

面向隐私保护的服务调用安全认证协议设计

柴林鹏^{1,2}, 张斌^{1,2}, 刘洋^{1,2}, 孙佳佳^{1,2}

(1. 信息工程大学, 河南 郑州 450001;

2. 河南省信息安全重点实验室, 河南 郑州 450001)

摘要: 针对 SOA 多域协作中认证信息的安全传递和用户隐私保护需求, 基于现有可证安全的无证书聚合签名方案提出一种面向隐私保护的服务调用安全认证协议。根据服务调用路径逐次对认证信息进行聚合签名, 有效支持服务提供方能够动态加入到服务调用认证流程; 分别利用聚合签名方案和 DH (Diffie-Hellman) 算法确保 SOAP 消息中认证信息和共享信息的机密性, 使 SOAP 消息中的隐私信息仅能被指定的服务提供方解密, 有效控制了隐私信息的披露范围; 同时利用聚合签名方案的公开可验证性确保服务调用流程中的其余服务提供方能够验证聚合签名值的有效性。与其他协议相比, 缩短了 SOAP 消息的长度, 提高了消息传输效率。

关键词: SOA 多域协作; 服务调用认证; 隐私保护; 无证书聚合签名; DH 算法

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018027

Design of privacy-preserving authentication protocol for service invocation

CHAI Linpeng^{1,2}, ZHANG Bin^{1,2}, LIU Yang^{1,2}, SUN Jiajia^{1,2}

(1. Information Engineering University, Zhengzhou 450001, China

2. Henan Province Information Security Key Laboratory, Zhengzhou 450001, China)

Abstract: Aiming at the requirement of the safe transmission of authentication credentials and the privacy preserving in service oriented multi-domain collaboration environment, a privacy-preserving authentication protocol for service invocation based on the provable secure certificateless aggregate signcryption scheme was proposed. By the path of the service invocation, the authentication information has been signcrypted successively, ensuring that the service providers can dynamically and orderly join in the process of service invocation authentication. The credentials and shared information can be safely transmitted respectively by the aggregate signcryption scheme and Diffie-Hellman algorithm, thus the SOAP message only can be decoded by specified acceptor, which is suitable for controlling the disclosure scope of the privacy information. Simultaneously, the public verifiability of CLASC can ensure that the validity of the aggregate signcryption can be verified by other service providers. The length of the SOAP message is shorter than existed protocols, which improve the transfer efficiency.

Key words: service oriented multi-domain collaboration, service invocation authentication, privacy protection, certificateless aggregate signcryption, diffie-hellman algorithm

收稿日期: 2018-01-02; 修回日期: 2018-02-04

通信作者: 柴林鹏, chailinpeng126@126.com

基金项目: 河南省基础与前沿技术研究计划基金资助项目 (No.142300413201); 信息保障技术重点实验室开放基金资助项目 (No. KJ-15-109); 信息工程大学新兴科研方向培育基金资助项目 (No. 2016604703)

Foundation Items: The Basic and Advanced Technology Research Project of Henan Province (No.142300413201), Open Fund Project of Key Laboratory of Information Assurance (No. KJ-15-109), Information Engineering University Emerging Research Direction Project of Information Engineering University (No. 2016604703)

1 引言

面向服务架构(SOA, service oriented architecture)作为一种服务部署模式,已成为整合信息系统内部资源的主流方法^[1,2]。服务调用作为SOA多域协作的主要技术手段,有力推动了企业间的业务协作^[3]。

为了确保服务的安全调用,学者基于不同的签名机制提出了多种服务调用认证协议,如基于PKI(public key infrastructure)签名机制^[4]、基于多重签名方案^[3]、基于身份的聚合签名方案^[5]以及基于无证书聚合签名方案^[6]。上述服务调用认证协议确保了认证信息的完整性、传递路径可鉴别、源可认证性。然而在链式调用过程中,认证消息需要随着服务的逐次调用披露给调用链上的其余服务提供方,未对用户个人信息的披露范围进行控制^[7],一旦某一服务提供方出现恶意行为或者遭受攻击,整个调用链路的认证信息将面临被泄露的安全风险;同时为了获取组合服务的功能,用户需要通过SOAP消息提交个人隐私信息以确保服务调用的执行。因此服务调用认证协议不仅需要满足认证信息安全传递,而且需要保证SOAP消息中的隐私信息仅能被指定的服务提供方解密,防止用户隐私信息扩散到服务调用链中的所有服务提供方。

目前针对Web服务组合中隐私保护问题的研究工作主要分为两方面:1)面向隐私数据的隐私保护方法,即采用传统安全技术为数据的整个生命周期提供隐私保护机制,如数据扰动^[8]、数据变换及隐藏^[9]、匿名化^[10]、加密技术^[11]以及访问控制^[12]等技术;2)面向计算过程的隐私保护方法,该类方法的核心思想是对服务提供方进行约束,防止用户的敏感信息遭到误用和传播,研究内容主要集中在用户隐私需求的建模与验证^[13]、隐私策略的匹配与协商^[14]以及隐私数据的暴露与风险^[15],该类方法建立了一套服务提供之前的隐私保护机制或者隐私泄露之后的分析评估模型^[13],但是需要提前明确Web服务组合的业务流程及用户的隐私需求。

本文设计了一种面向隐私保护的服务调用安全认证协议。对Zhang等^[16]提出的随机预言模型下可证安全的无证书聚合签密方案(CLASC,

certificateless aggregate signcryption)的聚合签密流程进行调整,使服务提供方能够动态加入到服务调用认证流程中;为了控制敏感信息披露范围,利用无证书聚合签密方案和DH算法分别用于确保SOAP消息中的认证信息和共享信息的安全传递,确保只能被指定的服务提供方接收解密,有效控制了个人信息的披露范围;同时利用无证书聚合签密的公开验证性确保其余服务提供方能够验证签密值的正确性;将协商因子封装在聚合签密信息中进行传递,进一步增强了对称密钥的安全性。

