

基于时态逻辑的自动信任协商模型^{*}

杨秋伟, 洪 帆, 杨木祥

(华中科技大学 计算机学院 信息安全实验室, 武汉 430074)

摘 要: 通过分析自动信任协商系统中的行为抽象, 形式化定义了协商模式。基于扩展的一阶时态逻辑给出了自动信任协商系统的抽象模型, 分析了模型的语法和语义, 为实现自动信任协商系统提供了有效的工具。

关键词: 自动信任协商; 时态逻辑; 授权; 访问控制

中图分类号: TP309 文献标志码: A 文章编号: 1001-3695(2007)11-0161-03

Automated trust negotiation based on temporal logic

YANG Qiu-wei, HONG Fan, YANG Mu-xiang

(Laboratory of Information Security, School of Computer Science, Huazhong University of Science & Technology, Wuhan 430074, China)

Abstract: This paper analysed the abstract action in automated trust negotiation and defined pattern of negotiation. Then proposed the abstract model of trust negotiation based on the first-order temporal logic. Presented the syntax and semantic meaning, which provided effective tool for realizing the automated trust negotiation systems.

Key words: automated trust negotiation(ATN); temporal logic; authorization; access control

在传统的计算机系统中, 授权管理主要是基于请求方的身份统一管理域的集中式管理。然而, 在开放的互联网中以及新近出现的 P2P(peer-to-peer) 和 grid 环境下, 迫切需求系统间的协同与资源共享。由于实体数量庞大、运行环境动态分散以及访问控制自主性需求等特点, 各实体往往隶属于不同的管理域, 使得基于身份的访问控制技术在跨域环境下进行授权及访问控制时显得力不从心, 暴露出许多弱点。为此, 需要寻求一种更为有效的信任关系建立方法, 实现从基于身份的访问控制技术到新技术的转换。

在文献[1] 中, Winsborough 等人提出了自动信任协商的概念, 它是“通过信任证、访问控制策略的交互披露, 资源的请求方和提供方自动地建立信任关系”^[1~4]。迄今为止, ATN 的研究已得到迅速发展, 提出了多种领先的研究方法和技术。

1 基本概念

自动信任协商的行为是一种动态现象, 其状态随着时间的推移和信任协商行为的执行不断改变。自动信任协商中的动态行为是经典逻辑和霍尔逻辑所不能描述的。

1.1 自动信任协商

ATN 主要研究跨多安全域的信任建立问题。它与传统访问控制的主要区别在于协商对端是否事先知道对方身份、拥有的权限和访问控制策略。而在自动信任协商里, 通过逐渐暴露属性证书, 最终建立信任关系, 协商过程一般强调自动化, 不需或需少量的人工参与。

在文献[1] 中, Winsborough 等人基于 P2P 的协作模式提

出了自动信任协商的概念, 并定义了 ATN 的抽象模型, 将双方实体间的信任建立抽象为构造一条信任证披露序列(credential disclosure sequence)。

定义 1 ATN 形式化模型^[5]。设请求方信任证集为 ClientCreds, 提供方信任证集为 ServerCreds, 对每份信任证 C 的保护, 记做 $gov_{client}(c)$ 或 $gov_{server}(c)$; 协商的信任证披露序列定义为 $\{C_i\}_{i \in [0..n]} = C_0, C_1, \dots, C_{2n+1}$ 。其中: $n \in N$; $C_{2i} \subseteq ClientCreds$; $C_{2i+1} \subseteq ServerCreds$ 。

1.2 一阶时态逻辑

R. Burstall 在 1974 年首先建议使用模态逻辑进行程序推理, A. Pnueli 和 Z. Manna 建立了可用于程序规约和验证的时态逻辑系统。时态逻辑具有很强的表达能力, 可表达事件行为的安全性(如互斥性和无死锁性等)、活性(如终止性和响应性等)和行为优先性, 是一种研究并发、交互行为强有力的形式化工具。

一阶时态逻辑(first-order temporal logic, FOTL) ^[3,6] 是在一阶逻辑的基础上增加模态操作(modal operators), 以提供时态推理功能。FOTL 已广泛用于交互系统中的描述、验证和分析^[6]。一阶时态逻辑语言由谓词公式、函数符号、变量、量词、连接词和模态操作符构成。其中模态操作符包括 $\Box$ 、 $\Diamond$ 、 $\bigcirc$ 、 $\bigtriangledown$ 和 $\dot{}$ 。

一阶时态逻辑系统中的符号作如下定义: 一组动作符号 $p, q, \dots$; 一组连接词 $\neg, \wedge, \vee$; 时态算子 $\Box, \Diamond, \bigcirc, *, \nabla$ 。

