基于可信敏感度的网格信任协商策略及其应用分析

杨明慧,王汝传
(南京邮电大学计算机学院,江苏南京 210003)

摘 要: 本文将证书敏感度和实体声誉相结合,提出基于可信敏感度的信任协商策略来避免敏感信息的披露;引入协商第三方来解决循环依赖策略,提高服务成功率.最后分析了策略的计算和通信开销,在 NUPT 网格平台的测试结果证实了该策略性能令人满意.

关键词: 网格自动信任协商; 协商策略; 可信敏感度; 协商第三方
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2010) 02-0422-05

Trusted Sensitivity Improved Trust Negotiation Strategy and Its Application Analysis for Grid Service

YANG Ming-hui, WANG Ru-chuan
(*College of Computing, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu* 210003, *China*)

Abstract: The paper proposes a trusted sensitivity improved negotiation strategy, which is orthogonal to credentials' sensitivity and entity's reputation. Such modifications help prevent inadvertent disclosure of sensitive information. We also introduce negotiation third parties to solve cyclic dependent policies, which effectively promote the response ratio of grid services request. Its practical performance was validated on NUPT-grid platform, and the results are satisfactory.

Key words: grid automated trust negotiation; negotiation strategy; trusted sensitivity; negotiation third party

1 引言

自动信任协商中为保护敏感资源,需使用披露策略逐步地公布证书和策略的条件,来避免敏感信息泄露[1].信任协商策略规定了证书交换中敏感属性的流向,在协商中控制着交换消息的内容,如披露哪些证书,什么时候披露以及什么时候结束[2].目前该领域的研究集中在策略保护[3~5],防止属性泄漏[6,7]等.但为提高协商成功率而放弃使用实际上有效的敏感证书,不能充分保护协商各方的隐私性.本文将证书敏感度和声誉相结合,定义可信敏感度来反映声誉对披露证书敏感度的影响;引入协商第三方(Negotiating Third Party, NTP)来解决循环依赖策略问题.基于以上措施提出可信敏感度策略,并分析了策略的计算和通信开销,在南京邮电大学网格平台(NUPT-grid)上实施该策略进行验证.

2 基于可信敏感度的信任协商策略

考虑到恶意实体可能会构建策略强迫其他实体向其披露更多不必要证书和信息,所以本文根据敏感性驱动来披露相应策略和证书.

2.1 相关定义

协商过程涉及的每个实体都拥有其协商策略 P,它是一系列规则的集合.规则由证书 $C_1, C_2, \cdots, C_k$ 的布尔表达式、布尔常量(true/false)和布尔算子($\wedge/\vee$)组成.表示为 $C = \{id, issuer, content, sensitivity, validtime\}$,分别代表证书的身份、发布者、内容、敏感性和有效期,$C.id$ 简写为 C_i.如资源 R 的策略 P: $R \leftarrow C_1 \wedge C_2 | 0.6$, $C_1 \leftarrow \text{true} | 0$, $R.sensitivity = 0.6$, $C_1.sensitivity = 0$.

定义 1 设 P 是实体 E 的协商策略,用 5 元组来描述该策略: $P = \{serials, index, rules, reputation, \Delta t\}$. $P.serials$ 是规则序号, $|P.serials|$ 表示规则数量; $P.index$ 是规则索引,由证书标识符组成; $P.rules$ 是策略规则; $P.reuptation$ 是 E 的声誉; $P.\Delta t$ 是有效的协商时间.

定义 2 对于 P 的第 i 个证书 C_i,其敏感度是 C_i 内容隐私级别,由拥有 P 的实体 E 设定,用 $C_i.sensitivity \in [0,1]$ 表示.设证书敏感度门限值 $\varepsilon_{sensitivity} \in [0,1]$,则有:

收稿日期:2009-01-02;修回日期:2009-07-18
基金项目:国家自然科学基金(No. 60573141, No. 60773041);江苏省自然科学基金(No. BK2008451);国家 863 高技术研究发展计划(No. 2007AA01Z404, No. 2007AA01Z478);现代通信国家重点实验室基金(No. 9140C1105040805);江苏高校科技创新计划(No. CX08B-085Z, CX08B-086Z);江苏省六大高峰人才项目

(1)如果 $0 \leqslant C.sensitivity \leqslant \varepsilon_{sensitivity}$,则称 C 的内容是不敏感的,可以自动被披露.

