第 36 卷 第 3 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.3 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)03—0148—04 文献标识码：A 中图分类号：TP309

开放网络环境中面向信任的单点登录

万灿军，李长云
(湖南工业大学计算机与通信学院，株洲 412008)

摘 要：在开放网络环境中，传统的单点登录易出现单点失效，难以解决跨域认证。针对以上问题，综合考虑身份信任机制和行为信任机制，提出一个面向信任的对等单点登录系统架构。构造基于主观逻辑的单点登录信任模型，给出模型的形式化信任描述，并在此基础上建立信任评估机制。该模型已应用于跨域认证，结果表明该模型是可行的。

关键词：单点登录；信任模型；主观逻辑；跨域认证

Trust-oriented Single Sign-On in Open Network Environment

WAN Can-jun, LI Chang-yun
(School of Computer and Communication, Hunan University of Technology, Zhuzhou 412008)

【Abstract】 In open network environment, the traditional Single Sign-On(SSO) is easy to lead to single point failure and difficult to solve the problems of cross-domain authentication. To resolve the above-mentioned problems, by considering the identity trust mechanism and the behavior trust mechanism, a trust-oriented Peer-to-Peer Single Sign-On system architecture is proposed. A Single Sign-On trust model based on subjective logic is built, the formal description of trust is given in this model, and the trust evaluation mechanism is established. This model is applied in the cross-domain authentication, and the results show that the model is feasible.

【Key words】 Single Sign-On(SSO); trust model; subjective logic; cross-domain authentication

1 概述

单点登录(Single Sign-On, SSO)是指用户只需在网络中主动进行一次身份认证，随后便可访问所有被授权的网络资源。开放网络环境下的 SSO 是近几年来 SSO 的研究热点，为了使开放网络环境下的 SSO 更安全、更可靠，SSO 中的信任机制显得格外重要，包括身份信任机制和行为信任机制。

身份信任机制主要负责身份认证，采用 Kerberos 认证协议[1]、公钥基础设施(PKI)[2]和安全断言标记语言(SAML)[3]等实施身份认证。身份信任机制很好地解决了传统的认证问题，但在开放网络环境下存在一些不足：

(1)在整个网络中使用单一认证中心，存在单点失效的缺陷；

(2)集中式的 SSO 模式无法满足跨域认证的需求；

(3)在认证过程中只看主体身份而不考察其行为可信性，这在开放网络环境下是不安全的。

因此，需要一种能够适应开放网络环境的行为信任机制。

行为信任机制主要负责在参与 SSO 的实体间建立信任关系，实现协同工作，其中最关键的是构建信任模型。Abdul-Rahman 模型[4]和 Beth 模型[5]均使用概率理论描述和度量信任，但难以描述信任的主观性和不确定性。Jøsang 模型[6]引入了主观逻辑，可确切地描述信任的主观性和不确定性。

借鉴上述成果，本文综合考虑身份信任机制和行为信任机制，采用基于主观逻辑的信任模型，引入 P2P 技术，提出了一个面向信任的对等单点登录(Trust-oriented Peer-to-Peer Single Sign-On, TP-SSO)系统。

2 TP-SSO系统架构

TP-SSO 系统的核心思想是身份联合，基于 Liberty 协议，参与 SSO 的各 Web 应用系统可保留原来的身份信任机制，通过行为信任机制建立它们之间的信任关系，以便用户能在相互信任的应用系统间自由穿梭。

如图 1 所示，TP-SSO 系统架构中主要有 4 个主体：(1)用户(User)；(2)身份提供者(Identity Provider, IDP)；(3)服务提供者(Service Provider, SP)；(4)信任代理(Trust Agent)。User 是指使用 SSO 服务的个体。IDP 是指为个体提供身份认证的认证中心，TP-SSO 系统中有多个相互独立存在的 IDP，即认证中心不是唯一的，这点与传统的单一认证中心具有根本区别；SP 是指为个体提供某种应用服务的机构，每个 Web 应用系统可看作 IDP 和 SP 的混合体，IDP 和 SP 采用 SAML 交换认证信息；Trust Agent 负责建立各 Web 应用系统之间的信任关系，并提供信任监测、评估、存储、查询和更新等服务，以便实现跨域认证。