具体功能描述如下: 假设 p 和 q 是两个谓词公式, $\Box p$ 表示从现在开始, p 永远为真; $\bigcirc p$ 表示 p 在下一时刻为真; $\Diamond p$ 表

收稿日期: 2006-07-13; 修返日期: 2006-09-25 基金项目: 国家自然科学基金资助项目(60403027)

作者简介: 杨秋伟(1980-), 男(侗族), 湖南怀化人, 博士研究生, 主要研究方向为信任管理、安全模型(qwyang@ smail. hust. edu. cn); 洪帆(1942-), 女, 教授, 博导, 主要研究方向为访问控制、网络安全; 杨木祥(1976-), 男, 博士研究生, 主要研究方向为密码学、安全模型。

示 p 在将来某个时刻为真; $p * q$ 表示 p 为真直到 q 为真; $p \vee q$ 表示 p 要先于 q 为真。

2 基于扩展的一阶时态逻辑的信任协商

2.1 自动信任协商的行为抽象

根据自动信任协商的行为方式,实体的行为具有以下几个特点:

- a) 目的性。实体的任何行为在信任协商中均体现出实体的一定意图。
- b) 交互性。实体通过一定的协商行为、其他实体交换的信息来改变自身的状态。
- c) 有序性。实体的行为依照信任协商策略在时间上严格排序。
- d) 实时性。实体能实时地对环境或本身状态的改变作出反应,从而执行相应的行为,并且行为执行通常也需要在确定的时间内完成。
- e) 自动性。实体的行为应避免过多的人工交互,具有可扩展性的管理能力。

一个协商模式描述了为完成在陌生实体间建立信任关系的通信协议。该通信协议包括如下诸多方面的要素:

- a) 协商目标(trust negotiation target),信任协商希望达到的目标。
- b) 协商行为(negotiation behavior),陌生实体之间为建立信任关系所进行的协作与交互,包括证书的披露请求和证书披露行为。
- c) 参与者(participant),执行信任协商的实体被称为参与者。
- d) 消息(message),协商实体之间通信的媒介,实体之间是通过发送消息来相互通信与协作的。
- e) 消息谓词(message predicate)是消息的表达形式,消息谓词的格式定义为 message (发送者,接收者,消息参数)。当消息发送成功时,谓词的值为真。
- f) 全局约束(global constraints),与信任协商目标相关的全局约束条件,包括目前环境和系统的状态。
- g) 协商策略(negotiation policy),参与信任协商的实体的证书披露规则,表达了实体在完成信任协商时所遵循的一种逻辑关系。比如说,实体间消息传递的顺序以及实体间的各种约束等。

定义 2 信任协商模式 A 是为完成在陌生实体间建立信任关系的通信协议,用六元组 $A(T, s_1, s_2, \text{PARA}, \text{GC})$ 来表示信任协商模式。其中: A 为协商模式的名字; T 表示信任协商的目标; s_1 、 s_2 分别表示服务请求方和服务提供方。每个实体表示为一个三元组 $\langle N, \text{Message}(A, T), \text{LCP}(A, T) \rangle$ 。其中: N 为实体的名字; $\text{Message}(A, T)$ 表示在协商模式 A 中与协商目标 T 有关的消息谓词的集合; $\text{LCP}(A, T)$ 表示与信任协商目标 T 相关的本地协商策略集合,定义了 $\text{Message}(A, T)$ 中消息的执行顺序和约束关系。 PARA 表示与协商模式 A 的输入和输出参数,包括目前环境和系统的状态; GC 表示与协商模式 A 相关

的全局约束条件,如执行协商行为的时间约束。

2.2 自动信任协商中的约束条件

在许多情况下,自动信任协商过程受到一定环境和系统状态的约束,如只有在工作日或特定地点才能访问某个资源。自动信任协商系统需要检查目前环境和系统的状态,这种决定因素被称为全局约束条件。

通常,一个约束条件是一个或多个属性的逻辑表达式。令 $f(a_1, \cdots, a_n)$ 表示多个属性 $a_1, \cdots, a_n$ 以 $x, \neg x, \wedge$ 和 $\vee$ 操作形式组成的布尔表达式。其中字母集合 $C = \{ a_1, \cdots, a_n \}$ 是布尔表达式中的常量或者变量。

2.3 基于扩展的一阶时态逻辑语法的自动信任协商行为

为了在线性时态逻辑的框架下表示信任协商实体的交互行为,需对线性时态逻辑作如下修改:

- a) 用证书披露符号(证书披露行为) 代替命题符号;
- b) 只考虑当前和将来要执行的动作,即只使用当前和将来的模态算子;
- c) 考虑到协商过程中行为间的执行顺序关系和逻辑关系,增加查询(request) 算子和悬挂(pending) 算子,即 $?$ 和 $!$ 。查询算子表示当前请求披露某证书;悬挂算子表示暂时挂起当前证书的披露。