(2)如果 $\varepsilon_{sensitivity} < C.sensitivity < 1$,则称 C 的内容比较敏感的.需要进一步考察后再做出协商决策,比如考虑实体的声誉.

(3)如果 $C.sensitivity = 1$,则称 C 的内容高度敏感.除非 E 愿意,否则不能自动披露 C.

对于 R 的策略 P,C 是满足 P 的有限证书集,记为 $sat(C,P)$.若 $sat(C,P)$ = true, $\forall C_i \in C$ 满足 $C_i.sensitivity \geqslant \varepsilon_{sensitivity}$,则称 C 能解锁 R,记为 $unlock(R,C)$.即当 $unlock(R,C)$ = true 时,R 不受敏感度保护,否则表示该方不拥有 R,或拒绝披露.人类社会协商中,$E.reputation$ 建立信任不可忽视的因素.因此引入可信敏感度来反映实体声誉对披露证书的影响.

定义 3　设 $G=(C_1,C_2,\cdots,C_k)$是资源 R 的一个有限披露序列,如果 $\forall C_i \in C(1 \leqslant i \leqslant k)$在披露时满足不受保护条件,即 $sat(C,P)$ = true,那么称 G 是一个安全披露序列.若满足 $C_n = R$,则称信任协商成功.

定义 4　可信敏感度是指拥有策略 P 的实体 E_i 的声誉 $E_i.reputation$ 和 P 中证书 C_j 敏感度 $C_j.sensitivity$ 的比值,记为 $ratio_{r\_s}$,有:

$$ratio_{r-s} = \frac{E_i.reputation}{C_j.sensitivity} \tag{1}$$

其中 $C_j \in E_j$, $E_j \neq E_i$, $E_i.reputation$, $C_j.sensitivity \in [0,1]$.

2.2　可信敏感度策略

可信敏感度协商策略旨在找到一个安全披露序列 $G=(C_1,C_2,\cdots,C_n=R)$.例 1 是一个信任协商实例,其中实体 E^C 向 E^S 发出协商服务请求,策略规则如下:

例 1　P^C: $C_1 \leftarrow S_1 \wedge S_2 | 0.6$
$C_2 \leftarrow S_2 | 0.5$
$C_3 \leftarrow S_1 \vee S_2 | 0.5$
$C_4 \leftarrow$ true $| 0$
$C_5 \leftarrow S_2 \wedge S_3 | 0.8$
P^S: $R \leftarrow (C_1 \wedge C_2) \vee C_5 | 0.7$
$S_1 \leftarrow C_2 | 0.5$
$S_2 \leftarrow C_4 | 0.4$
$S_3 \leftarrow$ true $| 0$

表 1 是策略 P^S 的存储形式.S_i 和 C_i 是 P^S 与 P^C 中的证书,*sensitivity* 指 S_i 的敏感度;*trusted* 是 *ES* 信任的实体集;*reputation* 的值为 $E^S.reputation$;协商时间超出 Δt 导致协商失败.

表 1　E^S 上维护的协商策略 P^S 的存储形式

serials	*index*	*rules*	*sensitivity*	*trusted*	*reputation*	Δt
1	$\{R,C_1,C_2,C_5\}$	$R \leftarrow (C_1 \wedge C_2) \vee C_5$	0.7	E^{S1}, E^{NTP}, E^{C1}	0.7	120s
2	$\{S_1,C_2\}$	$S_1 \leftarrow C_2$	0.5			
3	$\{S_2,C_5\}$	$S_2 \leftarrow C_5$	0.4			
4	$\{S_3\}$	$S_3 \leftarrow$ true	0			

