

文章编号:1001-9081(2012)03-0686-04

doi:10.3724/SP.J.1087.2012.00686

自动信任协商中环策略依赖检测技术

王 凯^{1,2*}, 张红旗^{1,2}, 任志宇^{1,2}

(1. 信息工程大学 电子技术学院, 郑州 450004; 2. 河南省信息安全重点实验室, 郑州 450004)

(*通信作者电子邮箱 wklwzy057@163.com)

摘要:针对自动信任协商(ATN)可能出现协商过程无限循环的问题,对循环产生的原因进行了分析并设计相应的检测算法以及时发现并终止协商循环。协商双方策略间的依赖关系存在环是无限循环协商产生的原因,将策略间的依赖关系建模成简单图并证明了模型的正确性;分析简单图的可达矩阵计算过程并给出简单图环检测定理,基于该定理设计检测算法对环策略依赖进行检测。最后,通过实例验证了算法的可行性。

关键词:自动信任协商;属性证书;访问控制;环策略依赖;简单图;可达矩阵

中图分类号: TP393.08 文献标志码:A

Cyclic policy interdependency detection in automated trust negotiation

WANG Kai^{1,2*}, ZHANG Hong-qi^{1,2}, REN Zhi-yu^{1,2}

(1. Electronic Technology Institute, Information Engineering University, Zhengzhou Henan 450004, China;

2. Henan Province Key Laboratory of Information Security, Zhengzhou Henan 450004, China)

Abstract: For Automated Trust Negotiation (ATN) consultative process may encounter the infinite cycling problem, the causes of the cycle were analyzed and the corresponding detection algorithm was designed to find and terminate the negotiation cycle. Interdependency relationships among policies in ATN were modeled as simple graph and the model's correctness was proved. The process of calculating simple graph's reachability matrix was analyzed and cycle detection theorem was given. The algorithm of detecting cyclic policy interdependency was designed according to the theorem. Finally, a case study verifies the feasibility of the algorithm.

Key words: Automated Trust Negotiation (ATN); attribute certificate; access control; cyclic policy interdependency; simple graph; reachability matrix

0 引言

在分布协同环境^[1]下,资源请求者和资源提供者通常由分属不同安全域^[2]的权威控制,资源提供者不能根据外域请求者身份制定访问控制策略^[3]。Winsborough 等^[4]提出了自动信任协商(Automated Trust Negotiation, ATN),通过在不同安全域间交互披露属性证书^[5]而使协商双方建立起相互信任关系,较好地解决了分布协同环境下的跨域资源访问^[6]问题。

然而,文献[7]指出由于协商者分别独立制定访问控制策略,协商过程中可能出现策略循环依赖,使得协商过程出现死锁^[8],导致协商无法正常终止。为了解决该问题,该文提出了一种不经意的基于签名信封方案,该方案通过公钥密码^[9]框架构造信封解决了环策略依赖造成的死锁,但对不存在环的协商过程将造成不必要的开销。文献[10]通过化简策略树的方法计算协商需要的最小证书集^[11]并对其进行一次性披露来消解环策略依赖,但文中仅给出一个必然存在环策略依赖的实例,缺乏对该问题的精确描述及相应的检测方法。文献[12]提出了一种基于契约的信任协商,该方法在协商之前限定协商次数,可以终止协商的无限循环,然而对于协商次数的设定很难取舍,如果取值较大,则可能在较早的情况下

出现环策略依赖而导致无效的协商产生;如果取值较小,可能导致存在成功信任协商的情况下提前终止协商。综上所述,虽然环策略依赖问题在现有文献中有所体现,但均没有针对自动信任协商中的环策略依赖问题给出一种有效的检测方法。

本文对自动信任协商中环策略依赖问题进行形式化描述,通过计算简单图的可达矩阵推导出简单图中是否存在环的定理,将信任协商中策略之间的依赖关系建模成为简单图并证明了模型的正确性,通过判断简单图中是否存在环的定理对自动信任协商的环策略依赖问题进行检测,给出了相应的算法并通过实例验证了方案的正确性。

1 自动信任协商中环策略依赖的数学描述

在自动信任协商中,资源请求者 Requester 发起对资源 R 的访问请求后,资源提供者要求资源请求者提供足够的证书以满足资源 R 的访问控制策略。然而,为了保护证书中的敏感信息^[13],资源请求者也通过制定访问控制策略要求服务提供方出示相应的属性证书证明其能力。经过多轮协商,直到某一方的证书不需要任何访问控制策略保护并能满足对方的访问控制需求时,协商成功;在协商过程中,若某一方不能提供满足对方访问控制策略足够的证书,则协商失败。