2 预备知识

2.1 双线性映射

设 G_1 和 G_2 是2个 q 阶的循环群,其中 q 是一个大素数。将 G_1 定义为有限域 F_p 中椭圆曲线上的一个点群, G_2 是定义在 F_p^* 上的一个子群。因此可以将 G_1 定义为一个阶数为 q 的加法循环群,其生成元为 P ,将 G_2 定义为一个阶数为 q 的乘法循环群^[17],定义双线性映射 $e: G_1 \times G_1 \rightarrow G_2$,其性质如下。

- 1) 双线性: 对于任意的 $M, N \in G_1, v, w \in Z_q^*$, 均有 $e(vM, wN) = e(M, N)^{vw}$ 。
- 2) 非退化性: 对于生成元 $P \in G_1$, $e(P, P) \neq 1$, 其中, 1是 G_2 的单位元。
- 3) 可计算性: 存在有效算法计算 $e(M, N)$ 。

2.2 困难假设

方案的安全性是基于以下困难数学问题。

离散对数问题(DLP, discrete logarithm problem): 给定 $M, N \in G_1$, 找到一个整数 $n \in Z_q^*$, 满足 $N = nM$ 。

计算性Diffie-Hellman问题(CDHP, computational Diffie-Hellman problem): 设 $v, w \in Z_q^*$, 给定 $P, vP, wP \in G_1$, 计算 $vwP \in G_1$ 。

双线性Diffie-Hellman问题(BDHP, bilinear Diffie-Hellman problem): 设 $v, w, z \in Z_q^*$, 给定 $P, vP, wP, zP \in G_1$, 计算 $e(P, P)^{vwz} \in G_2$ 。

3 面向隐私保护的服务调用安全认证协议设计及安全性分析

3.1 面向隐私保护的服务调用安全认证协议

在SOA多域协作中,引入信息管理中心作为

第三方, 利用层次化思想将信息管理中心分为 2 层, 即根管理中心(RMC, root management center)及其子节点 MC (management center), 其中 RMC 负责 MC 的管理及联盟多域协作环境^[18]的构建, 每个 MC 负责不同自治域的服务提供方的注册、管理及安全认证。

用户通过认证服务器 (AS, authentication server) 认证后将激活一个业务流程会话, 在该会话中应用服务器充当服务请求方, 向本域 MC 的注册中心 (RC, registration center) 查询所需服务, 如果本域服务无法满足业务需求, 则实施跨域服务调用。在服务调用过程中通过 SOAP 消息进行数据交互, 由 SOAP 消息代理生成调用请求消息, 将认证信息、公钥链及对称密钥的协商因子进行签名并聚合, 并以 SAML (security assertion markup language) 断言的形式嵌入到 SOAP 消息头中, 采用 DH 算法协商对称密钥, 按照 XML (extensible markup language) 加密规范对业务信

息及公钥链进行加密, 连同被调用方身份标识作为共享消息嵌入到消息体, 随后将 SOAP 消息发送至目标域中。系统中相关符号含义如表 1 所示。

3.1.1 系统初始化

系统初始化阶段完成 MC 层次化构建、系统参数选取以及各个自治域中实体的注册。RMC 主要包含根私钥生成器 (RPKG, root privacy key generation) 和根注册中心 (RRC, root register center), MC 包含私钥生成器 (PKG) 和注册中心。

1) RPKG 设置安全参数 λ , 选择阶数为 $q \geq 2^l$ 的加法群 G_1 和乘法群 G_2 , G_1 的生成元为 P , Z_q 为 q 阶的有限域, 定义双线对映射 $e: G_1 \times G_1 \rightarrow G_2$, 随机选择 $s \in Z_q^*$ 作为系统主密钥妥善保管, 选择 5 个防碰撞散列函数 $H_1, H_2: \{0,1\}^* \rightarrow G_1$, $H_3: \{0,1\}^* \rightarrow \{0,1\}^l$, $H_4: \{0,1\}^* \rightarrow Z_q^*$, $H_5: G_1 \rightarrow Z_q^*$, 其中, l 表示消息的长度, 系统公钥为 $PK_{RPKG} = sP$, 将系

表 1 相关符号含义

符号	含义
ID_{Pi}	第 i 个子 PKG 的身份标识
ID_{ij}	第 i 个子 PKG 中的第 j 个服务提供方的身份标识
s	RPKG 选取的系统主密钥
PK_{RPKG}	RPKG 的公钥
s_{Pi}	第 i 个子 PKG 的私钥
PK_{Pi}	第 i 个子 PKG 的公钥
D_{ij}	服务提供方 ID_{ij} 的部分私钥
r_{ij}	服务提供方 ID_{ij} 选取的秘密值
S_{ij}	服务提供方 ID_{ij} 的完整私钥
R	注册验证信息
A_u	用户 u 的访问权限信息
$MesID$	完成一次服务调用的唯一会话标识
T	调用请求消息的有效期
SIL_{ij}	服务调用过程的公钥链, 包含已参与调用的服务提供方的公钥信息
Mes_{1j}	第 1 个子 PKG 中的第 j 个服务提供方 ID_{1j} 完成服务调用需提供的业务信息
SK_{1j}	服务提供方 ID_{1j} 采用 DH 算法生成的对称密钥
EM_{1j}	服务提供方 ID_{1j} 依据对称密钥 SK_{1j} 加密生成的密文
$\eta_{1j} = (\alpha_{1j}, \delta_{1j}, \epsilon_{1j})$	服务提供方 ID_{1j} 根据 CLASC 对认证消息生成的信息签密值
$\beta_{ij}, \chi_{ij}, \phi, h_{ij}, Q_{ij}$	聚合签密操作过程中生成的中间值
η	服务提供方对认证信息生成的聚合签密值
B	字节 (byte)