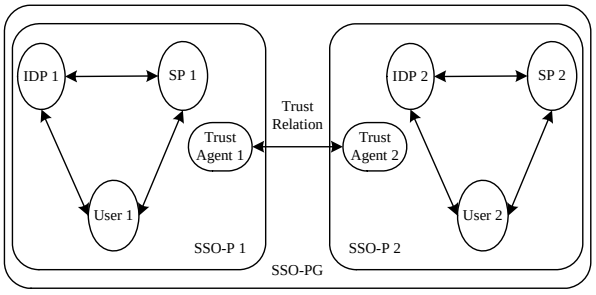

图 1 TP-SSO 系统架构

基金项目：国家自然科学基金资助项目(60773110)
作者简介：万灿军(1982－)，男，硕士研究生，主研方向：软件体系结构；李长云，教授
收稿日期：2009-08-14 **E-mail**：wancanjun2008@163.com

引入 P2P 技术后，每个 Web 应用系统作为单点登录的对等点(Single Sign-On Peer, SSO-P)，基于 JXTA 平台组织成 P2P 网络。不同 SSO-P 通过它们之间的信任关系与合作协议构成一个单点登录对等组(Single Sign-On Peer Group, SSO-PG)。只有属于同一组的 SSO-P 才有资格进行身份联合，有资格不等同于必然可以，还要看 SSO-P 的信任度是否符合要求。相对于传统的集中式 SSO 模式，TP-SSO 系统的 SSO 不要求集中在某个 SSO-P 上，克服了单点失效的缺陷。本文重点关注行为信任机制，下文如无特殊说明，所提信任均指行为信任。

3 TP-SSO信任模型

信任是指主体对客体行为的主观可能性预期，取决于实体间直接的交互行为历史和间接的经验推荐信息，且随实体的行为而动态变化。TP-SSO 系统架构在一个信任的环境下，TP-SSO 信任模型提供了建立、量化和管理各 SSO-P 之间信任关系的框架。

3.1 主观逻辑

基于主观逻辑，TP-SSO 信任模型引入事实空间和观念空间来描述和度量信任。事实空间由一系列节点产生的肯定事件和否定事件组成，观念空间由一系列对节点的主观信任评估组成。信任度由三元组 $\omega=\{b,d,u\}$ 来描述，并满足：$b+d+u=1\ (b,d,u\in[0,1])$。其中，b,d,u 分别描述对节点的信任程度、不信任程度和不确定程度。根据肯定事件数 r 和否定事件数 s，信任度 ω 可按式(1)计算：

$$\begin{cases} b=r/(r+s+1) \\ d=s/(r+s+1) \\ u=1/(r+s+1) \end{cases} \tag{1}$$

TP-SSO 信任模型提供了一套主观逻辑算子用于信任度计算，主要包括推荐算子和合意算子。

定义 1 设节点 A 对节点 B 作为推荐者的信任评价为 $\omega_B^A=\{b_B^A,d_B^A,u_B^A\}$，节点 B 对节点 C 的信任评价为 $\omega_C^B=\{b_C^B,d_C^B,u_C^B\}$，则 A 经过 B 的推荐对 C 的信任评价为 $\omega_C^{AB}=\omega_B^A\otimes\omega_C^B=\{b_C^{AB},d_C^{AB},u_C^{AB}\}$，并满足：

$$\begin{cases} b_C^{AB}=b_B^Ab_C^B \\ d_C^{AB}=b_B^Ad_C^B \\ u_C^{AB}=d_B^A+u_B^A+b_B^Au_C^B \end{cases}$$

其中，符号 $\otimes$ 表示推荐算子。

定义 2 设节点 A 和节点 B 对节点 C 的信任评价分别为 $\omega_C^A=\{b_C^A,d_C^A,u_C^A\}$ 和 $\omega_C^B=\{b_C^B,d_C^B,u_C^B\}$，则 A 和 B 对 C 的综合信任评价为 $\omega_C^{A,B}=\omega_C^A\oplus\omega_C^B=\{b_C^{A,B},d_C^{A,B},u_C^{A,B}\}$，并满足：

$$\begin{cases} b_C^{A,B}=(b_C^Au_C^B+b_C^Bu_C^A)/k \\ d_C^{A,B}=(d_C^Au_C^B+d_C^Bu_C^A)/k \\ u_C^{A,B}=u_C^Au_C^B/k \end{cases}$$