收稿日期:2011-09-01;修回日期:2011-11-18。 基金项目:国家 863 计划项目(2006AA01Z457, 2009AA01Z438);国家 973 计划项目(2011CB311801);河南省科技创新人才计划项目(114200510001)。

作者简介:王凯(1987-),男,四川射洪人,硕士研究生,主要研究方向:信任协商、访问控制; 张红旗(1962-),男,河北遵化人,教授,博士生导师,博士,主要研究方向:等级保护、信任管理、网络安全; 任志宇(1974-),女,河南汤阴人,讲师,博士研究生,主要研究方向:授权管理、访问控制。

因此,在自动信任协商中,证书和服务都被称为受保护的资源,并通过资源拥有者制定相关的访问控制策略实施保护。为了形式化描述自动信任协商环策略依赖问题,本文给出如下定义^[14]。

定义1 满足。如果证书集 C 中所提供的属性及相应的属性值能够使策略表达式 P 的取值为真,则称证书集 C 满足访问控制策略 P ,记为 $Sat(P, C)$,本文称证书 C 为策略 P 的一个属性证书解。

定义2 锁定。对于要保护的资源 $Object$ (资源 R 或证书 C),由其拥有者制定相应的访问控制策略 P 来实施保护,则称策略 P 将资源 $Object$ 进行“锁定”,记为 $lock(Object, P)$ 。

定义3 解锁。对于由策略 P 锁定的资源 $Object$,有 $lock(Object, P)$,如果资源请求方所提交的属性证书集 C 满足 $Sat(P, C)$,则称请求方提交的证书集 C 解锁资源 $Object$,记为 $unlock(Object, C)$ 。特别地,如果资源 $Object$ 不需要任何策略 P 保护时,则证书集 \emptyset 解锁 $Object$,记为 $unlock(Object, \emptyset)$ 。

定义4 自动信任协商。自动信任协商可被形式化为一个证书披露序列 $\{C_i\}_{i \in [0, 2n+1]} = C_0, C_1, \dots, C_{2n+1}$ ($n \in \mathbb{N}$)。其中, n 表示信任协商的轮数。 $C_j \subseteq ClientCreds$ ($0 \leq j \leq n$) 表示客户端的属性证书披露, $C_{j+1} \subseteq ServerCreds$ ($0 \leq j \leq n$) 表示服务端的属性证书披露。

对于一次信任协商,如果协商双方通过一系列的属性证书披露最终使得资源请求者获得资源 R 的访问权限,则称之为一次成功的信任协商。在实际运行中,并不是每次协商都能成功获得资源的访问权限,本文给出满足成功信任协商的充分条件如下。

定理1 满足成功信任协商的充分条件。若协商双方在协商过程中建立起一个证书披露序列 $\{C_i\}_{i \in [0, 2n+1]} = C_0, C_1, \dots, C_{2n+1}$ ($n \in \mathbb{N}$),满足 $unlock(C_0, \emptyset)$ 且 $unlock(C_{j+1}, C_j)$, $0 \leq j \leq 2n$, 则经过此次协商,资源请求者能够获得资源 R 的访问权限。

然而,并不是在每次协商过程中都一定能找到满足定理1的一条证书披露序列。特别是当协商双方策略存在环策略依赖时,将会出现死锁,导致协商无法正常终止。文献[7]给出了协商过程中出现环策略依赖的一个具体场景: Alice 和 Bob 均属于某保密组织的成员并拥有保密组织为他们颁发的证书。为了保护自身身份,他们都仅向其他拥有组织颁发证书的成员出示其证书。如果 Alice 和 Bob 需要利用自动信任协商建立安全会话连接,那么他们都不会首先出示自己的属性证书,从而导致死锁而不能成功建立会话。因此,本文给出环策略依赖的定义如下。

定义5 环策略依赖。对于一次自动信任协商 $\{C_i\}_{i \in [0, 2n+1]} = C_0, C_1, \dots, C_{2n+1}$ ($n \in \mathbb{N}$)。如果存在 C_i 和 C_j ,使得 $unlock(C_n, C_i) \wedge unlock(C_0, C_i) \wedge \dots \wedge unlock(C_j, C_{i_k}) \wedge unlock(C_i, C_j)$ 成立,导致两个证书集 C_i 和 C_j 彼此直接或间接需要对方进行解锁时,则称自动信任协商出现环策略依赖,记为 $LoopPolicy(C_i, C_j)$ 。其中, $0 \leq i, i_1, i_2, \dots, i_k, j \leq 2n + 1$ 且两两互不相等。