统参数 $\{G_1, G_2, e, q, P, PK_{RPKG}, H_1, H_2, H_3, H_4, H_5\}$ 签名后发布到根注册中心。

2) 各域中的 MC 向 RMC 进行注册, 由 PKG 向 RPKG 发送身份标识 ID_{P_i} , 其中, $1 \leq i \leq n$, 随后 RPKG 计算各自的私钥 $s_{P_i} = sH_1(ID_{P_i})$, 通过安全信道将 s_{P_i} 发送到各个 PKG, PKG 生成公钥 $PK_{P_i} = s_{P_i}P$, 并将本域参数 $\{G_1, G_2, e, q, P, PK_{P_i}, H_1, H_2, H_3, H_4, H_5\}$ 发布到注册中心。

3) 各域中的服务提供方向 MC 发送注册申请, 由 PKG 依据每个服务提供方的身份标识 ID_{ij} 为其生成部分私钥 $D_{ij} = s_{P_i}Q_{ij}$, 其中, $Q_{ij} = H_1(ID_{ij})$, $1 \leq i \leq n, 1 \leq j \leq m$, n, m 分别表示 PKG 和服务提供方的数量, 并将秘密值 D_{ij} 安全发送到每个服务提供方。服务提供方随机选择秘密值 $r_{ij} \in Z_q^*$, 生成完整私钥 $S_{ij} = (D_{ij}, r_{ij})$, 并将公钥 $PK_{ij} = r_{ij}P$ 及验证信息 (Q_{ij}, R) 安全发送至 PKG, 其中, $R = r_{ij}Q_{ij}$ 。PKG 通过验证 $e(R, P) = e(Q_{ij}, PK_{ij})$ 是否成立确认服务提供方拥有与公钥 PK_{ij} 对应的秘密值 r_{ij} , 并检查 PK_{ij} 与其他已注册服务提供方公钥是否相同, 若相同则需返回提示信息, 重新

进行注册。将每个服务提供方的描述信息发布到 RC 的服务列表, 并通过 RMC 获取具有合作关系的自治域的服务列表。

3.1.2 协议具体流程

假定在 SOA 多域环境中分布着存在业务合作关系的 n 个自治域 $Domain_1, Domain_2, \dots, Domain_n$ 。依据参与调用的服务提供方数量的不同可分为单一服务调用和链式服务调用两种形式^[6]。单一服务调用中只包含 2 个服务提供方, 如图 1 中 a) 所示, 而链式服务调用过程至少包含 3 个服务提供方才能完成业务需求, 如图 1 中 b) 所示。单一服务调用与链式服务调用相比, 减少了聚合签密算法。

在单一服务调用中, 假设 $Domain_1$ 中服务提供方 ID_{1j} 需要调用 $Domain_2$ 中的服务提供方 ID_{2k} 以实现业务功能。

1) 选择随机数 $y_{1j} \in Z_q^*$, 计算 DH 算法的协商因子 $Y_{1j} = y_{1j}P$ 及协商后的加密密钥 $SK_{1j} = H_5(y_{1j}PK_{2k})$ 。

由 SOAP 消息代理生成初始服务调用请求消息 $(SAML_{1j}, Mes_{1j})$, 其中, $SAML_{1j} = (A_u, ID_{1j},$

