基于证书签密的 IPv6 网络跨域认证协议*

张龙军[a]，夏　昂[a]，莫天庆[a]，赵李懿[b]
（武警工程大学 a. 信息工程系；b. 电子技术系 网络与信息安全武警部队重点实验室，西安 710086）

摘　要：为了解决 IPv6 网络互连过程中基于身份认证的域内用户与基于无证书认证的域内用户之间进行跨域认证和密钥协商的问题，提出了一种随机预言机模型下可证明安全的基于证书签密的认证方案，设计了一种 IPv6 网络跨域认证协议并对其安全性和效率进行了分析。结果表明，在安全性方面，该协议具有完美向前保密和双向实体认证等安全属性，满足了认证的安全需求；在效率方面，与同类协议相比，该协议无须进行公钥加/解密运算，也不受同步环境的限制，只需五条消息就能实现跨域认证，计算开销和通信开销都相对较小。

关键词：IPv6 网络；证书签密；认证；随机预言机模型
中图分类号：TP393　　**文献标志码**：A　　**文章编号**：1001-3695(2012)10-3800-05
doi:10.3969/j.issn.1001-3695.2012.10.051

Authentication protocol based on signcryption for multi-domain in IPv6 network

ZHANG Long-jun[a], XIA Ang[a], MO Tian-qing[a], ZHAO Li-yi[b]
(*a. Dept. of Information Engineering, b. Key Laboratory of Network & Information Security of CAPF, Dept. of Electrical Technology, Engineering University of CAPF, Xi'an* 710086, *China*)

Abstract: The proposed authentication scheme in proxy mobile IPv6 network has the flaw of system requirement and cannot resist the dictionary attack. To solve these problems, this paper proposed an authentication scheme based on certificateless signcryption in proxy mobile IPv6 network. The proposed scheme could not only realize mutual authentication between the endpoints but also simplify the key management in wireless mobile environment. Performance analysis results show that the proposed mechanism is very efficient. Finally, it proved the new scheme's security in the random oracle model.
Key words: IPv6 network; certificate-based signcryption; authentication; random oracle model

0　引言

随着网络规模的不断扩大，越来越多的企业、机构拥有属于自己的资源。为了保护这些资源免受非授权用户的访问，各机构会设置本地认证服务设备来提供认证服务，这样就形成了相对独立的自治域（autonomous system，AS）。从逻辑上看，IPv6 网络由很多支持 IPv6 技术的自治域组成。在这种环境中，共享资源的访问请求不仅来自本地信任域，也有可能来自外地信任域。因此当外地信任域的用户主体访问本地信任域的资源时就存在跨域认证问题。现实环境中存在许多类似的应用场景，如移动 IPv6 网络中，通信对端（correspondent node，CN）和移动节点（mobile node，MN）就有可能不在同一个信任域内。当位于不同信任域的 CN 要与 MN 通信时，为了保证安全就必须先进行跨域认证。

对跨域认证方面的研究主要有：文献[1]设计了一种基于真实 IPv6 地址的跨域身份认证方案。文献[2～4]对跨域基于口令认证的密钥交换协议的安全模型进行了研究，提出了一些针对性较强的安全模型。文献[5]提出了一种基于身份的多信任域认证模型，该模型避免了基于传统 PKI 认证框架的诸多弊端，实现了跨信任域的身份认证和资源访问主体的匿名性；但是该模型存在系统开销过大的缺点。文献[6]以基于身份的 PKI 为基础，设计了一个基于身份的多信任域网格认证模型。其主要思想是在不同信任域间采用基于身份签密的认证协议来实现认证和密钥交换。文献[7]针对可信计算平台的原始直接匿名证明方案在多信任域的环境下存在的不足，提出了一种多信任域内的直接匿名证明方案。该方案扩展了原始的直接匿名证明方案，利用基于离散对数的零知识证明协议解决了可信计算平台在多信任域内的隐私性保护问题。文献[8]针对采用不同认证方式的网络进行互连时，处于不同网络中采用不同认证方式的用户间的相互认证问题，提出了一种通用的多信任域认证协议，然后引入时间戳对其进行了改进。虽然改进的协议在安全性和系统开销方面都有一定的优势，但是该协议只适用于同步通信网络。文献[9]提出了一种基于信任链的跨域认证协议。文献[10]提出了一种结合信任机制的移动 IPv6 网络快速跨域认证方法，减少了总切换延时和系统开销。

通过分析可知，文献[1～10]提出的跨域认证方案主要针对以下四种网络环境：a）网络中所有用户都采用基于证书的认证方式；b）网络中所有用户都采用基于身份的认证方式；c）网络中每个子网内的用户采用基于身份的认证方式，不同子网

收稿日期：2012-03-19；**修回日期**：2012-04-30　　**基金项目**：国家自然科学基金资助项目（60842006）；武警工程大学基础基金研究资助项目（wjy201111）

作者简介：张龙军（1964-），男，教授，博士（后），主要研究方向为信息与网络安全（longjun-zhang@sohu.com）；夏昂（1989-），男，硕士研究生，主要研究方向为信息与网络安全；莫天庆（1986-），女，硕士，主要研究方向为信息与网络安全；赵李懿（1986-），男，硕士，主要研究方向为信息安全.