如果自动信任协商中协商双方策略存在环策略依赖,将会导致协商过程无限循环,并且因为不能满足定理1中 $unlock(C_0, \emptyset)$ 条件而导致协商失败。因此,需要有一种方法能够及时检测出协商过程出现的环策略依赖,及时终止不成功的信任协商。

2 基于可达矩阵的环检测定理

为了进行环策略依赖检测,本文将其检测过程归结为计算可达矩阵对角线是否存在元素值为1的过程。下面首先参考文献[15~16]给出可达矩阵的基本概念及计算方法,在此基础上利用可达矩阵给出环检测相关定理。

2.1 可达矩阵算法简介

定义6^[15] 设 $G = \langle V, E \rangle$ 是简单图,即无自回路且不含平行边的图^[16],其中 $V = \{v_1, v_2, \dots, v_n\}$, v_1, v_2, \dots, v_n 表示图 G 的 n 个节点。矩阵 $A = (a_{ij})_{n \times n}$ 为其对应的邻接矩阵,其中

$$a_{ij} = \begin{cases} 1, & v_i \text{ 邻接 } v_j \\ 0, & \text{其他} \end{cases}$$

因图 G 无自回路,故 $a_{ii} = 0$ 。邻接矩阵的意义在于能够精确描述简单图中各节点之间的直接依赖关系。

定义7^[15] 在简单图 $G = \langle V, E \rangle$ 中, $V = \{v_1, v_2, \dots, v_n\}$ 。矩阵 $P = (p_{ij})_{n \times n}$ 为其对应的可达矩阵。其中

$$p_{ij} = \begin{cases} 1, & v_i \text{ 与 } v_j \text{ 之间至少存在一条通路} \\ 0, & \text{其他} \end{cases}$$

可达矩阵的意义在于能够精确描述简单图中各节点之间所有直接和间接依赖关系。

为了便于清晰地描述和分析从邻接矩阵计算可达矩阵的计算过程,给出如下定义。

定义8^[15] 以二阶布尔代数 $\{0, 1\}, \wedge, \vee, \neg; 0, 1\}$ 的元素为元素的矩阵称为布尔矩阵。设 $A = (a_{ij})_{n \times n}, B = (b_{ij})_{n \times n}$ 均为 n 阶布尔矩阵,定义矩阵的布尔积运算“.”和布尔和运算“ \vee ”如下:

- 1) $A \cdot B = S, s_{ij} = \bigvee_{k=1}^n (a_{ik} \wedge b_{kj});$
- 2) $A \vee B = M, m_{ij} = a_{ij} \vee b_{ij};$
- 3) $A^{(2)} = A \cdot A, a_{ij}^{(2)} = \bigvee_{k=1}^n (a_{ik} \wedge a_{kj});$
- 4) $A^{(n)} = A^{(n-1)} \cdot A.$

其中:对于矩阵中每一个元素“0,1”的运算“ \vee ”和“ \wedge ”分别表示取大和取小运算。

文献[16]给出可达矩阵的常用求法:

$$P = I \vee A \vee A^{(2)} \vee \dots \vee A^{(n)}$$

其中: I 为 n 阶单位矩阵, $A = (a_{ij})_{n \times n}$ 为简单图 $G = \langle V, E \rangle$ 的邻接矩阵。

2.2 基于可达矩阵的环检测定理

可达矩阵可以清晰地表达简单图中各节点之间的所有直接和间接依赖关系。然而,可达矩阵并不能直接用来进行环策略依赖检测,下面通过对计算过程进行分析并给出简单图中是否存在环的定理。

对于一个具有 n 个节点的简单图 G ,其邻接矩阵 $A = (a_{ij})_{n \times n}$ 的数学意义在于表示了节点之间的直接依赖关系,本文称其为节点与节点之间经过 1 步的可达性描述。对于矩阵 $A^{(2)} = A \cdot A$ 中的每一个元素 $a_{ij}^{(2)} = \bigvee_{k=1}^n (a_{ik} \wedge a_{kj})$,使其

为 1 的充分条件是简单图内至少存在一个节点 k ,使得节点 i 到 k 经 1 步可达且节点 k 到 j 经 1 步可达。因此, $A^{(2)}$ 的数学意义在于表示节点与节点之间通过 2 步的可达性描述。类似地, $A^{(k)}$ 表示简单图中节点与节点之间经过 k 步的可达性描述。