其中，$k=u_C^A+u_C^B-u_C^Au_C^B$，u_C^A 和 u_C^B 不能同时为 0，即 $k\neq0$；符号 $\oplus$ 表示合意算子。

3.2 信任描述

TP-SSO 信任模型可描述为一个三元组 $TM=\{E,TR,O\}$。其中，E 表示参与 SSO 的实体集合；TR 表示实体间的信任关系集合；O 表示管理信任关系的操作集合。

定义 3 $TE=\{ID,O,V\}$ 表示一个信任实体，ID 为实体的唯一标识，O 为实体中的 Trust Agent 实施的信任管理操作，V 为存储信任度的信任评估列表。TE 是实体集 E 的子集，可为任意 SSO-P，分为信任者(trustor)和被信任者(trustee)，也将信任者称为评估主体，被信任者称为评估客体。

定义 4 信任关系定义为一个六元组

$TR=\{tr,te,ct,ef,py,tv\}$

其中，tr 和 te 分别表示评估主体和评估客体；ct 表示 tr 和 te 所处的上下文环境；ef 是信任影响因素集 EF 的子集；py 是信任策略集 PY 的子集；tv 表示 tr 对 te 的信任度。

定义 5 $TC=\{DT,RT,IT\}$ 表示信任关系类型，按照实体间建立信任的途径不同，分为直接信任 DT、推荐信任 RT 和间接信任 IT，且 $DT,RT,IT\in TR$。DT 是指主体与客体之间根据过去的直接交互行为而建立的一种信任关系；RT 是指主体与推荐者之间建立的一种信任关系；IT 是指主体与客体之间没有直接交互行为，而是根据推荐者提供的经验推荐信息建立的一种信任关系。

定义 6 $TV=\{DTV, RTV, ITV, OTV\}$ 表示信任度类型，按照信任关系类型不同，分为直接信任度 DTV、推荐信任度 RTV、间接信任度 ITV 和综合信任度 OTV。DTV 是对实体间的直接信任进行评估得出的结果；RTV 是指评估主体对推荐者的信任程度；ITV 是对实体间的间接信任进行评估得出的结果；OTV 是利用权重因子综合直接信任度和间接信任度得出的结果。

定义 7 信任策略定义为一个三元组 $PY=\{to,w,cr\}$。其中，to 表示信任度阈值；$w=\{w_1,w_2,\cdots,w_n\}$ 表示权重因子集合；$cr=\{tv_1,tv_2,\cdots,tv_n\}$ 表示信任度标准集合。

定义 8 信任管理操作定义为一个五元组

$O=\{T_e,T_m,T_a,T_s,T_u\}$

其中，T_e 表示信任建立，确定实体间的信任度初始值；T_m 表示信任监测，监测实体间的交互行为，为信任评估提供原始数据；T_a 表示信任评估；T_s 表示信任存储；T_u 表示信任更新。

3.3 信任评估

直接信任评估是指主体与客体之间存在直接信任关系，无须经过推荐者的信任评估。如图 2 所示，主体 A 与客体 B 之间存在直接交互行为，A 对 B 进行直接信任评估。间接信任评估是指主体与客体之间存在间接信任关系，需经过推荐者的信任评估。如图 3 所示，主体 A 经过推荐者 B 对客体 C 进行间接信任评估，前提是 B 与 C 之间存在直接信任关系。

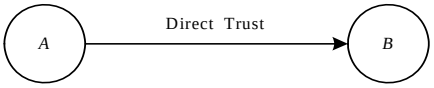

图 2 直接信任评估

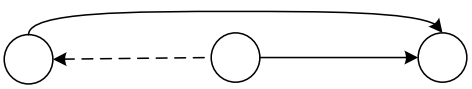

图 3 间接信任评估

3.3.1 直接信任评估

在 TP-SSO 系统中，影响 SSO-P 直接信任评估的因素主要有以下 4 个：(1)节点间的直接交互行为历史，如交互总次数、成功次数和失败次数，该影响因素的权重最大；(2)IDP 提供的身份认证强度；(3)IDP 提供的授权管理质量；(4)SP 提供的应用服务质量。由上述各影响因素确定信任影响因素集 $EF=\{ef_1,ef_2,ef_3,ef_4\}$，再根据 EF 中各子因素对信任评估的不同影响程度确定权重因子集合 $w=\{w_{ef_1},w_{ef_2},w_{ef_3},w_{ef_4}\}$。