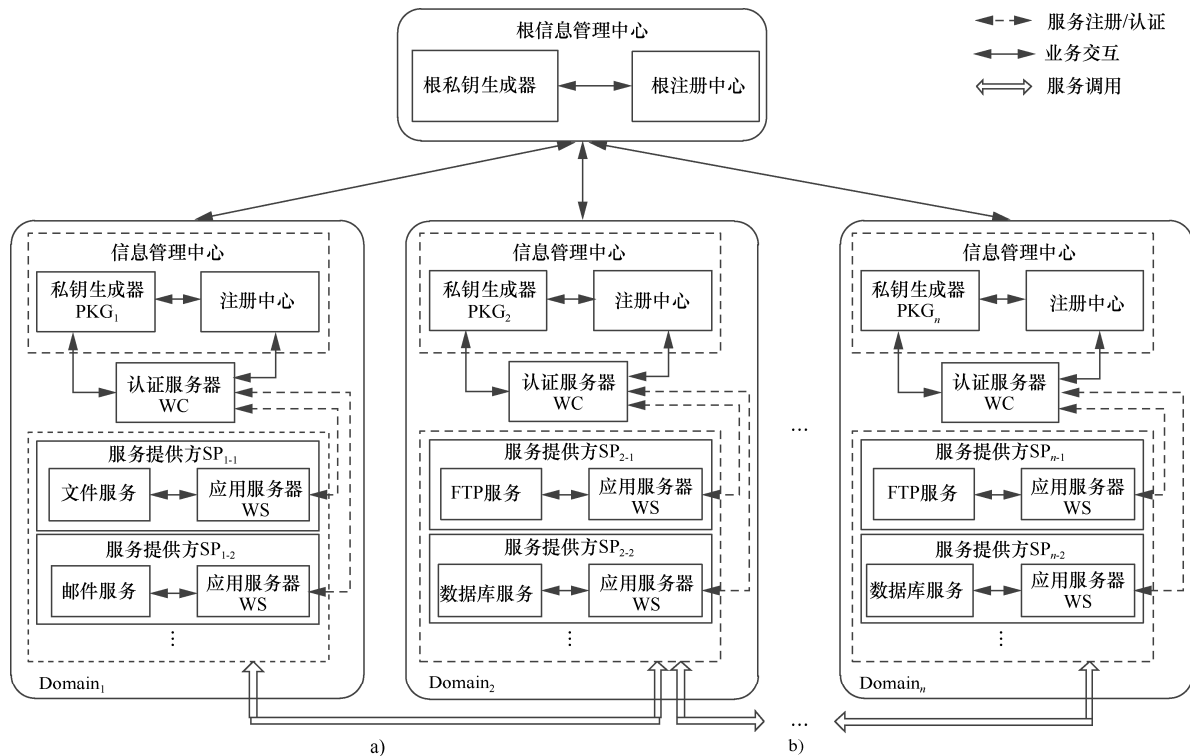


图1 SOA多域协作服务调用认证协议流程

$ID_{p1}, ID_{2k}, ID_{p2}, SIL_{1j}, Y_{1j}, MesID, T)$, $ID_{1j}, ID_{p1}, ID_{2k}, ID_{p2}$ 分别为调用发起方、被调用方及其第三方 PKG 的身份标识, $SIL_{1j} = (ID_{1j}, ID_{2k})$ 为公钥链。

依据无证书聚合签密方案对 SAML 断言实施签密, 服务调用发起方的身份标识及公私钥分别为 ID_{1j} 、 PK_{1j} 、 $S_{1j} = (D_{1j}, r_{1j})$, 被调用方的身份标识及公钥分别为 ID_{2k} 、 PK_{2k} , 发起方执行以下步骤。

① 选择随机数 $c_{1j} \in Z_q^*$, 计算 $\alpha_{1j} = c_{1j}P$, $Q_{2k} = H_1(ID_{2k})$ 和 $\beta_{1j} = e(PK_{p2}, Q_{2k})^{c_{1j}}$ 。

② 计算 $\chi_{1j} = H_3(\alpha_{1j}, \beta_{1j}, c_{1j}PK_{2k}, ID_{2k})$, $\delta_{1j} = \chi_{1j} \oplus SAML_{1j}$ 。

③ 计算 $\varphi = H_2(PK_{RPKG})$, $h_{1j} = H_4(\alpha_{1j}, \delta_{1j}, ID_{1j}, ID_{2k})$, $\varepsilon_{1j} = D_{1j} + (h_{1j}c_{1j} + r_{1j})\varphi$, 输出签密信息 $\eta_{1j} = (\alpha_{1j}, \delta_{1j}, \varepsilon_{1j})$, 将其绑定到 SOAP 消息头。

④ 利用加密密钥 SK_{1j} 对业务信息及公钥链进行加密 $EM_{1j} = Enc(SK_{1j}, (Mes_{1j}, SIL_{1j}))$, 连同被调用方的身份标识 ID_{2k} 作为共享消息绑定到 SOAP 消息体中, 随后将整个 SOAP 消息发送到 $Domain_2$, 具体的 SOAP 消息处理如图 2 所示。

2) $Domain_2$ 中的 SOAP 消息代理接收到消息后, 与认证服务器交互完成解密验签, 验证过程如下。

① 由服务提供方 ID_{2k} 计算 $\beta_{1j} = e(\alpha_{1j}, D_{2k})$, $\chi_{1j} = H_3(\alpha_{1j}, \beta_{1j}, r_{2k}\alpha_{1j}, ID_{2k})$ 及 $SAML_{1j} = \chi_{1j} \oplus \delta_{1j}$,

输出消息 $SAML_{1j}$, 获得调用方标识 ID_{1j} , 结合服务列表确认调用方是否为业务合作方。

② 确认后计算 $\varphi = H_2(PK_{RPKG})$, $Q_{1j} = H_1(ID_{1j})$ 及 $h_{1j} = H_4(\alpha_{1j}, \delta_{1j}, ID_{1j}, ID_{2k})$, 验证等式 $e(\varepsilon_{1j}, P) = e(Q_{1j}, PK_{p1})e((h_{1j}\alpha_{1j} + PK_{1j}), \varphi)$ 是否成立, 若成立, 则继续执行, 否则, 返回报错信息。

③ ID_{2k} 结合自身私钥 S_{2k} 计算解密密钥 $SK_{1j} = H_5(r_{2k}Y_{1j})$, 计算 $Dec(SK_{1j}, EM_{1j})$ 获得业务信息及公钥链, 验证公钥链的一致性, 若不一致或者认证失败, 则返回报错信息, 具体流程如图 3 所示。

当需要进行链式服务调用时, ID_{2k} 将作为新的调用发起方发送服务调用请求, 首先对更新后 SAML 断言 (更新公钥链、用户权限信息、调用方及被调用方相关信息) 和协商因子进行签密处理后, 连同之前的签密值进行聚合后绑定到 SOAP 消息头; 同时协商新的加密密钥, 按照步骤 3)~步骤 4) 执行。

3) 假设 $Domain_{n-1}$ 中的服务提供方 $ID_{(n-1)x}$ 已验证调用请求的合法性, 需要进一步调用 $Domain_n$ 中的服务提供方 ID_{ny} , 协议具体流程如图 4 所示, $ID_{(n-1)x}$ 执行以下步骤。

① 将被调用方的公钥 PK_{ny} 加入公钥链中 $SIL_{(n-1)x} = (PK_{1j}, \dots, PK_{(n-1)x}, PK_{ny})$, 生成签密消息 $\eta_{(n-1)x} = (\alpha_{(n-1)x}, \delta_{(n-1)x}, \varepsilon_{(n-1)x})$ 。