间的用户采用基于证书的认证方式;d)网络中基于证书认证的域内用户与基于身份认证的域内用户之间采用基于证书的认证方式。随着计算机技术和网络技术的不断发展,IPv6 网络中出现了基于无证书的认证方式[11]。因此,基于身份认证的域内用户与基于无证书认证的域内用户之间如何进行认证和密钥协商成为了一个新问题。

1　基本知识

1.1　基于证书的签密

一个基于证书的签密方案由系统建立、密钥生成、证书生成、签密以及解签密五个算法组成,其具体细节参见文献[12]定义 3.3.1。

同样,本文也考虑基于证书签密方案的机密性和不可伪造性,即在适应性选择密文攻击下具有不可区分性和在适应性选择消息攻击下能抗存在性伪造。

1.2　IPv6 网络跨域认证模型

为了解决基于身份认证的域内用户和基于无证书认证的域内用户之间如何进行跨域认证与密钥协商的问题。结合 IPv6 网络环境和签密技术,建立了一种基于签密的跨域认证模型,其系统结构如图 1 所示。该模型由基于无证书认证的域 A 和基于身份认证的域 B 组成。该模型没有对具体的域内认证方式加以限制,为了描述方便,假设域 A 采用无证书签密的认证方式实现具体的域内认证,域 B 采用基于身份签密的认证方式实现具体的域内认证,且域 A 中的用户没有进行基于身份运算的能力,域 B 中的用户也没有基于无证书相关运算的能力。为了实现跨域认证,系统必须具备一些基本组件,这些组件包括:

a)可信的认证中心(certificate authority,CA)。可信的 CA 负责为每个信任域 AS 颁发证书,使得采用不同认证方式的 AS 之间通过 CA 颁发的证书来实现域间的安全认证。

b)基于无证书签密的域 A 和基于身份签密的域 B。域 A、B 分别由 KGC 和 PKG 作为域内的可信第三方,其中 KGC 和 PKG 都包含一个认证服务模块(authentication sevice module,ASM)来负责管理域间的认证服务。

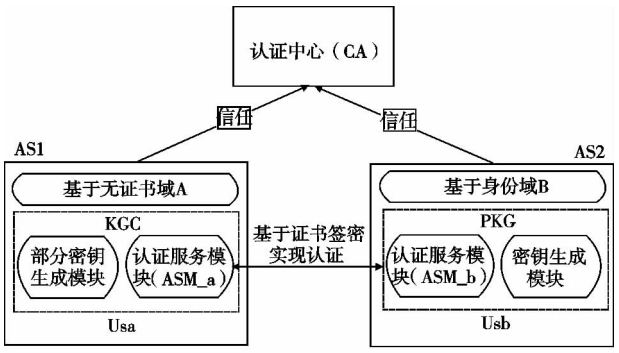

图1　IPv6网络基于签密的跨域认证模型

2　基于签密的 IPv6 跨域认证协议

2.1　一种基于证书的签密方案

本节在 Boneh 等人[13]签名的基础上提出了一种基于证书的签密方案。在本方案中,CA 利用 IBE 方案生成证书,减少了计算量和通信成本。其具体细节如下:

设 G_1 为由 P 生成的循环加法群,其阶为 q,G_2 为具有相同阶 q 的循环乘法群,且在 G_1、G_2 中离散对数问题都是难解的。E、D 为安全的对称密码算法,$\hat{e}: G_1 \times G_1 \rightarrow G_2$ 为双线性映射。定义三个安全的 hash 函数,$H_1: \{0,1\}^n \times \{0,1\}^\lambda \rightarrow G_1$,$H_2: G_1^2 \rightarrow \{0,1\}^\lambda$,$H_3: \{0,1\}^n \times G_1 \rightarrow G_1$(其中 n 表示用户身份的长度,λ 表示密钥的长度)。CA 选择一个随机数 $s \in Z_q^*$ 作为系统主密钥,计算系统公钥 $P_{pub} = s \cdot P$,公开系统参数 $\{G_1, G_2, q, \hat{e}, P, P_{pub}, H_1, H_2, H_3, E, D\}$。

1)用户密钥生成　用户 U 随机选择 $x_U \in Z_q^*$ 作为私钥,计算相应的公钥 $y_U = x_U \cdot P$。假定 $U = i$ 和 $U = j$ 分别表示发送者和接收者,它们的私/公钥对分别为 (x_i, y_i),(x_j, y_j)。