信任与实体所处的上下文环境有关，例如 SSO-P 在提供身份认证服务上下文和提供应用服务上下文中具有不同的信任程度。此外，信任会随时间的推移而动态变化，呈现衰减弱化的趋势，即具有时衰性。在指定上下文 c 和当前时刻 t，节点 P_i 对 P_j 的直接信任度 $DTV(P_i,P_j,c,t)$ 可按式(2)计算：

$$DTV(P_i,P_j,c,t)=\sum_{k=1}^{4} w_{ef_k}\omega_{ef_k}\times\psi(t-t_{ij},c) \tag{2}$$

其中，w_{ef_k} 指信任影响子因素 ef_k 在信任评估中所占的权重，且 $\sum_{k=1}^{4} w_{ef_k}=1$；$\omega_{ef_k}=(b_{ef_k},d_{ef_k},u_{ef_k})$ 指子因素 ef_k 对应的信任度。对子因素 ef_k 进行信任监测，若监测结果高于信任策略库中的信任度标准 $py\cdot cr\cdot tv_{ef_k}$，则肯定事件数 r 加 1，否定事件数 s 不变；否则，r 不变，s 加 1。ω_{ef_1} 表示节点 P_i 与 P_j 完成交互活动的信任度，根据交互成功次数和交互失败次数，即肯定事件数 r 和否定事件数 s，信任度 ω_{ef_1} 可按式(1)计算得出；ω_{ef_2} 表示节点 P_i 对 P_j 提供的身份认证强度的信任度；ω_{ef_3} 表示节点 P_i 对 P_j 提供的授权管理质量的信任度；ω_{ef_4} 表示节点 P_i 对 P_j 提供的应用服务质量的信任度。$\psi(t-t_{ij},c)$ 是引入的时间衰减函数，其中，t 指当前时间；t_{ij} 指最近一次交互时间；c 为指定上下文，其值随时间的增加而减少。

3.3.2　间接信任评估

在开放网络环境下，仅通过直接信任评估很难对客体的行为作出全面的判断，还需考虑间接信任评估。间接信任评估主要解决信任传递和信任合并的问题。

信任传递是指将来自推荐者的经验推荐信息传递给评估主体。主体对客体的间接信任取决于：

(1)主体对推荐者的推荐信任；

(2)推荐者对客体的直接信任。

如图 4 所示，主体 A 经过推荐者 B 的推荐与客体 C 建立了间接信任关系。在指定上下文 c 和当前时刻 t，B 作为推荐者，主体 A 对客体 C 的间接信任度为 $ITV(A,C,c,t)=\omega_{i:C}^{A\leftarrow B}=(b_{i:C}^{A\leftarrow B},d_{i:C}^{A\leftarrow B},u_{i:C}^{A\leftarrow B})$；主体 A 对推荐者 B 的推荐信任度为 $RTV(A,B,c,t)=\omega_{r:B}^{A}=(b_{r:B}^{A},d_{r:B}^{A},u_{r:B}^{A})$，$A$ 对 B 的推荐信任度可取 A 对 B 的直接信任度；推荐者 B 对客体 C 的直接信任度为 $DTV(B,C,c,t)=\omega_{d:C}^{B}=(b_{d:C}^{B},d_{d:C}^{B},u_{d:C}^{B})$。使用推荐算子 $\otimes$，主体 A 对客体 C 的间接信任度可按式(3)计算：

$$\omega_{i:C}^{A\leftarrow B}=\omega_{r:B}^{A}\otimes\omega_{d:C}^{B}=(b_{i:C}^{A\leftarrow B},d_{i:C}^{A\leftarrow B},u_{i:C}^{A\leftarrow B}) \tag{3}$$