② 计算 $\varepsilon = \sum_{i=1}^{n-1} \varepsilon_{ij}, j \in (1, m)$, 将聚合签密信

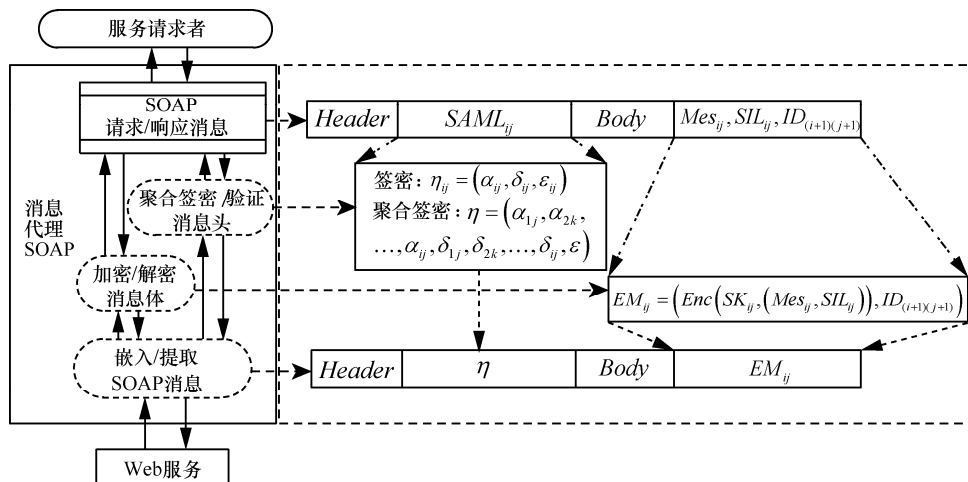


图2 SOAP 消息处理

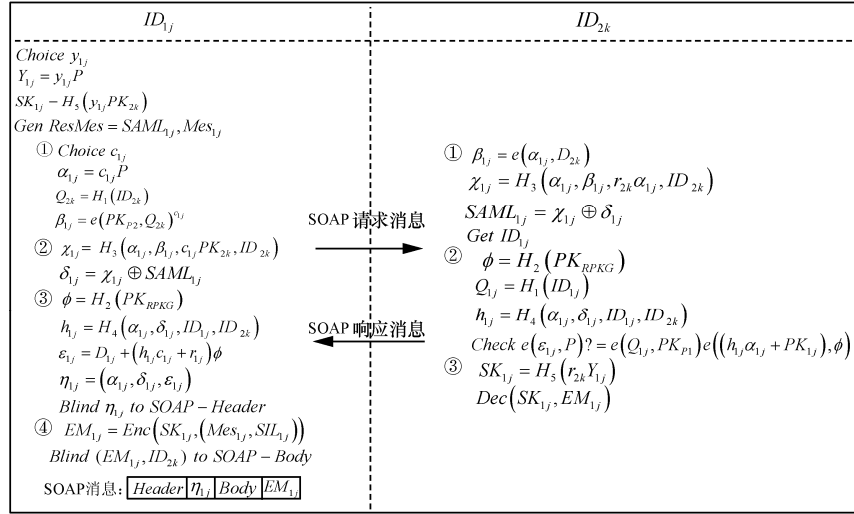


图3 单一服务调用流程

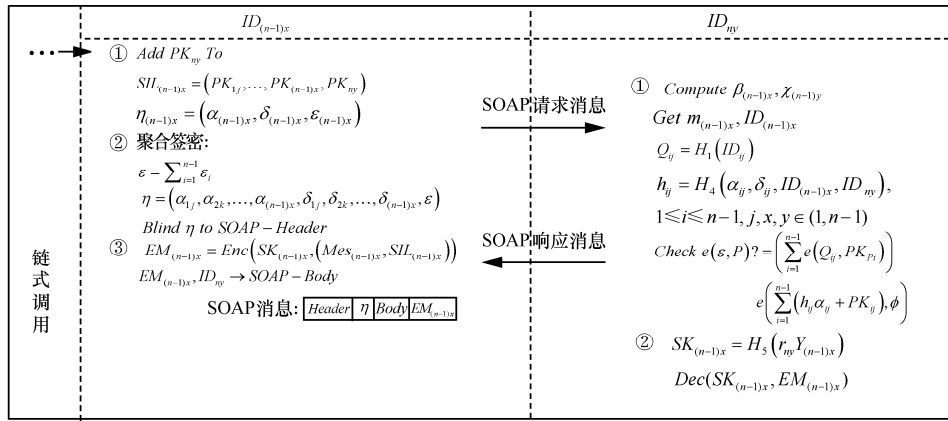


图4 链式服务调用流程

息 $\eta = (\alpha_{1j}, \alpha_{2k}, \dots, \alpha_{(n-1)x}, \delta_{1j}, \delta_{2k}, \dots, \delta_{(n-1)x}, \epsilon)$ 绑定到 SOAP 消息头。

③ 将业务信息及公钥链信息进行加密 $EM_{(n-1)x} = Enc(SK_{(n-1)x}, (Mes_{(n-1)x}, SIL_{(n-1)x}))$ ，连同被调用方的身份标识 ID_{ny} 绑定到 SOAP 消息体，随后将 SOAP 消息发送到 $Domain_n$ 。

5) $Domain_n$ 中的 SOAP 消息代理接收到消息后，与认证服务器交互完成解密验签，验证过程如下。

① ID_{ny} 结合自身私钥 S_{ny} 计算 $\beta_{(n-1)x}, \chi_{(n-1)y}$ ，进而获得认证消息及调用方标识 $ID_{(n-1)x}$ ，计算 $Q_{ij} = H_1(ID_{ij})$ ， $h_{ij} = H_4(\alpha_{ij}, \delta_{ij}, ID_{(n-1)x}, ID_{ny})$ ，其中， $1 \leq i \leq n-1, j, x, y \in (1, m-1)$ ，验证等式

$$e(\epsilon, P) = \left(\sum_{i=1}^{n-1} e(Q_{ij}, PK_{Pi}) \right) e\left(\sum_{i=1}^{n-1} (h_{ij}\alpha_{ij} + PK_{ij}), \phi \right)$$