可信敏感度策略要求请求者不仅需要通过“规则为真”,而且要通过资源敏感性验证.遇到 $C_i.sensitivity > \varepsilon_{sensitivity}$时,则结合 $E.reputation$ 对 $C_i.sensitivity$ 修正后再做出协商决策.根据 $ratio_{r_s}$对 C_i 修正后的敏感值记为 $C_i^*.sensitivity$,具体计算公式如下:

$$C_i^*.sensitivity = \begin{cases} C_i.sensitivity - (ratio_{r-s} - 1), & \text{if } ratio_{r-s} > 1; \\ C_i.sensitivity, & \text{if } ratio_{r-s} \leqslant 1 \end{cases} \tag{2}$$

情况 1　不含循环依赖策略的协商

不含循环依赖的协商中 $P^C.index \cap P^S.index = \varnothing$.设敏感度门限 $\varepsilon_{sensitivity} = 0.5$, $E^C.reputation = 0.85$.表 2 中给出了其中的一个证书请求序列 G_1: $G_1 = \{\{C_4\},\{S_3,S_2\},\{C_2\},\{S_1\},\{C_1\},\{R\}\}$.

表 2　G_1 的证书请求序列

协商者 \ 协商轮次	1	2	3
E^C	$\{C_4\}$	$\{C_2\}$	$\{C_1\}$
E^S	$\{S_3,S_2\}$	$\{S_1\}$	$\{R\}$

G_1 第三轮协商中,$C_1.sensitivity = 0.6 > \varepsilon_{sensitivity}$, $R.sensitivity = 0.7 > \varepsilon_{sensitivity}$,修正敏感度后得 $C_1^*.sensitivity = 0.433 < \varepsilon_{sensitivity}$, $R^*.sensitivity = 0.486 < \varepsilon_{sensitivity}$,这样才可披露 C_1 和 R,完成协商.对于例 1,它的另一个证书交换序列是 G_2: $G_2 = \{\{C_4\},\{S_3,S_2\},\{C_5\},\{R\}\}$,如表 3 所示.

表 3　G_2 的证书请求序列

协商者 \ 协商轮次	1	2
E^C	$\{C_4\}$	$\{C_5\}$
E^S	$\{S_3,S_2\}$	$\{R\}$

在 G_2 第二轮协商中,$C_5.sensitivity = 0.8 > \varepsilon_{sensitivity}$, $ratio_{r\_s} = 7/8 < 1$,需要修正 C_5 的敏感度,得到 $C_5^*.sensitivity = 8/7 > \varepsilon_{sensitivity}$,所以 E^C 不能披露证书 C_5,不能完成协商.实际中常常存在循环依赖的策略而导致了许多协商失败的情况,如例 2 的情况.

情况 2　含有循环依赖策略的协商

定义 5　协商第三方(*NTP*)是与协商双方都有交互的实体,且协商双方信任它.当存在策略循环依赖时,*NTP* 作为协调者在恰当时机向双方披露证书和策略规则,打破循环依赖.

下面来看例 2,E^C 和 E^S 分别在其本地维护着各自策略(如表 4 和表 5).策略规则如下:

例 2 P^C: $C_1 \leftarrow S_1 \wedge S_2 \mid 0.6$
$C_2 \leftarrow S_2 \vee S_3 \mid 0.5$
$C_3 \leftarrow \text{true} \mid 0$
$C_4 \leftarrow S_2 \mid 0.4$
$C_5 \leftarrow S_2 \wedge S_3 \mid 0.5$
P^S: $R \leftarrow C_1 \wedge C_2 \mid 0.7$
$S_1 \leftarrow C_2 \wedge C_3 \mid 0.6$
$S_2 \leftarrow C_4 \mid 0.5$
$S_3 \leftarrow C_4 \wedge C_5 \mid 0.6$
$S_4 \leftarrow \text{true} \mid 0$

表 4 在 E^S 上维护的协商策略 P^S 的存储形式

serials	*index*	*rules*	*sensitivity*	*trusted*	*reputation*	Δt
1	$\{R, C_1, C_2\}$	$R \leftarrow (C_1 \wedge C_2) \mid 0.7$	0.7	E^{S_1}, E^{C_1}, E^{NTP}	0.7	120s
2	$\{S_1, C_2, C_3\}$	$S_1 \leftarrow C_2 \wedge C_3 \mid 0.6$	0.6			
3	$\{S_2, C_4\}$	$S_2 \leftarrow C_4 \mid 0.5$	0.5			
4	$\{S_3, C_4, C_5\}$	$S_3 \leftarrow C_4 \wedge C_5 \mid 0.6$	0.6			
5	$\{S_4\}$	$S_4 \leftarrow \text{true} \mid 0$	0			