其中，A 对 B 的推荐信任度 $\omega_{r:B}^{A}$ 和 B 对 C 的直接信任度 $\omega_{d:C}^{B}$ 均可按式(2)计算得出；$b_{i:C}^{A\leftarrow B}=b_{r:B}^{A}b_{d:C}^{B}$，$d_{i:C}^{A\leftarrow B}=b_{r:B}^{A}d_{d:C}^{B}$，$u_{i:C}^{A\leftarrow B}=d_{r:B}^{A}+u_{r:B}^{A}+b_{r:B}^{A}u_{d:C}^{B}$。

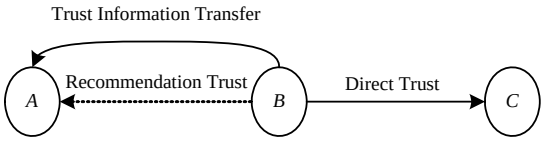

图 4　信任传递

主体对客体的经验可通过推荐者获得，而推荐者提供的经验同样可通过其他推荐者获得，这就形成了一条信任链。

如图 5 所示，$p=\{(A,R_1),(R_1,R_2),\cdots,(R_{n-1},R_n),(R_n,B)\}$ 表示客体 B 到主体 A 的一条信任链，R_n 为信任链的最终推荐者，$R_i(i=1,2,\cdots,n-1)$ 为中间推荐者。$\Phi(p)$ 表示信任链 p 上推荐者的集合，$|\Phi(p)|$ 表示推荐者集合中元素的个数。$D(p)$ 表示信任链 p 上推荐者的个数，则 $D(p)=|\Phi(p)|=n$。θ 表示最大推荐者个数，$\forall p$ 满足 $D(p)\leqslant\theta$，可设置合适的 θ，以控制推荐者的个数。

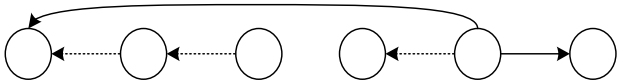

图 5　信任链

在图 5 中，经验推荐信息从推荐者 R_n 到 R_{n-1}，再从 R_{n-1} 到 R_{n-2}，依次传递，最后从 R_1 到主体 A，主体 A 对客体 B 的间接信任度可按式(4)计算：

$$\omega_{i:B}^{A\leftarrow R_n}=\omega_{r:R_1}^{A}\otimes\omega_{r:R_2}^{R_1}\otimes\ldots\otimes\omega_{r:R_n}^{R_{n-1}}\otimes\omega_{d:B}^{R_n} \tag{4}$$

在间接信任评估中，可能存在多条到评估主体的信任链，需将不同信任链提供的推荐信任进行合并。

如图 6 所示，设 A 为评估主体；E_i ($i=1,2,\cdots,n$)为各信任链的最终推荐者；B 为评估客体。在指定上下文 c 和当前时刻 t，A 对 B 的间接信任度为 $ITV(A,B,c,t)=\omega_{i:B}^{A}$；$A$ 对最终推荐者 E_i 的推荐信任度为 $RTV(A,E_i,c,t)=\omega_{r:E_i}^{A\leftarrow E_i}$；$E_i$ 对 B 的直接信任度为 $DTV(E_i,B,c,t)=\omega_{d:B}^{E_i}$；$A$ 从 E_i 处获得的对 B 的间接信任度为 $\omega_{i:B}^{A\leftarrow E_i}$。

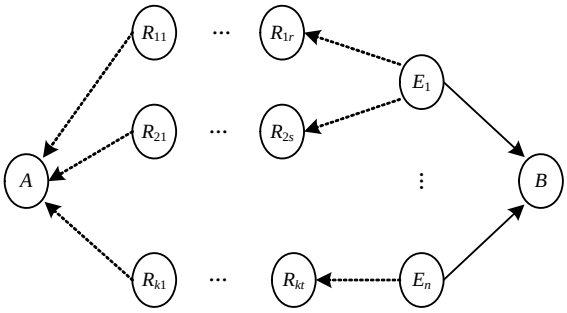

图 6　信任合并

在图 4 中，信任链分为 2 类：(1)以 E_i 为最终推荐者，仅有一条信任链；(2)以 E_i 为最终推荐者，存在多条信任链。对于第(1)类，A 从 E_i 处获得的对 B 的间接信任度 $\omega_{i:B}^{A\leftarrow E_i}$ 可按式(4)计算得出。对于第(2)类，设以 E_i 为最终推荐者的信任链的个数为 m_i，使用合意算子 $\oplus$ 融合源自同一个最终推荐者 E_i 的 m_i 条信任链上的推荐信任度，A 对最终推荐者 E_i 的推荐信任度可按式(5)计算：