是否成立，若成立则继续执行，否则返回报错信息。

② 结合 S_{ny} 计算解密密钥 $SK_{(n-1)x} = H_3(r_{ny}Y_{(n-1)x})$ ，计算 $Dec(SK_{(n-1)x}, EM_{(n-1)x})$ 获得业务信息及公钥链，验证公钥链表的一致性，验证通过后则提供服务，若不一致或者认证失败，则返回报错信息。

3.2 安全性及效率分析

3.2.1 正确性

服务链中的每个服务提供方均可验证本服务节点之前全部服务提供方的聚合签名值 ϵ 的正确性，验证方法如下。

$$\begin{aligned} e(\epsilon, P) &= e\left(\sum_{i=1}^n \epsilon_{ij}, P \right) = e\left(\sum_{i=1}^n D_{ij} + (h_{ij}c_{ij} + r_{ij})\phi, P \right) \\ &= e\left(\sum_{i=1}^n D_{ij}, P \right) e\left(\sum_{i=1}^n (h_{ij}c_{ij} + r_{ij})\phi, \phi \right) \\ &= \left(\sum_{i=1}^n e(Q_{ij}, PK_{Pi}) \right) e\left(\sum_{i=1}^n (h_{ij}\alpha_{ij} + PK_{ij}), \phi \right) \end{aligned}$$

3.2.2 不可否认性

只有服务提供方拥有完整私钥 $S_{ij} = (D_{ij}, r_{ij})$ ，其中 r_{ij} 为服务提供方选取的随机数，因此在随机数被妥善保管的情况下，只有服务提供方能够解密验证调用请求信息，并作为新的调用方发起服务调用，同时服务提供方的公钥信息在系统初始化阶段已经公布到服务列表中，结合聚合签名验证可实现认证信息的不可否认性。

3.2.3 传递路径的可鉴别性及源可认证性

引入无证书聚合签名机制使整个公钥链中所有参与服务提供方均可通过验证聚合签名值鉴别本节点之前所有服务提供方的身份信息，进而确定初始发起方实现源可认证，确保整个服务调用过程属于同一个会话。

3.2.4 用户隐私保护

对用户隐私信息保护可分为两方面。

1) 在 SOAP 消息头中认证信息仅包含用户的权限信息及服务提供方的相关信息，并未暴露用户具体的身份信息；SOAP 消息体中包含的用户隐私信息采用协商对称密钥 SK_{ij} 进行加密传输，确保外部用户无法获取用户的任何敏感信息，且只有指定的接收方结合自身私钥才能获得对称密钥，进而解密信息。

2) 以 Domain_{n-1} 中的服务提供方 $ID_{(n-1)x}$ 需要调用 Domain_n 中的服务提供方 ID_{ny} 为例， ID_{ny} 仅能解密 $ID_{(n-1)x}$ 中的 SAML 断言 $SAML_{(n-1)x}$ ，无法解密之前服务提供方之间的通信消息 $SAML_{ij}, EM_{ij}, 1 \leq i < n-1$ ，因此本文协议可在满足传递路径可鉴别及高效验证的同时，确保其他服务提供方之间通信消息的密态传递，有效控制隐私信息的披露对象和范围，在一定程度上保护了用户的隐私信息。

3.2.5 密钥托管问题

密钥托管问题主要分为两方面。

1) 假设 PKG 是诚实可信的，PKG 只为服务提供方生成部分私钥，提高了服务提供方在私钥生成过程中的参与度，避免了 PKG 完全拥有实体私钥或者遭受恶意攻击带来的安全问题。

2) 假设 PKG 存在泄露服务提供方私钥的行为，或者自身冒充服务提供方实施恶意服务调用，恶意 PKG 将服务提供方部分私钥 D_{ij} 泄露给敌

手，协助敌手伪造服务提供方的完整私钥 $S'_{ij} = (D_{ij}, r'_{ij})$ ，其中 $r'_{ij} \in Z_q^*$ 为敌手选取的随机数，或者自身选取随机数，伪装成合法服务提供方进行服务恶意调用。由于服务提供方的公钥 $PK_{ij} = r_{ij}P$ 是由服务提供方选取的随机数 $r_{ij} \in Z_q^*$ 结合生成元 P 生成的，通过 PKG 验证后公布到本域服务列表中，同时在其他域中进行列表备份，被调用方可结合服务列表进行公钥链验证，依据公钥的一致性判断 PKG 是否存在不诚实行为。

3.3 协议传输效率分析

以下将对基于不同签名机制的服务调用协议进行性能分析。假定服务提供方具有足够的计算能力，整个调用公钥链中共有 n 个服务提供方，为了确保信息的安全性，散列函数统一选用防碰撞的 SHA-256，RSA 签名算法选用长度为 2 048 bit 的模数，依据国际组织规定，在同等安全强度下，ECC 签名算法的模数长度为 244 bit。整个服务调用过程中的传输开销为整个调用断言的总长度， L_i 分别表示对应文献中的消息传输总长度，单位为 B。