因此,在不考虑单位矩阵 I ,即节点自身到自身可达的情

况下,对于一个有 n 个节点的简单图 G ,可以得到其可达性矩阵计算公式为 $\mathbf{P} = \bigvee_{k=1}^n \mathbf{A}^{(k)}$,对于矩阵 \mathbf{P} 中的每个元素 p_{ij} ,使其为 1 的充要条件是至少存在一个 $a_{ij}^{(k)} = 1, 1 \leq k \leq n$ 。其意义在于对简单图 $G = \langle V, E \rangle$,节点 i 到节点 j 可达的充要条件是 i 到 j 经过 1 步或多步可达。

定理2 简单图 $G = \langle V, E \rangle$ 拥有 n 个节点,其对应的邻接矩阵为 $\mathbf{A} = (a_{ij})_{n \times n}$,计算 G 的可达性矩阵 $\mathbf{P} = \bigvee_{k=1}^n \mathbf{A}^{(k)}$,若有 $\bigvee_{i=1}^n p_{ii} = 1$,那么简单图 G 中至少存在一个节点使得该节点自身到自身间接可达,即简单图 G 中存在环。

证明 由于简单图 $G = \langle V, E \rangle$ 是不存在自回路的图,那么 G 中不可能存在自身到自身 1 步可达的节点。当 $\bigvee_{i=1}^n p_{ii} = 1$ 时,图 G 中至少存在一个自身到自身经过 $k (2 \leq k \leq n)$ 步间接可达节点,因此简单图 G 中存在环。

定理2给出了求解一个简单图中是否存在环的数学描述,为自动信任协商中环策略依赖检测提供了理论基础。

3 自动信任协商中环策略依赖检测方法

为解决第1章中提出的自动信任协商环策略依赖检测问题,结合定理2对检测简单图中是否存在环的数学描述,如果能够将自动信任协商过程中的环策略依赖建模成为一个简单图,那么通过计算其可达矩阵对角线上是否存在值为 1 的元素即可有效实现环策略依赖检测。

3.1 自动信任协商策略直接依赖关系简单图建模

为了对自动信任协商过程中的环策略依赖进行检测,首先需要将自动信任协商过程中的策略依赖建模成为简单图。依据定义4,本文将一次证书披露序列中的属性证书集 $\{C_i\}_{i \in [0, 2n+1]} = \{C_2\} \cup \{C_{2j+1}\} (0 \leq j \leq n)$ 转化为简单图中的 $2n+2$ 个节点,将 $\{C_i\}_{i \in [0, 2n+1]}$ 中证书之间的直接解锁关系 $\{\text{unlock}\}_{|C_i|}$ 转化为简单图中的边,得到自动信任协商策略依赖的简单图 \mathbf{G}_{ATN} 。

定义9 自动信任协商策略依赖图形化表示。 $\mathbf{G}_{\text{ATN}} = \langle \{C_i\}_{i \in [0, 2n+1]}, \{\text{unlock}\}_{|C_i|} \rangle$ 为自动信任协商策略依赖简单图,其中 $\{C_i\}_{i \in [0, 2n+1]}$ 为 \mathbf{G}_{ATN} 的顶点集,表示一次自动信任协商过程中所有被披露的证书集合, $\{\text{unlock}\}_{|C_i|}$ 为 \mathbf{G}_{ATN} 的边集,表示 $\{C_i\}$ 之间的直接解锁关系。

定理3 \mathbf{G}_{ATN} 为一简单图。

证明 根据文献[16]关于简单图的定义,无自回路且不含平行边的图称为简单图。由于直接解锁关系涉及到的两个证书 C_i, C_j 必然分属于客户端和服务端证书,图 \mathbf{G}_{ATN} 中不会出现自身直接依赖于自身的节点, \mathbf{G}_{ATN} 不包含自回路。对于 \mathbf{G}_{ATN} 中的边集 $\{\text{unlock}\}_{|C_i|}$,由于其不可能出现两个相同的元素, \mathbf{G}_{ATN} 不会出现平行边。因此, \mathbf{G}_{ATN} 为一简单图。

本文将图 \mathbf{G}_{ATN} 对应的邻接矩阵记为 $\mathbf{A}_{\text{ATN}} = (a_{ij})_{(2n+2) \times (2n+2)}$,其中:

$$a_{ij} = \begin{cases} 1, & \text{unlock}(C_j, C_i), 0 \leq i, j \leq 2n+1 \text{ 且 } i \neq j \\ 0, & \text{其他} \end{cases}$$