协商行为公式按照如下规则递归定义:

- a) p, q 是信任协商行为公式;
- b) 如果 p, q 是信任协商行为,则 $? p, p \wedge q, p \vee q, \Box p, \Diamond p, \bigcirc p, p \nabla q, ? p, ! p$ 是协商行为公式;
- c) 仅由 a), b) 构造的是协商行为公式。

定义 3 令 A_i 表示原子行为集, L^A 为基于扩展的一阶时态逻辑的信任协商行为的逻辑语言,则信任协商过程产生的语法用 BNF 表示如下:

$\langle \text{formula} \rangle := \langle \text{predicate} \rangle \mid \langle \text{cation} \rangle \mid ? \langle \text{formula} \rangle \mid$
 $? \langle \text{formula} \rangle \mid \langle \text{formula} \rangle \mid \Diamond \langle \text{formula} \rangle \mid ! \langle \text{formula} \rangle \mid$
 $\bigcirc \langle \text{formula} \rangle \mid \langle \text{formula} \rangle \wedge \langle \text{formula} \rangle \mid \langle \text{formula} \rangle \vee \langle \text{formula} \rangle \mid$

而信任协商的策略表示的语法用 BNF 表示如下:

$\langle \text{formula} \rangle := \langle \text{predicate} \rangle \mid \langle \text{action} \rangle \mid ? \langle \text{formula} \rangle \mid \langle \text{formula} \rangle \mid$
 $\langle \text{formula} \rangle \vee \langle \text{formula} \rangle \mid \langle \text{formula} \rangle \wedge \langle \text{formula} \rangle \mid$
 $\langle \text{formula} \rangle \nabla \langle \text{formula} \rangle \mid \langle \text{formula} \rangle * \langle \text{formula} \rangle \mid$

定义 4 用证书披露符号代替命题符号, C, C_1, C_2 为证书披露符号。 L^A 的语义定义如下:

- a) $? C$ 当前请求披露证书 C ;
- b) $\neg C$ 当前不披露证书 C ;
- c) $C_1 \wedge C_2$ 当前同时披露证书 C_1, C_2 ;
- d) $C_1 \vee C_2$ 当前披露证书 C_1 或 C_2 , 两者必居其一;
- e) $\bigcirc C$ 下一时刻披露证书 C ;
- f) $C_1 * C_2$ 一直披露证书 C_1 , 直至披露证书 C_2 , 此算子表示证书披露之间的互斥约束执行关系;
- g) $C_1 \nabla C_2$ 证书 C_1 先于证书 C_2 披露, 此算子表示证书披露之间的顺序执行关系;
- h) $! C$ 将当前证书 C 的披露挂起;
- i) $\Box C$ 将来永远披露证书 C ;
- j) $\Diamond C$ 将来可能披露证书 C 。

定义 5 L^A 关于时态算子 $\Box$ 、 $\Diamond$ 、 $\bigcirc$ 、 $*$ 、 ∇ 以及新增算子 $?$ 和 $!$ 的公理及推理规则如下:

- a) $? p \setminus \quad ? \Diamond p$

b) $\neg p \setminus \quad \Box ? p$

c) $\Box p \rightarrow \bigcirc p$

d) $\bigcirc \neg p \rightarrow \neg \bigcirc p$

e) $\Box p \rightarrow \bigcirc \Box p$
- f) $\Box W p \setminus \quad \Box p$

g) $p \nabla q \setminus \quad (q \vee (p \wedge \bigcirc (p \nabla q)))$

h) $p \nabla q \rightarrow \Diamond q$

i) $! p \setminus \quad \neg p \vee (\Diamond p)$

j) $p * q \setminus \quad (\neg p \wedge q) \vee (p \wedge \neg q)$
- 推理规则为 $(p * q, q) \not\models (\neg p \wedge q) ; (p \nabla q, p) \not\models q$ 。

以上的公理均在线性时态逻辑的框架下定义,符号“ $\rightarrow$ ”和“ $\setminus$ ”的含义与经典逻辑中的定义相同。 L^A 是一个符合线性时态逻辑的形式化系统。在 L^A 下定义的行为公式即是信任协商过程中的行为表达式;在 L^A 下定义的策略公式亦是信任协商系统的策略表达式。