2)证书生成　输入系统参数、CA 的主密钥 s、用户的身份标志 ID_u 及其公钥 y_u,计算 $Q_u = H_3(ID_u \| y_u)$,然后输出用户的证书 $Cert_u = s \cdot Q_u$。用户 i 的证书 $Cert_i = s \cdot Q_i$,用户 j 的证书 $Cert_j = s \cdot Q_j$。

3)签密　为了发送一个消息 m 给接收者 j,发送者 i 执行以下步骤:

a)随机选取 $k \in \{0,1\}^\lambda$,计算 $h_1 = H_1(m,k)$,$c = E_k(m \| y_j)$;

b)计算 $Y = \dfrac{1}{(h_1 + Cert_i \cdot Q_j)}$,$S = Y \cdot y_i$,$V = Y \cdot x_i \cdot y_j$;

c)计算 $h_2 = H_2(S,V)$,$U = k \oplus h_2$;

d)将签密密文 (U,c,S) 发送给接收方。

4)解签密　当接收者收到 (U,c,S) 时,执行以下步骤:

a)计算 $h_2 = H_2(S, S \cdot x_j)$,$k = U \oplus h_2$;

b)计算 $m \| y_j = D_k(c)$,$h_1 = H_1(m,k)$;

c)计算 $Y = \dfrac{1}{(h_1 + Cert_j \cdot Q_i)}$;

d)验证等式 $\hat{e}(P,S) = \hat{e}(P, y_i)^Y$ 是否成立,若成立,则接收发送者的消息 m;否则,输出 $\perp$。

5)正确性证明　(本方案的正确性取决于以下三个等式的正确性)

a)$S \cdot x_j = V$

证明:$S \cdot x_j = Y \cdot y_i \cdot x_j =$

$Y \cdot x_i \cdot x_j \cdot P =$

$Y \cdot x_i \cdot y_j = V$

b)$Cert_i \cdot Q_j = Cert_j \cdot Q_i$

证明:$Cert_i \cdot Q_j = s \cdot Q_i \cdot Q_j =$

$Q_i \cdot s \cdot Q_j = Q_i \cdot Cert_j$

c)$\hat{e}(P,S) = \hat{e}(P, y_i)^Y$

证明:$\hat{e}(P,S) = \hat{e}(P, Y \cdot y_i) = \hat{e}(P, y_i)^Y$

2.2　方案的安全性证明

1)机密性

假设任意一多项式时间攻击者 $A_{\eta(\eta=1,2)}$ 获取了第 μ 次会话产生的密文 $c_\mu = E_{k_\mu}(m_\mu \| y_j)$,其中 $k_\mu = U \oplus h_2$,$h_2 = H_2(S, x_i \cdot y_j \cdot Y)$。对于攻击者 $A_{\eta(\eta=1,2)}$ 来说,获得该次会话的明文在计算上是不可行的,因为计算 h_2 面临解决一个 CDH 问题。因此,本章提出的方案在适应性选择密文攻击下具有不可区分

性。通常,A_2 较 A_1 在计算明文 m_μ 上更有优势[12],因此只需证明本方案在敌手 A_2 进行适应性选择密文攻击下具有不可区分性。

定理 1 在随机预言机模型下,若存在一个敌手 A_2 能在时间 t 内以 ε 的优势赢得文献[12]3.3.1 节中定义的 Game IND-CBSC-CCA2-II(在游戏中敌手 A_2 最多能进行 q_{H_τ} 次 H_τ 询问($\tau=1,2,3$),q_k 次公钥提取询问,q_s 次私钥提取询问,q_{sc} 次签密询问,q_{usc} 次解/签密询问),则存在一个算法 C 能在 $t'<t+(4q_{sc}+2q_{usc})\cdot t_{sm}+2q_{usc}\cdot t_e$ 内以 $\varepsilon'\geqslant\dfrac{\varepsilon}{(1-\frac{2}{q_s})q_{H_2}q_{usc}}$ 的优势解决 CDH 问题,其中 t_{sm} 表示点乘运算所需的时间,t_e 表示双线性对运算所需的时间。

证明 C 接收一个随机的 CDH 实例,已知 P、aP、bP、C 的目标是输出 CDH 问题的一个解 abP。C 把 A_2 作为子程序并扮演文献[12]中 3.3.1 节中定义的 Game IND-CBSC-CCA2-II 中 A_2 的挑战者。游戏一开始,C 将系统参数$\{G_1,G_2,q,\hat{e},P,P_{\text{pub}},H_1,H_2,E,D\}$和主密钥 s 一起发送给 A_2。C 维护着 L_1、L_2、L_3、L_k、L_s、L_{sc}、L_{usc}七张列表。其中,表 L_1、L_2、L_3 分别用于跟踪 A_2 对预言机 H_1、H_2、H_3 的询问,表 L_k、L_s、L_{sc}和 L_{usc}分别用于对公钥生成预言机、私钥生成预言机、签密预言机和解/签密预言机的模拟。这些表一开始为空,在游戏中建立。