3.2 基于可达矩阵的环策略依赖检测算法

通过对自动信任协商策略依赖简单图建模获得协商双方证书与证书之间直接依赖关系的邻接矩阵,结合第2章可达

矩阵计算相关知识,计算 \mathbf{A}_{ATN} 的可达矩阵 $\mathbf{P}_{\text{ATN}} = \bigvee_{k=1}^{2n+2} (\mathbf{A}_{\text{ATN}})^{(k)}$,其中:

$$p_{ij} = \begin{cases} 1, & \text{unlock}(C_{il}, C_i) \wedge \text{unlock}(C_{il}, C_{il}) \wedge \cdots \wedge \text{unlock}(C_j, C_{ik}) \\ 0, & \text{其他} \end{cases}$$

其中: $C_i, C_{il}, C_{il}, \dots, C_{ik}, C_j$ 均为证书披露序列中的证书,并且两两互不相等。

文献[15]利用逐次平方法给出了一种快速计算可达矩阵的方法,然而该方法将单位矩阵也加入到邻接矩阵,即节点自身依赖于自身解锁的初始条件,其并不适合用来进行环策略依赖检测。因而,只能通过逐步计算 $(\mathbf{A}_{\text{ATN}})^k = (\mathbf{A}_{\text{ATN}})^{k-1} \cdot (\mathbf{A}_{\text{ATN}})$ 计算出 \mathbf{P}_{ATN} (其中 $2 \leq k \leq 2n+2$),再根据定理2判断 $\bigvee_{i=1}^{2n+2} p_{ii}$ 是否等于 1 确定自动信任协商过程中是否出现环策略依赖。计算算法如下:

算法1 基于可达矩阵的环策略依赖检测算法。

输入 协商双方证书与证书之间直接依赖关系的邻接矩阵 $\mathbf{A}_{\text{ATN}} = (a_{ij})_{(2n+2) \times (2n+2)}$ 。

输出 是否出现环策略依赖(True/False)。

```

1) Let  $\mathbf{P}_{\text{ATN}} = \mathbf{A}_{\text{ATN}}$ 
2) Let  $\mathbf{Temp} = \mathbf{A}_{\text{ATN}}$ 
3) Let  $N = |\mathbf{A}_{\text{ATN}}|$  // 矩阵  $\mathbf{A}_{\text{ATN}}$  的阶数  $2n+2$ 
4)  $Flag = \text{false}$ 
5) Let  $i = 1$ 
6) while( $i < N$ )
7)    $\mathbf{Temp} = \mathbf{Temp} \cdot \mathbf{A}_{\text{ATN}}$  // 矩阵的布尔积运算
8)    $\mathbf{P}_{\text{ATN}} = \mathbf{P}_{\text{ATN}} \vee \mathbf{Temp}$  // 矩阵的布尔和运算
9)    $i = i + 1$ 
10) End-while
11) For each  $p_{ii}$  in  $\mathbf{P}_{\text{ATN}}$ 
12)   if ( $p_{ii} == 1$ )
13)     {  $Flag = \text{true}$ ; break; }
14) End-for
15) return  $Flag$ 
```

第1) ~ 10) 行计算环策略依赖检测的可达矩阵 $\mathbf{P}_{\text{ATN}} =$

$\bigvee_{k=1}^N (\mathbf{A}_{\text{ATN}})^{(k)}$,第11) ~ 15) 行计算该可达矩阵对角线上是否存在值为 1 的元素。下面将对该算法的时间复杂度和空间复杂度分别进行分析。

时间复杂度 算法第6) ~ 10) 行执行 N 次 while 循环,其中每次循环执行矩阵的布尔积和布尔和运算各一次,一次布尔积运算的时间复杂度为 $O(N^3)$,一次布尔和运算的时间复杂度为 $O(N^2)$,则求解可达矩阵的时间复杂度为 $O(N * (N^3 + N^2))$,算法第11) ~ 14) 行平均执行 $N/2$ 次循环检测可达矩阵对角线是否存在 1。算法1的总时间复杂度为 $O(N^4 + N^3 + N/2)$ 。

空间复杂度 算法中主要定义两个 $N \times N$ 的矩阵 \mathbf{P}_{ATN} 和 \mathbf{Temp} ,其空间复杂度为 $O(2 * N^2)$ 。