3 实例

在线电子书城系统中,仅注册了用户能浏览的所有产品;全时服务的用户可以在任何时刻在线观看视频文件,限定时间区间服务的用户必须提供信用卡以及驾驶执照(驾驶执照包含了主体的年龄信息。考虑到规范未成年人的日常行为,如果是未成年人则必须在有效服务时间接受服务,那么用户还需要提交本地系统时间)。利用上述的基于线性时态逻辑的动作行为表示方法已可以完整表示实体在信任协商中的各种行为以及协商策略。

```
Trust Negotiation Target “在线订阅图书”
service provider: eBookMarket;
service request: Alice;
Alice own
{
    Credentials:
        C1: eBookMarket. PartTimeUser ← Alice
        C2: BMV. driverLicense( name = 'Alice ', DoB = 06/07/1980 ) ← Alice)
        C3: Bank. Credit( CardNo = x) ← Alice
    Local policies:
        P1: BBB. businessLicenseè eBookMarket. PartTimeUser← Alice
        P2: ( BBB. goodSecProcess ∧ Bank. partnor) è Bank. Credit← Alice
        P2: ( BBB. goodSecProcess ∧ BBB. businessLicense) è BMV. driverLicense← Alice
};
eBookMarket own
{
    Credentials:
        C1: BBB. businessLicense← eBookMarket
        C2: BBB. goodSecProcess← eBookMarket
        C3: BMV. Cooperate← eBookMarket
        C4: Bank. partnor← eBookMarket
    Local policies:
        P1: □ BBB. businessLicense ∧ □ BBB. goodSecProcess ∧ □ Bank. Partnor
        P2: ( eBookMarket. PartTimeUser ∨ eBookMarket. FullTimeUser) è eBookMarket. productlist
        P3: eBookMarket. FullTimeUserè eBookMarket. onlineWatch
        P4: ( eBookMarket. PartTimeUser ∧ Bank. Credit) è eBookMarket.
```

```
onlineWatch
P5: ( eBookMarket. PartTimeUser ∨ false) * eBookMarket. FullTimeUser
};
Global constrains:
    ( Alice ∈ EBookMarket. FullTimeUser) ∨ ( Alice ∈ eBookMarket. PartTimeUser ∧ CurrentTime ∈ useful-time) ;
Initial:
    input( CurrentTime) ;
Messages exchange:
a) Alice  $\xrightarrow{? \text{eBookMarket. productlist}}$  eBookMarket
b) BookMarket  $\xrightarrow{\Diamond \text{eBookMarket. productlist}}$  Alice
    eBookMarket  $\xrightarrow{? \text{eBookMarket. PartTimeUser}}$  Alice
c) lice  $\xrightarrow{\Diamond \text{eBookMarket. PartTimeUser}}$  eBookMarket
    Alice  $\xrightarrow{? \text{BBB. businessLicense}}$  eBookMarket
d) BookMarket  $\xrightarrow{\text{BBB. businessLicense}}$  Alice
    eBookMarket  $\xrightarrow{? W \text{eBookMarket. PartTimeUser}}$  Alice
e) lice  $\xrightarrow{\text{eBookMarket. PartTimerUser}}$  eBookMarket
    Alice  $\xrightarrow{? W \text{eBookMarket. productlist}}$  eBookMarket
f) eBookMarket  $\xrightarrow{\text{eBookMarket. productlist}}$  Alice
end negotiation.
```

4 结束语

自动信任协商技术主要研究跨多安全域的隐私保护、信任建立等问题,伴随着 Internet 技术的发展、商务信息的全球化,其应用领域也将不断拓展。

参考文献:

[1]INSBOROUGH W H, SEAMONS K E, JONES V E. Automate trust negotiation[C] //Proc of DARPA Information Survivability Conference and Exposition. New York: IEEE Press, 2000: 88-102.

[2]BARLOW T, HESS A, SEAMONS K E. Trust negotiation in electronic markets[C] //Proc of the 8th Research Symposium on Emerging Electronic Markets. Maastricht, Netherianels: [s. n.], 2001.

[3]SEAMONS K E, WINSLETT M, YU Ting, *et al.* . Protecting privacy during on-line trust negotiation[C] //DINGLEDINE R, SYVERSON P F. Proc of the 2nd Workshop on Privacy Enhancing Technologies. Berlin: Springer-Verlag, 2003: 129-143.

[4]WINSBOROUGH W H, LI N H. Towards practical automated trust negotiation[C] //Proc of the 3rd Int’l Workshop on Policies for Distributed Systems and Networks. Washington D C: IEEE Computer Society Press, 2002: 92-103.

[5]李建欣,怀进鹏,李先贤.自动信任协商研究[J].软件学报,2006,17(1): 124-133.

[6]李贵,尹朝万,郑怀远.对象互操作的行为模型[J].计算机学报,1999,22(5): 502- 507.

[7]MANNA Z, WORLPER P. Synthesis of communicating processes from temporal logic specifications[J]. ACM Transaction on Programming Language System, 1984,6(1): 68-93.