第一阶段,敌手 A_2 可以执行下列多项式有界的适应性询问。

a)公钥提取询问。C 首先从$\{1,\cdots,q_k\}$中随机选取两个数$\{i_a,i_b\}$,假设 A_2 不作重复询问。对于 A_2 的第 i_a 次公钥提取询问,C 令 $y_u=P_1$(其中 $P_1=aP$,$a\in Z_q^*$,C 不知道具体的私钥 a),$x_u=\perp$,$\text{ID}_a=\text{ID}_{i_a}$。对于 A_2 的第 i_b 次公钥提取询问,C 令 $y_u=P_2$(其中 $P_2=bP$,$b\in Z_q^*$,C 不知道具体的私钥 b),$x_u=\perp$,$\text{ID}_b=\text{ID}_{i_b}$。对于其他询问,$C$ 选择 $x_u\in Z_q^*$,计算 $y_u=x_u\cdot P$,将(ID_u,y_u)写入表 L_k,(ID_u,x_u)写入表 L_s,并将 y_u 返回给 A_2。

b)私钥提取询问。假设 A_2 在对 ID_u 执行私钥提取询问前已经对其执行过公钥提取询问了。如果 $\text{ID}_u=\text{ID}_a$ 或 $\text{ID}_u=\text{ID}_b$ 则终止模拟,否则在表 L_s 中取出 ID_u 对应的项,返回相应的私钥 x_u 给 A_2。

c)H_3 询问。假设 A_2 在对 ID_u 执行 H_3 询问前已经对其执行过公钥提取询问了。当 A_2 询问$\langle\text{ID}_u,y_u,(Q_u)\rangle$时,$C$ 随机选取 $w\in Z_q^*$,计算 $Q_u=w\cdot P$,将$\langle\text{ID}_u,y_u,(Q_u)\rangle$写入表 L_3 并将 Q_u 返回给 A_2。

d)H_2 询问。C 首先检查表 L_2 中是否有$\langle S,(h_2)\rangle$存在,如果存在,则返回 h_2 给 A_2;否则,随机选择 $h_2\in\{0,1\}^\lambda$,将$\langle S,(h_2)\rangle$写入表 L_2,并将 h_2 返回给 A_2。

e)H_1 询问。C 首先检查表 L_1 中是否有(m,k_i,h_1)存在,如果存在,则返回 h_1 给 A_2;否则,随机选择 $h_1\in G_1$,将(m,k_i,h_1)写入表 L_1,并将 h_1 返回给 A_2。

f)签密询问。敌手 A_2 对明文 m、身份 ID_1 和 ID_2 执行签密询问之前已经对 ID_1 和 ID_2 执行过公钥提取询问和私钥提取询问了。在这里,可以分三种情况讨论:

(a)如果 $\text{ID}_1\notin\{\text{ID}_a,\text{ID}_b\}$,$C$ 可以通过公钥提取询问获得 ID_1 和 ID_2 的公钥$\{y_1,y_2\}$,通过 H_3 询问获得$\{Q_1,Q_2\}$,通过私钥提取询问获得 ID_1 的私钥 x_1。计算 $\text{Cert}_1=s\cdot Q_1$,利用 2.1 节的签密算法计算签密密文 $\sigma=\text{signcrypt}(m,\text{Cert}_1,s_1,\text{ID}_2)$,并将 σ 返回给 A_2。

(b)如果 $\text{ID}_1\in\{\text{ID}_a,\text{ID}_b\}$ 且 $\text{ID}_2\notin\{\text{ID}_a,\text{ID}_b\}$,$C$ 可以通过公钥提取询问获得 ID_1 的公钥 y_1,ID_2 的公钥 y_2,通过私钥提取询问获得 ID_2 的私钥 x_2,通过 H_3 询问获得$\{Q_1,Q_2\}$。然后执行以下操作:

ⓐ选择随机数 $k\in\{0,1\}^\lambda$,计算 $h_1=H_1(m,k)$,$c=E_k(m\parallel y_2)$;

ⓑ计算 $Y=1/(h_1+\text{Cert}_1\cdot Q_2)$,$S=Y\cdot y_1$;

ⓒ计算 $h_2=H_2(S,S\cdot x_2)$,$U=k\oplus h_2$;