$$\omega_{r:E_i}^{A\leftarrow E_i}=\omega_{r:E_{i1}}^{A\leftarrow E_{i1}}\oplus\omega_{r:E_{i2}}^{A\leftarrow E_{i2}}\oplus\ldots\oplus\omega_{r:E_{im_i}}^{A\leftarrow E_{im_i}} \tag{5}$$

求出 A 对 E_i 的推荐信任度 $\omega_{r:E_i}^{A\leftarrow E_i}$ 后，再根据 E_i 对 B 的直接信任度 $\omega_{d:B}^{E_i}$，按式(4)计算得出 A 从 E_i 处获得的对 B 的间接信任度 $\omega_{i:B}^{A\leftarrow E_i}$。

求出以 E_i 为最终推荐者的每类信任链上 A 对 B 的间接信任度后，使用合意算子进行信任合并，A 对 B 的间接信任度可按式(6)计算：

$$\omega_{i:B}^{A}=\omega_{i:B}^{A\leftarrow E_1}\oplus\omega_{i:B}^{A\leftarrow E_2}\oplus\cdots\oplus\omega_{i:B}^{A\leftarrow E_{n-1}}\oplus\omega_{i:B}^{A\leftarrow E_n} \tag{6}$$

3.3.3　综合信任评估

综合信任评估是指主体根据与客体的直接交互行为历史，并根据推荐者提供的间接经验推荐信息，得出对客体的信任度。节点 P_i 对 P_j 的综合信任度取决于 P_i 对 P_j 的直接信

任度和间接信任度，可按式(7)计算：

$$OTV(P_i,P_j,c,t)=\alpha\times DTV(P_i,P_j,c,t)+\beta\times ITV(P_i,P_j,c,t) \quad (7)$$

其中，α 和 β 是权重因子，$\alpha+\beta=1$ $(\alpha,\beta\in[0,1])$，分别表示直接信任度和间接信任度在综合信任评估中所占的权重。α 和 β 的值由各节点根据自己的信任策略设置，通常 $\alpha>\beta$，即 $\alpha>0.5$，因为直接信任比间接信任具有更多的理性成分。

4 TP-SSO应用实例

下面将 TP-SSO 信任模型应用到跨域认证中。开放网络环境中参与 SSO 的各 Web 应用系统都是独立自治的信任域，通过身份联合，各信任域之间能协同工作，实现跨域认证。下面给出一个实例说明 TP-SSO 系统的跨域认证。假设 SSO-P1 和 SSO-P2 属于同一个 SSO-PG，通过 SSO-P1 的信任代理 Trust Agent1 和 SSO-P2 的信任代理 Trust Agent2 已建立信任关系，能进行有效协作。跨域认证如图 7 所示。

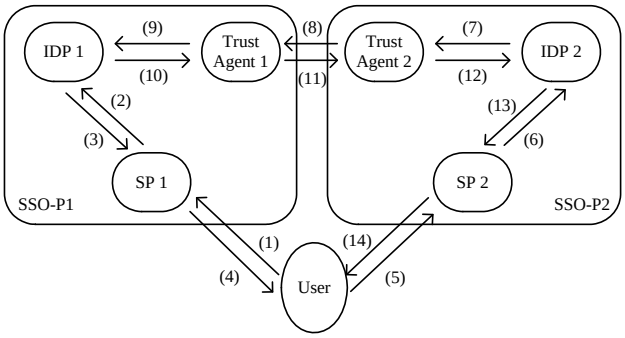

图 7　跨域认证

具体实现过程如下：

(1)用户向 SSO-P1 的服务提供者 SP1 提出服务请求，并进行登录操作。

(2)SP1 将用户的登录信息传递给 SSO-P1 的身份提供者 IDP1，基于身份信任机制 IDP1 对该用户进行身份认证，若认证成功，转到步骤(3)；若认证失败，要求重新登录。