算法1严格按照定理2计算出图 \mathbf{G}_{ATN} 的可达矩阵并判断是否出现环策略依赖。事实上,为了检测一个简单图中是否存在环,可能并不需要完全计算出其可达矩阵。例如,对于一个 N 阶矩阵,如果 $\mathbf{A}_{\text{ATN}}^{(2)}$ 中出现 $a_{ii}^{(2)} = 1$,则已经可以判断自动信任协商出现环策略依赖并且环的路径长度为 2。因此,给出定理2的改进定理如下。

定理4 简单图 $G = \langle V, E \rangle$ 拥有 n 个节点,其对应的邻接

矩阵为 $A = (a_{ij})_{n \times n}$, 若对于 C 的 k 步可达矩阵 $A^{(k)}$ 有 $\bigvee_{i=1}^n a_{ii}^{(k)} = 1$, 则简单图 G 中存在环并且该环的路径长度为 k 。

根据定理 4, 可将算法 1 作如下改进:

算法 2 改进后的可达矩阵环策略依赖检测算法。

输入 协商双方证书与证书之间直接依赖关系的邻接矩阵 $A_{ATN} = (a_{ij})_{(2n+2) \times (2n+2)}$ 。

输出 是否出现环策略依赖(True/False)。

```

1) Let  $\text{Temp} = A_{ATN}$ 
2) Let  $N = |A_{ATN}|$  // 矩阵  $A_{ATN}$  的阶数  $2n + 2$ 
3) Let  $i = 1$ 
4) while( $i < N$ )
5)    $\text{Temp} = \text{Temp} \cdot A_{ATN}$  // 矩阵的布尔积运算
6)   For each  $t_{ii}$  in  $\text{Temp}$ 
7)     if ( $t_{ii} = 1$ )
8)       return true
9)   End-for
10)   $i = i + 1$ 
11) End-while
12) return false

```

算法 2 并不计算 A_{ATN} 的可达矩阵, 而是逐一计算 A_{ATN} 的 2 至 N 步可达矩阵, 如果其 K 步可达矩阵 ($2 \leq K \leq N$) 出现了环, 则直接返回 True。下面对其时间复杂度和空间复杂度分别进行分析。

时间复杂度 算法 2 平均执行 $N/2$ 次 while 循环, 对于每一次循环, 做一次布尔积运算并判断是否出现环, 其复杂度为 $O((N^3 + N/2) * N/2) = O(N^4/2 + N^2/4)$ 。

空间复杂度 算法中仅定义一个 $N \times N$ 的矩阵 Temp , 其空间复杂度为 $O(N^2)$ 。

相对算法 1, 算法 2 在空间复杂度略优于算法 1。从统计的角度, 由于当 $N \geq 1$ 时, $(N^4 + N^3 + \frac{N}{2}) - (\frac{N^4}{2} + \frac{N^2}{4}) > 0$ 恒成立, 算法 2 的时间复杂度也低于算法 1, 但是在最坏的情况下, 如计算到 $A_{ATN}^{(N)}$ 时才检测出环策略依赖, 算法 2 由于多进行了 $N-1$ 次环判断, 其时间复杂度将高于算法 1。然而, 由于并不能事先知道经过几轮协商将会出现环策略依赖, 从统计的角度讲, 本文推荐在实际应用中采用算法 2。

4 实例分析

一次自动信任协商中客户端欲访问服务端的资源 R , 客户端拥有的属性证书集合为 $\{C_0, C_2, C_4, C_6\}$, 服务端拥有的属性证书集合为 $\{C_1, C_3, C_5, C_7 = R\}$, 为了获取资源 R 的访问权限, 双方通过逐步向对方披露满足访问控制策略的属性证书来获得资源的访问权限。图 1(a) 为一次自动信任协商策略依赖的简单图 G_{ATN} , 其中的边表示客户端和服务端证书之间的解锁关系(如边“ $C_1 \rightarrow C_2$ ”表示服务端要想获得 C_2 的访问权限, 必须先向客户端出示自己的证书 C_1)。图 1(b) 为其对应的邻接矩阵 A_{ATN} 。

为了验证算法 1 和算法 2 的有效性, 本文以 Visual Studio 2008 为开发平台, C# 为开发语言实现了求解矩阵 A_{ATN} 的任意 N 阶矩阵及其可达矩阵的计算过程。鉴于篇幅所限, 这里只给出 A_{ATN} 的可达矩阵和对角线上首次出现元素值为 1 的幂矩阵, 程序运行结果如下所示。