表 5 在 E^C 上维护的协商策略 P^C 的存储形式

serials	*index*	*rules*	*sensitivity*	*trusted*	*reputation*	Δt
1	$\{C_1, S_1, S_2\}$	$C_1 \leftarrow S_1 \wedge S_2 \mid 0.6$	0.6	E^{S_2}, E^{NTP}	0.85	120s
2	$\{C_2, S_2, S_3\}$	$C_2 \leftarrow S_2 \vee S_3 \mid 0.5$	0.5			
3	$\{C_3\}$	$C_3 \leftarrow \text{true} \mid 0$	0			
4	$\{C_4, S_2\}$	$C_4 \leftarrow S_2 \mid 0.4$	0.4			
5	$\{C_5, S_2, S_3\}$	$C_5 \leftarrow S_2 \wedge S_3 \mid 0.5$	0.5			

由于 $C_4 \leftarrow S_2$ 和 $S_2 \leftarrow C_4$，即 $P^C.index \cap P^S.index = \{C_4, S_2\} \neq \emptyset$，无法达成协商. 但无论 E^C 或 E^S 都不愿意先于对方披露其规则，只有 E^C 和 E^S 找到 *NTP* 后，向该 *NTP* 发送协助请求. 支持 *NTP* 的可信敏感度协商策略执行如下步骤：

Step1 实体 E^C 执行初始协商策略，当 E^C 决定协商失败时，向 E^S 发送其可信协商者集合.

Step2 若 E^S 返回的可信协商者集合 $NTP = \{E^C.trusted \cap E^S.trusted\} \neq \phi$，则双方都各自将被披露的证书和策略发送给有效的 *NTP*，等待回复消息；否则转 step5.

Step3 *NTP* 根据证书的敏感度来评估循环依赖策略. $ratio_{r-s}$ 最大的策略，将最先被 *NTP* 披露.

Step4 一旦 E^C 收到 *NTP* 发送得非空回复消息，它将启动协商策略.

Step5 如果协商双方收到的是空的 *NTP* 集合，那么协商终止.

由此得到其中序列 G_3（如表 6 所示）：$G_3 = \{\{C_4\}, \{S_2\}, \{C_2, C_3\}, \{S_1\}, \{C_1\}, \{R\}\}$.

对于例 2，$NTP = \{E^{NTP}\}$，C_4、$S_2 \in ENTP$. G_3 的第一轮中 E^{NTP} 打破 $C_4 \leftarrow S_2$ 和 $S_2 \leftarrow C_4$ 的循环，因为 $ratio_{r-s}(C_4) > ratio_{r-s}(S_2)$，所以 E^{NTP} 先将 C_4 向 *ES* 披露. 第三轮中修正 C_1 和 *R* 敏感度，得到 $C_1^*.sensitivity = 0.433 < \varepsilon_{sensitivity}$，$R^*.sensitivity = 0.486 < \varepsilon_{sensitivity}$，因此 E^{NTP} 能帮助 E^C 和 E^S 协商成功.

表 6 G_3 的证书请求序列

协商者 \ 协商轮次	1	2	3
E^C	$\{C_4\}$	$\{C_2, C_3\}$	$\{C_1\}$
E^S	$\{S_2\}$	$\{S_1\}$	$\{R\}$

3 复杂性分析

策略的效率依赖于其计算和通信开销. 设双方拥有证书总数为 n，拥有的策略总数为 m.

3.1 计算复杂性分析

计算开销主要受证书和策略数量的影响，包含证书解锁、搜索最小证书披露序列，分别产生在证书请求协商阶段和证书披露阶段. 证书请求协商阶段：最差情况下，协商初始者必须完全遍历协商对方的策略才能对所需证书 *C* 解锁. 即对 *C* 最多有 n 条请求，策略最多被遍历 n 次. 对于 m 条策略，最差为 $O(nm)$. 证书披露阶段：披露开销包含敏感度的计算以及搜索证书披露序列的开销. 因为 $m \geqslant n$，所以策略计算复杂性是 $O(nm)$.

