1998.

[6] Kent S, Atkinson R. IP encapsulating security payload (ESP). RFC2406, 1998.

[7] Kent S, Atkinson R. IP authentication header. RFC2402, 1998.

[8] Cheng PC. An architecture for the Internet key exchange protocol. IBM Systems Journal, 2001,40(3):721−746.

[9] Kaufman C. Internet key exchange (IKEv2) protocol. draft-ietf-IPSec-ikev2-11.txt, 2003.

[10] Piper D. The Internet IP security domain of interpretation for ISAKMP. RFC2407, 1998.

[11] Maughan D, Schertler M, Schneider M, Turner J. Internet security association and key management protocol (ISAKMP). RFC2408, 1998.

[12] Harkins D, Carrel D. The Internet key exchange (IKE). RFC2409, 1998.

[13] Boneh D, Franklin M. Identity based encryption from the Weil pairing. In: Proc. of the Crypto 2001. LNCS 2139, Springer-Verlag, 2001. 213−229. http://crypto.stanford.edu/~dabo/pubs.html

[14] Cha J, Cheon J. An identity-based signature from gap Diffie-Hellman groups. In: Proc. of the PKC 2003. LNCS 2567. 2003. 18−30. http://www.math.snu.ac.kr/~jhcheon/publication.html

[15] Aboba B, Beadles M. The network access identifier. RFC2486, 1999.