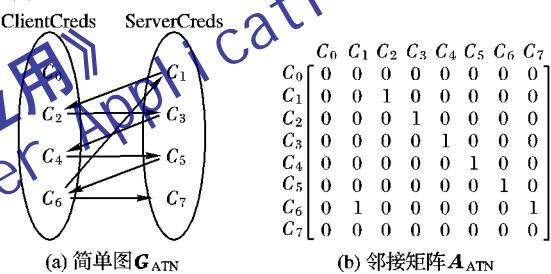
可达矩阵 P_{ATN} :

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

矩阵 A_{ATN} 的 6 次幂:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

由于 A_{ATN} 的可达矩阵 P_{ATN} 及 6 次幂矩阵对角线上均出现值为 1 的元素, 算法 1 和算法 2 的运行结果均为 True, 说明本次自动信任协商出现环策略依赖, 应采取相应的机制及时终止协商的无限循环。



(a) 简单图 G_{ATN} (b) 邻接矩阵 A_{ATN}

图 1 自动信任协商策略依赖图

5 结语

本文针对自动信任协商出现环策略依赖导致协商循环无法终止的问题, 设计并实现了相应的环策略依赖检测算法。首先对环策略依赖问题进行数学描述并通过求解一个简单图的可达矩阵计算过程进行分析, 将该问题转化为求解一个可达矩阵对角线上是否出现元素值为 1 的数学问题。随后, 将自动信任协商过程建模成为简单图并设计了相应的环策略依赖检测算法。最后通过实例验证了算法的正确性和有效性。然而, 由于算法 1 和算法 2 的时间复杂度都随着矩阵 A_{ATN} 的阶数呈指数增长, 如何对算法进行改进是有待进一步研究的问题。

参考文献:

- [1] 朱贤, 邢光林, 洪帆. 分布式环境下的访问控制综述[J]. 微型机与应用, 2005, 24(1): 4–7.
- [2] 马晓宁, 冯志勇, 徐超. Web 服务中跨安全域的基于信任的访问控制模型[J]. 计算机应用研究, 2009, 26(12): 4571–4573.
- [3] 汪应龙, 胡金柱. 自动信任协商中一种策略一致性管理方法[J]. 计算机应用, 2008, 28(7): 1795–1797.
- [4] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation [C]// Proceedings of DARPA Information Survivability Conference and Exposition. Piscataway, NJ: IEEE Press, 2000: 88–102.
- [5] FERRALL S. RFC3281, An Internet attribute certificate profile for authorization[S], 2000.

(下转第 693 页)

朋友网首先应该明确与QQ空间的关系,明确各自的定位。对于用户在朋友网上发布的照片和日志,不应该直接同步至QQ空间,至少应该让用户自己选择是否同步。单个相册和单篇日志应该提供单独的隐私控制,让用户可以控制到单个相册和单篇日志能被什么样的人看到。对于那些不需要细粒度控制的动态信息,如留言板、分享和好友列表等,均应该在各自的维护界面上提供分散式的隐私控制入口。

3.2 黑名单功能

黑名单功能是一种较强的隐私控制手段,用户可以利用该功能禁止别人对自己所有信息的访问权限,包括禁止查看自己所有的个人信息,禁止别人搜索自己,甚至禁止别人向自己发出好友请求。就黑名单功能而言,朋友网的可用性远远不如人人网。根据实验数据,人人网黑名单设置任务的完成率是83.3%,而朋友网黑名单设置任务的完成率仅为58.3%,这严重影响了朋友网的平均任务完成率。首先,朋友网黑名单功能的实现方式单一,只有通过点击对方主页左下角的“加入黑名单”链接来实现。其次,朋友网中对于黑名单功能实现方式的解释也比较模糊,且不准确。解释中提到可以点击对方主页左下角的禁止图标实现该功能,但事实上对方主页左下角根本没有这个禁止图标,用户很容易被误导,因为用户更倾向于寻找那个禁止图标。

建议朋友网的黑名单功能除了目前的实现方式之外,应该在该功能项的界面上增加输入框,允许用户直接输入需要加入黑名单的用户名,因为这种方式更为直接和简单。此外,朋友网应该改变并纠正其对黑名单功能的解释,利用图标确实是一个很好的方式,朋友网应该在个人主页上“加入黑名单”链接之前加上图标,以方便用户快速找到该项功能。