3.2 通信复杂度分析

策略的通信复杂度依赖于总的消息数量、大小及协商轮次. 证书请求阶段：包含请求消息、修正消息、拒绝消息和授权消息. 证书 *C* 最多只能授权一次，最多被请求 n 次，因此请求消息数量最多为 $O(n^2)$. 修正、拒绝消息与请求消息对应. 最坏情况下每个证书敏感度需修正，大小是 $O(n^2)$. 证书披露阶段：最差情况下每个证书对应一条解锁消息，每次请求者需遍历对方全部策略才能解锁证书，那么交换消息数量为 $O(nm)$. 综上，通信复杂度最差为 $O(n^2)$.

4 网格图像渲染的自动信任协商服务

我们在 NUPT-grid 图像渲染应用中评估了可信敏感度协商策略的性能. 采用的渲染软件是 PBRT(Physically-based Ray Tracer)，一种图像生成引擎，能够构建图像纹理，并将场景描述转化为三维图像. 图 1 描述了网格 PBRT 服务的信任协商过程.

首先在 NUPT-grid 节点上部署 PBRT 服务，通过该策略协商进行作业请求. 节点配置：双核 Intel Xeon 3.16GHz CPU，4G RAM，RedHat® Linux 操作系统. 门户提交 PBRT 作业后，服务请求实体激活协商服务并度量协商策略性能. 测试中，我们将 100 个协商样本划分为 4 组，

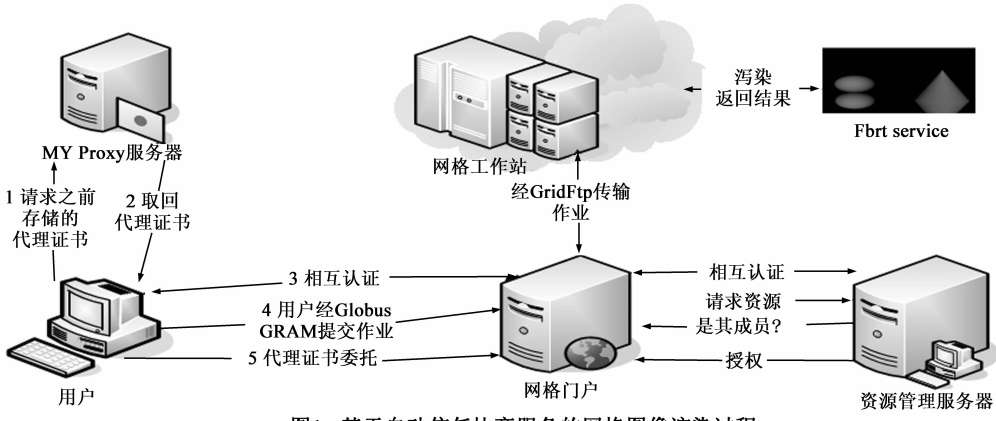

图1　基于自动信任协商服务的网格图像渲染过程

分别使用可信敏感度策略和传统的协商策略提交 PBRT 服务请求.每组中 60%含有循环依赖策略,30%不含循环依赖策略,剩余 10%是协商失败的样本.对于可信敏感度策略和传统 PURNEs 策略,图 2 中是策略协商开销的对比结果.

图2　两类协商策略的协商开销

虚线代表引入 *NTP* 的基于可信敏感度协商策略,点划线代表 PURNEs 策略.由于 *NTP* 减少了协商交换的证书数量,使得协商耗时更少.图 2 底部实线代表敏感度计算的开销,测试中敏感度计算开销为 43.6/893.8 =5.24%.即其中 94.76%的计算能力用在证书的解锁和消息通信方面,如 SSL、SOAP 消息加密和签名验证等,而敏感度的计算仅占总开销的 5.24%.鉴于提高整体安全性需求,这样额外开销在实际应用中是可以接受的.

协商成功率是成功协商的样本在整体样本中占的比例.用"1"表示协商成功,"-1"表示协商失败.在网格 PBRT 服务中分别使用可信敏感度策略和传统 PURNEs 策略,协商成功并响应服务请求的结果对比如图 3 所示.