(3)IDP1 验证该用户为合法用户后，将认证结果返回给 SP1，并记录该用户在 SSO-P1 的登录信息，产生一组登录凭证。

(4)SP1 收到 IDP1 返回的认证结果后，回应该用户的服务请求，提供应用服务。

(5)用户携带其登录凭证向 SSO-P2 的服务提供者 SP2 提出服务请求。

(6)SP2 将登录凭证传递给 SSO-P2 的身份提供者 IDP2，并选定由 SSO-P1 提供跨域认证。

(7)IDP2 将登录凭证传递给 SSO-P2 的 Trust Agent2。

(8)Trust Agent2 收到用户信息后，基于行为信任机制计算 SSO-P2 对 SSO-P1 的信任度，若满足身份联合的信任度阈值要求，则向 SSO-P1 的 Trust Agent1 发送跨域认证请求；若不满足，结束跨域认证。

(9)Trust Agent1 收到跨域认证请求后，转发给 IDP1。

(10)IDP1 检验该用户的登录凭证，确认已通过 SSO-P1 的身份认证后，将认证结果回传给 Trust Agent1。

(11)Trust Agent1 将认证结果回传给 Trust Agent2。

(12)Trust Agent2 将认证结果回传给 IDP2。

(13)IDP2 将认证结果返回给 SP2，并记录该用户在 SSO-P2 的登录信息，产生一组登录凭证。

(14)SP2 收到 IDP2 返回的认证结果后，回应该用户的服务请求，提供应用服务。

在进行跨域认证时，若每次都选择 SSO-PG 中信任度较高的 SSO-P 提供服务，会导致节点负载不均衡。在此，可设定信任度阈值，随机选择比阈值高的 SSO-P，避免信任度较高的节点负载过重。

5 结束语

本文针对传统 SSO 在开放网络环境中存在的问题，提出了一个面向信任的对等 SSO 系统架构。信任模型是面向信任的 SSO 的关键，基于主观逻辑，构造了一个较完整的 SSO 信任模型。引入了信任策略和信任影响因素，强调信任的上下文相关性与时衰性，提高了信任评估的准确性。提供了一种行为信任机制，在参与 SSO 的实体间建立了信任关系，实现了有效协作，SSO 不要求集中在某个节点上，克服了单点失效的缺陷。

最后将信任模型应用在跨域认证中，解决了跨域认证的问题，证明了该模型的可行性。由于开放网络环境中参与 SSO 的实体众多且动态变化，因此下一步将研究如何在 2 个陌生实体之间自主建立信任。

参考文献

[1] Iliano C, Aaron D J, Ander S, et al. Specifying Kerberos 5 Cross-realm Authentication[C]//Proc. of the 2005 Workshop on Issues in the Theory of Security. Long Beach, California, USA: ACM Press, 2005: 12-26.

[2] Tuecke S, Welch V, Engert D, et al. Internet X. 509 Public Key Infrastructure Proxy Certificate Profile[EB/OL]. (2004-06-11). http://www.ietf.org/rfc/rfc3820.

[3] Grob T. Security Analysis of the SAML Single Sign-On Browser/Artifact Profile[C]//Proc. of the 19th Annual Computer Security Applications Conference. Washington D. C., USA: IEEE Computer Society, 2003: 298-307.

[4] Abdul-Rahman A, Halies S. A Distributed Trust Model[C]//Proc. of the 1997 Workshop on New Security Paradigms. Cumbria, United Kingdom: ACM Press, 1997: 48-60.

[5] Beth T, Borcherding M, Klein B. Valuation of Trust in Open Networks[C]//Proc. of the European Symposium on Research in Security. Brighton, UK: Springer-Verlag, 1994: 3-18.

[6] Jøsang A, Knapskog S J. A Metric for Trusted Systems[C]//Proc. of the 21st National Security Conference. Wien, Austria: Austrian Computer Society, 1998: 541-549.

编辑　张正兴