最后 C 返回签密密文 $\sigma=(U,c,S)$给 A_2。

(c)如果 $\text{ID}_1=\text{ID}_a$,$\text{ID}_2=\text{ID}_b$(或 $\text{ID}_1=\text{ID}_b$,$\text{ID}_2=\text{ID}_a$),C 随机选择 $k'\in\{0,1\}^\lambda$,$h_2\in\{0,1\}^\lambda$,计算 $h'_1=H_1(m,k')$,$c'=E_{k'}(m\parallel y_2)$,$Y'=1/(h'_1+\text{Cert}_1\cdot Q_2)$,$S'=Y'\cdot y_1$,$U'=k'\oplus h'_2$。最后 C 返回签密密文 $\sigma'=(U',c',S')$给 A_2。

g)解签密询问。敌手 A_2 对密文 σ、身份 ID_1 和 ID_2 执行解/签密询问之前已经对 ID_1 和 ID_2 执行过公钥提取询问和私钥提取询问了。在这里,可以分两种情况讨论:

(a)如果 $\text{ID}_2\notin\{\text{ID}_a,\text{ID}_b\}$,则可以通过私钥提取询问获得 ID_2 的私钥 x_2。因此,C 可以根据 2.1 节的解/签密算法计算解/签密结果,并将该结果返回给 A_2。

(b)如果 $\text{ID}_2\in\{\text{ID}_a,\text{ID}_b\}$,$C$ 按以下步骤遍历表 L_2 中的项$\langle S,(h_2)\rangle$:

ⓐ如果 $\text{ID}_1\in\{\text{ID}_a,\text{ID}_b\}$,则移动到 L_2 的下一项并重新开始,否则从表 L_2 中取出 h_2 并计算 $k=U\oplus h_2$,$m\parallel y_2=D_k(c)$,$h_1=H_1(m,k)$;

ⓑ如果 $\text{ID}_1\in L_k$,则取出相应的 y_1,否则移动到 L_2 的下一项并重新开始;

ⓒ如果 $\text{ID}_1\in L_3$,则取出相应的 Q_1,计算 $Y=1/(h_1+\text{Cert}_2\cdot Q_1)$,否则移动到 L_2 的下一项并重新开始;

ⓓ验证等式 $\hat{e}(P,S)=\hat{e}(P,y_1)^Y$ 是否成立,若成立则返回消息 m,否则移动到 L_2 的下一项并重新开始;

ⓔ如果遍历完表 L_2 中的所有项后都没有消息输出,则返回 $\perp$(表示该密文不正确)。

第一阶段询问结束后 A_2 输出两个希望挑战的身份$\{\text{ID}_A,\text{ID}_B\}$和两个等长的消息$\{m_0,m_1\}$。如果$\{\text{ID}_A,\text{ID}_B\}\notin\{\text{ID}_a,\text{ID}_b\}$,$C$ 终止模拟;否则随机选择 $\theta\in\{0,1\}$,$k\in\{0,1\}^\lambda$,$V\in G_1$,计算 $h_1=H_1(m,k)$,$c=E_k(m\parallel y_B)$,$S=Y\cdot y_A$(其中 $y_A=P_1=aP$,$y_B=P_2=bP$),$h_2=H_2(S,V)$,$U=k\oplus h_2$。将密文 $\sigma=(U,c,S)$返回给 A_2。

A_2 经过第二阶段询问(这些询问与第一阶段询问相同,但不能对 σ 执行解/签密询问,也不能对 S 执行 H_2 询问)后,在模拟结束时 A_2 输出一个 θ'作为对 θ 的猜测。如果 $\theta'=\theta$,C 输出 $abP=x_A\cdot y_B=Y/V$ 作为 CDH 问题的答案,否则 C 没有解决 CDH 问题。

下面计算 C 成功的概率。若敌手 A_2 在第一阶段对 ID_A 或 ID_B 执行了私钥提取询问,则 C 将失败。由于 A_2 最多只执行 q_s 次私钥提取询问,所以 C 不失败的概率大于 $1-(\frac{2}{q_s})$。在

第二阶段的询问中,A_2 将以大于$\frac{1}{q_{H_2}}$的概率不对 S 执行 H_2 询问,大于$\frac{1}{q_{usc}}$的概率不对 σ 执行解/签密询问。因此,若 A_2 赢得此游戏,则在多项式有界的时间内 C 解决 CDH 问题的优势至少为$\frac{\varepsilon}{(1-\frac{2}{q_s})q_{H_2}q_{usc}}$(与 CDH 困难问题的不可计算性相矛盾)。所以不存在这样的敌手能赢得此游戏。因此,本方案在适应性选择密文攻击下具有不可区分性。在计算时间方面,每次签密最多需 4 次点乘运算,每次解/签密最多需 2 次点乘运算,2 次对运算。