基于 PKI 签名机制^[4]：公钥链表中的 X.509 证书只考虑用户标识、公钥和证书签名长度，其长度分别为 50 B、256 B 和 256 B，其余的数据可忽略；断言中主要包含用户及断言生成者的身份信息、随机数及公钥链表，其长度分别定为 50 B、50 B、16 B、562 n B；断言摘要长度为 32 n B；待签名信息采用 RSA 签名算法生成的签名值 D_i 长度为 256 n B，因此消息传输总长度为

$$L_4 = L_{SAML} + L_{D_i} + L_{X.509} = 132 + 1412n$$

基于身份的聚合签名机制^[5]：调用断言为 $(SAML_i, ML_i, AD_i, PKL_i)$ ，其中 SAML 断言主要包含 ID_C, IDP, N_C, T, PKL_i ，长度分别为 50 B、50 B、16 B、16 B、64 n B， $ML_i = \text{hash}(SAML_i)$ ，长度为 32 n B；断言签名采用 ECC 签名算法实现，生成的聚合签名元素为 $AD_n = (w, S_n, T_n)$ ，其中 w 为任意长度的字符串，假设长度为 16 B， S_n, T_n 均为椭圆曲线上的点，长度均为 64 B，签名长度为 $L_{AD_i} = 144$ B；公钥链中的公钥为椭圆曲线上的点，长度为 64 n B；因此消息传输总长度为

$$L_5 = L_{SAML} + L_{AD_i} + nL_{PK} = 276 + 160n$$

基于无证书聚合签名机制^[6]：公钥链中的长度为 64 n B；断言签名采用 ECC (elliptic curve

cryptography) 签名算法聚合后, 生成的签名为 $QM_n = (U_1, U_2, \dots, U_n, V_n)$, U_n 、 V_n 均为椭圆曲线上的点, 因此其长度为 $L_{QM} = 64(n+1)B$, 公钥链表中的元素为 $MK_i = (Q_i, sk_{IDi})$, Q_i 、 sk_{IDi} 均为椭圆曲线上的点, 其长度均为 $64nB$, 因此消息传输总长度为

$$L_6 = L_{BA} + L_{SL} + L_{QM} + L_{GK} = 262 + 234n$$

本文协议: 将整个 SAML 断言进行签密操作, 将整个调用请求压缩成长度固定的签密值 $\eta = (\alpha_{1j}, \alpha_{2k}, \dots, \alpha_{ij}, \delta_{1j}, \delta_{2k}, \dots, \delta_{ij}, \varepsilon)$, 其中, α_{ij} 、 ε 均为椭圆曲线上的点, 其长度均为 $64B$, δ_{ij} 属于实数域, 假设长度为 $16B$, 因此消息传输总长度为

$$L_0 = L_\eta + L_{PKi} = 64 + 80n$$

在同样的网络环境中, 用 EF_1 、 EF_2 、 EF_3 分别表示本文协议相对于基于 PKI 机制、基于身份签名机制以及基于无证书签名机制的协议在传输效率方面的提升率, 传输提升率变化如图 5 所示。

$$EF_1 = \frac{|L_4 - L_0|}{L_4} = \frac{68 + 1332n}{132 + 1412n}$$

$$EF_2 = \frac{|L_5 - L_0|}{L_5} = \frac{212 + 80n}{276 + 160n}$$

$$EF_3 = \frac{|L_6 - L_0|}{L_6} = \frac{198 + 154n}{262 + 234n}$$

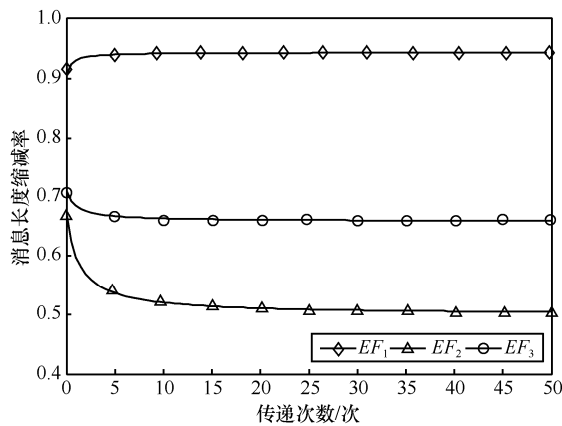


图5 服务调用消息长度缩减率

从图 5 中可以看出, 基于无证书聚合签密方案的协议与基于 PKI 机制的协议相比, 传递次数达到 5 次以上时, 消息长度缩减率 EF_1 趋于 0.94; 与基于身份的聚合签名和基于无证书聚合签名的协议相比, 缩减率 EF_2 、 EF_3 随着传递次数的增

加逐渐降低, 分别趋于 0.5、0.66, 因此, 基于无证书聚合签密方案的服务调用认证协议在调用消息传输方面优势更突出。

4 结束语

本文分析了 SOA 多域协作中服务调用存在的认证及隐私保护需求, 指出服务调用认证协议需要在满足认证信息安全传递及高效验证的基础上, 有效控制 SOAP 消息中认证信息和共享信息的披露范围。分别采用无证书聚合签密方案和 DH 算法确保 SOAP 消息中的认证信息和共享信息的机密性, 使 SOAP 消息只能被指定的服务提供方解密, 有效控制了信息的披露对象和范围, 同时其余服务提供方仍能根据签密信息验证认证消息的安全性; 进一步缩短了传输消息的长度, 提升了服务调用请求消息的传输效率。下一步将结合匿名认证相关技术, 为用户隐私信息的安全防护工作提供更加全面的技术支撑。

参考文献:

- [1] SOA. 引领软件发展新方向官方主页[EB/OL]. <http://www.eworks.ne.tcn/tbbd/soa/x1.htm>.
SOA, The official homepage of guiding development of the software[EB/OL]. <http://www.eworks.ne.tcn/tbbd/soa/x1.htm>.
- [2] 朱志良, 苑海涛, 宋杰, 等. SOA 与云计算: 竞争还是融合[J]. 计算机科学, 2011, 38(12): 6-11.
ZHU Z L, YUAN H T, SONG J, et al. SOA and cloud computing: competition or integration[J]. Computer Science, 2011, 38(12): 6-11.
- [3] 韩崇硯. 面向 SOA 多域协作环境的认证技术研究[D]. 郑州: 信息工程大学, 2011.
HAN C Y. Research on authentication technologies in service oriented multi-domain collaboration environment[D]. Zhengzhou: Information Engineering University, 2011.
- [4] OASIS. Web services security: SOAP message security 1.1 (WS-Security 2004)[EB/OL]. <https://www.oasis-open.org/standards/wssv1.1.1>
- [5] 张斌, 王曦. 面向 Web 服务的 SAML 路径验证协议及其性能分析[J]. 计算机科学, 2013, 40(3): 192-196.
ZHANG B, WANG X. SAML path verification protocol for Web service and its performance analysis[J]. Computer Science, 2013, 40(3): 192-196.
- [6] 王冠众. 面向大数据的 SOA 认证关键技术研究[D]. 郑州: 信息工程大学, 2015.
WANG G Z. Research on key technologies of authentication in service oriented big data environment[D]. Zhengzhou: Information Engineering University, 2015.
- [7] 刘雅辉, 张铁赢, 靳小龙, 等. 大数据时代的个人隐私保护[J].

- 计算机研究与发展, 2015, 52(1): 229-247.
- LIU Y H, ZHANG T Y, JIN X L, et al. Personal privacy protection in the era of big data[J]. Journal of Computer Research and Development, 2015, 52(1): 229-247.
- [8] 方跃坚, 朱锦钟, 周文, 等. 数据挖掘隐私保护算法综述[J]. 信息安全学报, 2017(2): 6-11.
- FANG Y J, ZHU J Z, ZHOU W, et al. A survey on data mining privacy protection algorithms[J]. Netinfo Security, 2017(2): 6-11.
- [9] 严文博, 姚远志, 张卫明, 等. 基于二维码和信息隐藏的物流系统隐私保护方案[J]. 网络与信息安全学报, 2017, 3(11): 22-28.
- YAN W Y, YAO Y Z, ZHANG W M, et al. Privacy-preserving scheme for logistics systems based on 2D code and information hiding[J]. Chinese Journal of Network and Information Security, 2017, 3(11): 22-28.
- [10] 张磊, 马春光, 杨松涛, 等. 面向关联攻击的轨迹匿名方法[J]. 网络与信息安全学报, 2017, 3(6): 8-20.
- ZHANG L, MA C G, YANG S T, et al. Trajectories anonymous algorithm for association attack[J]. Chinese Journal of Network and Information Security, 2017, 3(6): 8-20.
- [11] 巩林明, 李顺东, 窦家维, 等. 同态加密方案及安全两点直线计算协议[J]. 软件学报, 2017, 28(12): 6-11.
- GONG F L, LI S D, DOU J W, et al. Homomorphic encryption scheme and a protocol on secure computing a private points[J]. Journal of Software, 2017, 28(12): 6-11.
- [12] 马铭鑫, 史国振, 王亚琼, 等. 适用于分布式系统的多级安全访问控制策略[J]. 网络与信息安全学报, 2017, 3(8): 28-34.
- MA M X, SHI Z G, WANG Y Q, et al. Multilevel secure access control policy for distributed systems[J]. Chinese Journal of Network and Information Security, 2017, 3(8): 28-34.
- [13] 刘博. 满足用户隐私需求的 Web 服务组合方法研究[D]. 南京: 南京航空航天大学, 2015.
- LIU B. Research on the method of Web services composition for user's privacy requirement[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2015.
- [14] KAGAL L, PATO J. Preserving privacy based on semantic policy tools[J]. Security & Privacy, 2010, 8(4): 25-30.
- [15] LIU L T Y, ZHU H B, HUANG Z Q. Analysis of the minimal privacy disclosure for Web services collaborations with role mechanisms[J]. Expert System & Application, 2011, 38(4): 4540-4549.
- [16] 张玉磊, 王欢, 李臣意, 等. 可证安全的紧致无证书聚合签密方案[J]. 电子与信息学报, 2015, 37(12): 2838-2844.
- ZHANG Y L, WANG H, LI C Y, et al. Provable secure and compact certificateless aggregate signcryption scheme[J]. Journal of Electronics & Information Technology, 2015, 37(12): 2838-2844.
- [17] DAN B, MATT F. Identity-based encryption from the weil pairing[J]. Lecture Notes in Computer Science, 2001(1): 213-229.
- [18] JAMES J, RAFAE B, ELISA B, et al. X-RBAC: an access control language for multi-domain environments[R]. West Lafayette of USA: Center for Education and Research in Information Assurance and Security, Purdue University, 2004.

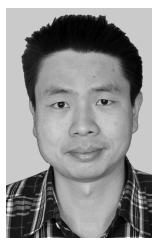
[作者简介]



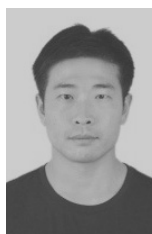
柴林鹏 (1993-), 男, 山西临汾人, 信息工程大学硕士生, 主要研究方向为信息安全。



张斌 (1969-), 男, 河南郑州人, 信息工程大学教授、博士生导师, 主要研究方向为网络空间安全。



刘洋 (1980-), 男, 河南南阳人, 信息工程大学讲师, 主要研究方向为信息系统安全。



孙佳佳 (1987-), 男, 河南洛阳人, 博士, 信息工程大学讲师, 主要研究方向为信息对抗与信息安全。