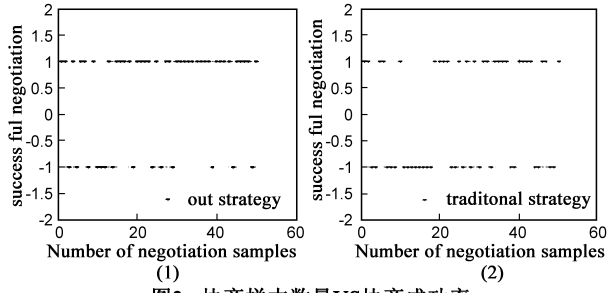

图3　协商样本数量VS协商成功率

图 3(1)是本文提出的基于可信敏感度的协商策略的协商结果,其中大部分样本点分布在水平线"1"的坐标轴上,表明该策略能消除循环依赖策略的影响,成功协商率比较高;图 3(2) 是 PURNEs 策略的协商结果,其中大部分样本点分布在水平线"1"的坐标轴上,说明循环依赖策略影响了其协商性能,成功率相对本文策略的性能较低.我们使用基于可信敏感度的协商策略对于不同样本进行多次测试,成功协商率都保持在 85%以上,因此该策略的适用性较好,有助于推进网格安全应用的展开.

5　结论及展望

自动信任协商是保证安全可信网格环境的重要手段.我们使用可信敏感度信任协商策略和 NTP,解决循环依赖策略,提高协商成功率,保护网格环境安全.策略的计算、通信复杂性分析和网格平台的评估结果都表明该策略性能令人满意,适应网格环境.目前还存在一些要深入研究的问题,如协商中的风险控制等,这将在以后工作中逐步解决.

参考文献:

[1] W H Winsborough, K E Seamons, V E Jones. Automated trust negotiation[A]. DARPA Information Survivability Conference and Exposition[C]. New York: IEEE Press, 2000. 88 - 102.

[2] Ting Yu, Ma Xiaosong, M Winslett. PRUNES: An efficient and complete strategy for automated trust negotiation over the internet[A]. Proc. of the 7th ACM conference on Computer and communications security[C]. Athens, Greece. New York: ACM Press, 2000. 210 - 219.

[3] W H Winsborough, Li Ninghui. Protecting sensitive attributes in automated trust negotiation[A]. Proc. of the ACM Workshop on Privacy in the Electronic Society Washington[C]. DC. New

York: ACM Press, 2002. 41 – 51.
[4] Ting Yu, M Winslett. A unified scheme for resource protection in automated trust negotiation[A]. Proc. of IEEE Symposium on Security and Privacy[C]. Washington, DC, USA: IEEE Computer Society, 2003. 110 – 122.
[5] 熊焰,张伟超,等.一种基于计算能力的无需可信第三方公平非抵赖信息交换协议[J].电子学报,2006,34(3):563 – 566.
Xiong Yan, Zhang Weichao, et al. A fair non-repudiation protocol without TTP based on entity's computing power[J]. Acta Electroinco Sinaca, 2006, 34(3): 563 – 566. (in Chinese)
[6] 姚慧,高承实,戴青,等.一种基于动态规划的自动信任协商策略[J].计算机应用.2008,(28)4:892 – 895.
Yao Hui, Gao Chengshi, et al. Dynamic programming-based strategy for automated trust negotiation[J]Journal of Computer Application. 2008, (28)4: 892 – 895. (in Chinese)
[7] A C Squicciarini, E Bertino, E Ferrari, et al. PP-Trust-X: A system for privacy preserving trust negotiations[J]. Acm Tissec-Transactions on Systems and Information Security, 2007, 10(3): 1 – 50.

作者简介:

杨明慧 女,1981 年生,南京邮电大学博士研究生,研究方向为分布式计算、网格技术、信息安全等.
E-mail: yangmh2000@yahoo.cn

王汝传 男,1943 年生,南京邮电大学教授、博士生导师.主要研究方向是计算机软件、计算机网络和网格、对等计算、信息安全、无线传感器网络、移动代理等.
E-mail: wangrc@njupt.edu.cn