2)不可伪造性

如果一个敌手能伪造一个本文提出的签密方案,那么它也能伪造一个文献[13]中的签名方案。然而,文献[13]已经证明了这个签名方案是具有不可伪造性的,因此,本文的方案在适应性选择消息攻击下能抗存在性伪造。

2.3　基于证书签密的 IPv6 网络跨域认证协议

为了解决基于无证书认证的域内用户与基于身份认证的域内用户之间的认证和密钥协商问题,针对 1.2 节提出的跨域认证模型和 2.1 节提出的基于证书的签密方案,结合前两节的研究成果,本节提出了一种基于签密的跨信任域认证协议,其具体流程如图 2 所示。

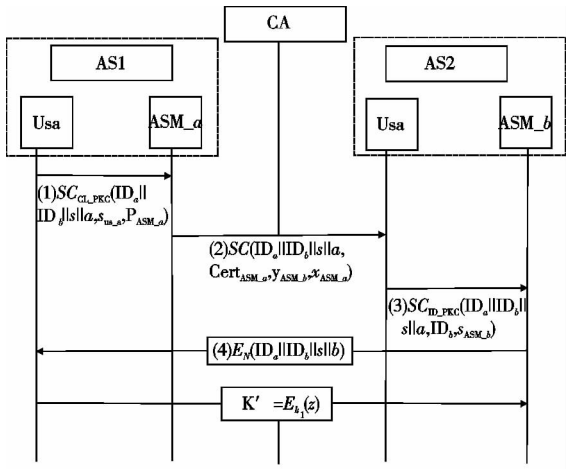

图2　跨域协议流程

图 2 涉及的符号的含义如下:Usa、Usb 代表用户 A 和用户 B;ID_a、ID_b 代表用户 A 和 B 的身份;s、a、b 为密钥材料且 $s,a,b\in Z_q^*$;$P_{\mathrm{ASM_}a}$代表域 A 的认证服务管理模块(ASM_a)在自治信任域内的公钥;$s_{\mathrm{us_a}}$表示用户 A 在自治信任域内的私钥,$s_{\mathrm{ASM_b}}$表示域 B 的认证服务管理模块(ASM_b)在自治信任域内的私钥;$SC_{\mathrm{CL_PKC}}()$表示域 A 使用的基于无证书的签密算法;$SC_{\mathrm{ID_PKC}}()$表示域 B 使用的基于身份的签密算法;$SC()$表示基于证书的签密算法;$y_{\mathrm{ASM\_}a}$、$y_{\mathrm{ASM_}b}$表示 ASM_a 和 ASM_b 在自治域之间基于证书的公钥;$x_{\mathrm{ASM\_}a}$、$x_{\mathrm{ASM_}b}$表示 ASM_a 和 ASM_b 在自治域之间的私钥;$\mathrm{Cert}_{\mathrm{ASM_}a}$为 ASM_$a$ 的证书。

该协议的具体认证过程如下:

a)用户 A 利用无证书签密算法计算签密密文 $\sigma=SC_{\mathrm{CL\_PKC}}(m,s_{\mathrm{us\_a}},P_{\mathrm{ASM\_}a})$,其中 $m=(\mathrm{ID}_a\parallel\mathrm{ID}_b\parallel s\parallel a)$,随机数 $s\in Z_q^*$,$a=g^x(x\in Z_q^*)$;并将密文 σ 发送给 ASM_a。

b)ASM_a 收到该消息时利用相应的算法对其进行解/签密处理,实现对用户 A 的认证后执行以下步骤:

(a)选取随机数 $k\in\{0,1\}^{\lambda}$,计算 $h_1=H_1(m,r)$,$c=E_k(m\parallel y_{\mathrm{ASM\_}b})$;

(b)计算 $Y=\frac{1}{(h_1+\mathrm{Cert}_{\mathrm{ASM\_}a}\cdot Q_{\mathrm{ASM\_}b})}$,$S=Y\cdot y_{\mathrm{ASM\_}a}$,$V=Y\cdot x_{\mathrm{ASM\_}a}\cdot y_{\mathrm{ASM\_}b}$;

(c)计算 $h_2=H_2(S,V)$,$U=k\oplus h_2$;

(d)将签密密文 $\sigma=(U,c,S)$ 发送给 ASM_b。

c)ASM_b 收到该消息后执行以下步骤:

(a)计算 $h_2=H_2(S,x_{\mathrm{ASM\_}b}\cdot S)$,$k=U\oplus h_2$;

(b)计算 $m\parallel y_{\mathrm{ASM\_}b}=D_k(c)$,$h_1=H_1(m,k)$,$Y=\frac{1}{(h_1+\mathrm{Cert}_{\mathrm{ASM\_}b}\cdot Q_{\mathrm{ASM\_}a})}$;