4 结语

社交网络的不断普及和应用,使得人们的个人信息和在线行为非常详细地展现在互联网上,这些信息如果不能得到有效的保护和控制,一旦泄露将会给用户带来严重的伤害和困扰。尽管社交网络都提供了隐私控制功能,但这些功能的可用性不太理想,影响了用户隐私保护的效果。本文通过科学实验和访谈获得定量数据,对比研究人人网和朋友网这两个社交网络隐私控制功能的可用性,发现朋友网隐私控制功能的总体可用性比人人网稍好,但两者之间没有显著的差异,均存在较大的改进空间。如,人人网需改进其隐私控制功能的集中式导航设计,并需更加合理地设计其集中的隐私设置界面;而朋友网应更加关注其隐私控制功能分散式导航的设计。

(上接第689页)

- [6] 戴常英,张会娟.基于信任度的Web服务跨域访问控制[J].计算机工程与科学,2009,31(8):42-45.
- [7] LI N H, DU W, BONEH D. Oblivious signature-based envelope [C]// Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 2003: 182-189.
- [8] 卢超,卢炎生,谢晓东,等.一种基于依赖分析的并发程序潜在死锁检测算法[J].小型微型计算机系统,2007,28(5):841-844.
- [9] RFC2459, Internet X.509 public key infrastructure certificate and CRL profile[S], 2000.
- [10] 夏冬梅,曾国荪,陈波,等.基于标签树的自动信任协商策略分析[J].计算机科学,2009,36(12):154-158.
- [11] YU T, WINSLETT M. A unified scheme for resource protection in automated trust negotiation[C]// Proceedings of the 2003 Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2003:

计,厘清其与QQ空间的关系,完善隐私控制功能,还应该改进其黑名单的设置功能。本研究成果可在理论和实践的层面为社交网络隐私控制功能的设计和实现提供参考建议,有助于提高社交网络隐私控制功能的可用性,从而帮助用户更好地保护隐私信息。

参考文献:

- [1] 胡启平,陈霞.试析社交网络环境中个人隐私保护[J].信息网络安全,2010(8):43-44.
- [2] 李响.社交网站:开放中隐藏危险[J].信息网络,2008(6):56-57.
- [3] NARENDULA R, PAPAOANNOU T G, ABERER K. Privacy-aware and highly-available OSN profiles[C]// WETICE'10: Proceedings of the 2010 19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises. Piscataway, NJ: IEEE Press, 2010: 211-216.
- [4] DEBATIN B, LOVEJOY J P, HORN A K, et al. Facebook and online privacy: attitudes, behaviors, and unintended consequences [J]. Journal of Computer-Mediated Communication, 2009, 15(1): 83-108.
- [5] International Organizational for Standardization. ISO 9241-11, Ergonomic requirements for office work with visual display terminals (VDTs): Part 11: Guidance on usability. Switzerland: International Organizational for Standardization, 1998.
- [6] 张丽霞,梁华坤,傅烟,等.鱼眼菜单可用性研究[J].计算机工程与设计,2011,32(2):706-710.
- [7] 李倩,孙林岩,吴疆,等.个人网上银行的可用性测试与评价[J].工业工程与管理,2008(6):99-102,113.
- [8] 张喆,毛基业.网上银行可用性测评[J].信息系统学报,2008,2(1):55-65.
- [9] 葛列众,王宇轩,王琦君.电子信箱的可用性实验研究[J].人类工效学,2010,16(1):9-13.
- [10] 董旭.2011年Q1中国SNS市场活跃账户份额[EB/OL].[2011-07-20].<http://www.eguan.cn/cache/1338/101878.html>.
- [11] LEE S, KOUBEK R J. The effects of usability and Web design attributes on user preference for e-commerce Web sites[J]. Computers in Industry, 2010, 61(4): 329-341.
- [12] NIELSEN J. 可用性工程[M].刘正捷,译.北京:机械工业出版社,2004.
- [13] ZHELEVA E, GETOOR L. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles [C]// WWW'09: Proceedings of the 18th International World Wide Web. New York: ACM Press, 2009: 531-540.

245-257.

- [12] 李建欣,怀进鹏. COTN: 基于契约的信任协商系统[J].计算机学报,2006,29(8):1290-1330.
- [13] WINSBOROUGH W H, LI N H. Protecting sensitive attributes in automated trust negotiation[C]// Proceedings of the ACM Workshop on Privacy in the Electronic Society. New York: ACM Press, 2002: 41-51.
- [14] YU T, WINSLETT M, SEAMONS K E. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation[J]. ACM Transactions on Information and System Security, 2003, 6(1):1-42.
- [15] 杨秀文,严尚安,曾顺鹏,等.关于可达矩阵的求法探讨[J].数学的实践与认识,2003,33(11):128-130.
- [16] 方世昌.离散数学[M].2版.西安:西安电子科技大学出版社,2006: 87-100,266-267.