(c)验证 $\hat{e}(P,S)=\hat{e}(P,y_{\mathrm{ASM\_}a})^Y$ 是否成立,若成立则接收该消息,然后利用基于身份的签密算法计算密文 $\sigma=SC_{\mathrm{ID\_PKC}}(m,s_{\mathrm{ASM\_}b},\mathrm{ID}_b)$,并将其发送给用户 B。

d)当用户 B 收到该消息时利用相应的算法进行解/签密处理,实现 B 对 ASM_b 的认证后从消息 m 中分离出 s 和 a,进行如下处理:

(a)计算加密密钥 $N=a\oplus s$;

(b)随机选择 $y\in Z_q^*$,计算 $R=a^y$,$b=g^y$;

(c)生成会话密钥 $K_1=H(\mathrm{ID}_a\parallel\mathrm{ID}_b\parallel s\parallel R)$(其中 $H:\{0,1\}^*\rightarrow Z_q^*$);

(d)计算 $E_N(\mathrm{ID}_a\parallel\mathrm{ID}_b\parallel R\parallel b)$,并将其发送给用户 A。

e)用户 A 收到该消息后计算 $N'=a\oplus s$,判断等式 $N'=N$ 是否成立。若成立,则计算$(\mathrm{ID}_a\parallel\mathrm{ID}_b\parallel R\parallel b)=D_N[E_N(\mathrm{ID}_a\parallel\mathrm{ID}_b\parallel R\parallel b)]$,判断等式 $R=b^x$ 是否成立。若该等式成立,则用户 A 完成了对用户 B 的认证,生成双方共享的会话密钥 $K_1=H(\mathrm{ID}_a\parallel\mathrm{ID}_b\parallel s\parallel R)$。A 随机选择 $z\in Z_q^*$,计算 $K'=E_{K_1}(z)$,生成新密钥 $K_2=H(K_1\parallel z)$,并将 $K'=E_{K_1}(z)$ 发送给用户 B 用于密钥更新。

采用基于无证书签密认证方式的域内用户 A 与采用基于身份签密认证的域内用户 B 在相互认证的同时实现了密钥协商,获得了会话密钥 K_1。另外,会话双方在每次通信时都使用新的会话密钥 K_2,在每次通信的同时完成会话密钥的更新。

3　协议的性能分析

3.1　协议的安全性分析

1)实体之间的双向认证

在每个信任域内,通过域内的认证方式来实现用户和认证代理间的认证(在 AS1 中采用基于无证书签密的认证方式,在 AS2 中采用基于身份签密的认证方式),代理 ASM_a 和 ASM_b 通过基于证书签密的认证方式实现相互认证。代理ASM_a 完成对用户 A 的认证后,把认证结果反馈给 ASM_b,由于 ASM_b 和 ASM_a 之间建立了信任关系,从而 ASM_b 也获得对 A 的认证,然后 ASM_b 把认证的结果告诉 B,实现了 B 对 A 的认证。同时,A 对 B 的认证是通过验证等式 $R=b^x$ 即($b^x=g^{x\cdot y}$)是否成立来完成的。又因为 a 和 b 在传输过程中一直处于加密状

态(能知道 a 的 ASM_b 和 ASM_a 均可信),所以用户 A 和 B 之间实现了双向认证。

2)密钥协商

用户 A 和 B 之间的会话密钥是由双方分别给出的密钥材料 a、b、随机数 s 以及双方的身份信息产生,且 a、b、s 以及双方的身份信息都是以加密方式传输的。因此,通过计算 a^y 或 b^x 得到的会话密钥 $K_1 = H(\mathrm{ID}_a \| \mathrm{ID}_b \| s \| g^{x \cdot y})$ 是安全的。若攻击者能获得 $g^{x \cdot y}$,那么它就能高效地解决 CDH 问题。因此,K_1 只在用户 A 和 B 之间共享,任何不可信的第三方都无法获得。

3)完美前向保密(perfect forward secretly, PFS)

在密钥的生成过程中,由于每次会话密钥的产生都有随机数 z 的参与,且 z 是以加密方式传送,只有同时持有 K_1 和 z 的用户才能得到会话密钥,密钥更新时新旧密钥不存在任何关联等式,故具有 PFS 性质。

4)已知密钥安全

用户间生成的会话密钥为 $K_1 = H(\mathrm{ID}_a \| \mathrm{ID}_b \| s \| b^x) = H(\mathrm{ID}_a \| \mathrm{ID}_b \| s \| a^y)$,其中,$x$、$y$、$s$ 都是随机选择且以密文的形式在网络中传输,故每次生成的会话密钥 K_1 都是独立的。因此本认证协议是已知密钥安全的。

5)非密钥泄露伪装(no key compromise impersonation, non-KCI)

当用户的长期私钥泄露后,攻击者在协议中只能伪装成该用户,而不能将该用户伪装成其他任何用户。对于域 A 中的用户,其私钥由用户和 KGC 共同产生,攻击者即使知道用户的私钥也无法知道系统选取的秘密值(这是一个 DL 问题),进而无法推导出其他用户的私钥。对于域 B 中的用户,攻击者即使知道用户的私钥和用户的身份也无法计算出系统的秘密值,因为在式 $s_u = \dfrac{P}{(s + Q_U)}$ 中已知 Q_U、s_u 求 s 是一个数学困难问题。故本认证协议具有 non-KCI 的性质。

6)防止中间人攻击

因为 s 和 a 都采用了加密的形式传输,攻击者不能伪造类似 $E_N(\mathrm{ID}_a \| \mathrm{ID}_b \| R \| b)$ 的消息,因此该协议能有效防止中间人攻击。

3.2 协议的效率分析

本节对协议的计算开销(表 1)和通信开销(表 2)进行了分析,并将其与同类的其他协议进行了比较。

表 1 协议的计算开销

协议	P_U	E_U	S_U	E_x	P_A	E_A	S_A
文献[5]	2	0	1	2	4	0	4
文献[8]3.2 节	1	1	1	2	2	0	2
文献[8]3.4 节	1	1	1	2	2	0	2
本文	0	2	1	2	0	2	2

表 2 协议的通信开销

协议	C	C_{AB}	C_{ab}
文献[5]	14	6	0
文献[8]3.2 节	10	3	1
文献[8]3.4 节	5	1	2
本文	5	1	2

注:文献[5]——基于身份的多信任域密钥交换协议(IDAKE-M)

文献[8]3.2 节——一种通用多信任域认证协议

文献[8]3.4 节——一种基于时戳的改进工作协议

由表 1、2 可知,在计算开销方面,用户只需进行两次对称加/解密运算,一次签名或验证签名运算,两次指数运算;域间认证代理只需进行两次对称加/解密运算(本文提出的协议需要一定的运算开销,但不作为文章重点讨论)和两次签名或验证签名运算。在通信开销方面,本协议所需的通信次数与文献[8]3.4 节提出的改进跨域认证协议的通信次数相同。但是,本协议不受网络环境的限制,而文献[8]3.4 节中的认证协议只适合于同步通信网络(因为在该协议中引入了时间戳)。因此,与同类协议相比,本文的跨域认证协议不仅具有更好的可移植性而且还能降低系统开销。

4 结束语

本文首先介绍了 IPv6 网络跨域认证的相关知识,抽象了一种基于签密的多信任域认证模型;然后提出了一个随机预言机模型下可证明安全的基于证书的签密方案。提出了一种 IPv6 网络跨信任域认证协议并对其安全性和系统开销进行了分析。结果表明:本协议为解决 IPv6 网络互连过程中基于无证书认证的域内用户与基于身份认证的域内用户之间相互认证提供了较为实用的解决方案,具有安全、高效和可移植性好的特点。

参考文献:

[1] 张凌. 基于真实 IPv6 地址的跨域身份认证的研究和实现[D]. 重庆:重庆大学,2008.

[2] 王凤娇,张玉清. 跨域基于口令认证的密钥交换协议的安全模型[J]. 通信学报,2008,29(4): 24-29.

[3] YIN Yin, BAO Li. Secure cross-realm C2C-PAKE protocol[C]//Proc of the 11th Australasian Conference on Information Security and Privacy. 2006:395-406.

[4] BYUN J W, LEE D H, LIM J. Efficient and provably secure client-to-client password-based key exchange protocol[C]//Proc of the 8th Asia-Pacific Web Conference. Berlin: Springer-Verlag, 2006:830-836.

[5] 彭华熹. 一种基于身份的多信任域认证模型[J]. 计算机学报,2006,29(8):1271-1281.

[6] 路晓明,冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报,2006,34(4):577-582.

[7] 陈小峰,冯登国. 一种多信任域内的直接匿名证明方案[J]. 计算机学报,2008,31(7): 1122-1130.

[8] 朱辉. 若干安全认证协议的研究与设计[D]. 西安:西安电子科技大学, 2009.

[9] 游红. 移动 IPv6 绑定更新认证协议设计及分析[D]. 重庆:重庆大学,2006.

[10] 张娇,张玉军,张瀚文,等. 结合信任机制的移动 IPv6 网络快速跨域认证方法[J]. 计算机研究与发展,2008,45(6):951-959.

[11] 郑晓丽,姜迪刚. 基于无证书公钥密码体制的密钥管理[J]. 通信技术,2008,43(7): 95-97.

[12] 罗铭. 基于双线性对的签密和密钥协商方案研究[D]. 沈阳:东北大学,2009.

[13] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4):297-319.