

文章编号:1001-9081(2015)07-1858-07

doi:10.11772/j.issn.1001-9081.2015.07.1858

基于交错螺旋矩阵加密的自动信任协商模型

李健利*, 谢 悅, 王艺谋, 丁洪骞

(哈尔滨工程大学 计算机科学与技术学院, 哈尔滨 150001)

(*通信作者电子邮箱 lijianli@hrbeu.edu.cn)

摘要:针对自动信任协商(ATN)中的敏感信息保护问题,提出了基于交错螺旋矩阵加密(ISME)的自动信任协商模型。此模型采用交错螺旋矩阵加密算法以及策略迁移法,对协商中出现的3种敏感信息进行保护。与传统的螺旋矩阵加密算法相比,交错螺旋矩阵加密算法增加了奇偶数位和三元组的概念。为了更好地应用所提模型,在该协商模型的证书中,引入了属性密钥标志位的概念,从而在二次加密时更有效地记录密钥所对应的加密敏感信息。同时列举了在协商模型中如何用加密函数对协商规则进行表示。为了提高所提模型协商成功率和效率,提出了0-1图策略校验算法。该算法利用图论中的有向图构造了6种基本命题分解规则,可以有效地确定由访问控制策略抽象而成的命题种类。之后为了证明在逻辑系统中此算法的语义概念与语法概念的等价性,进行了可靠性、完备性证明。仿真实验表明,该模型在20次协商中策略披露的平均条数比传统ATN模型少15.2条且协商成功率提高了21.7%而协商效率提高了3.6%。

关键词:自动信任协商; 敏感信息保护; 访问控制策略; 交错螺旋矩阵加密; 0-1图策略校验算法

中图分类号: TP393.08 **文献标志码:**A

Automated trust negotiation model based on interleaved spiral matrix encryption

LI Jianli*, XIE Yue, WANG Yimou, DING Hongqian

(College of Computer Science and Technology, Harbin Engineering University, Harbin Heilongjiang 150001, China)

Abstract: The Automated Trust Negotiation (ATN) Model based on Interleaved Spiral Matrix Encryption (ISME) was proposed for the protection of sensitive information in the automated trust negotiation. The interleaved spiral matrix encryption and policy migration were used in the model to protect three kinds of sensitive information of negotiation. Compared with the traditional spiral matrix encryption algorithm, the concept of odd-even bit and triple were added into the interleaved spiral matrix encryption algorithm. In order to make the model adapt the application better, the concept of key attributes flag was introduced in the certification of negotiations, and thus it recorded the sensitive information which corresponded to the encrypted key effectively. Meanwhile, how to represent the negotiation rules through encryption function was listed in the negotiation model. To increase efficiency and success rate of the model, the 0-1 graph policy parity algorithm was proposed. The decomposition rules of six basic propositions were constructed by directed graph of graph theory in the 0-1 graph policy parity algorithm. The propositions abstracted by the access control policies could be determined effectively and the reliability and completeness was testified to prove the equivalence of semantics concept and syntax concept in logistic system. Finally, the simulation results demonstrate that the model of the average number of disclosure strategy is 15.2 less than the traditional model in 20 negotiations. The successful rate of the negotiation is increased by 21.7% and the efficiency of the negotiation is increased by 3.6%.

Key words: Automated Trust Negotiation (ATN); sensitive information protection; access control policy; Interleaved Spiral Matrix Encryption (ISME); 0-1 graph policy parity algorithm

0 引言

Winsborough等^[1]提出的自动信任协商(Automated Trust Negotiation, ATN),已经成为网络安全中一个全新的研究领域。自动信任协商是通过资源访问者和资源拥有者利用证书、访问策略的互相披露,从而为处于不同安全域之间的主体建立信任,来达到交换资源的目的。它与传统的访问控制差异较大,普通的访问控制对于不同的安全域不能进行有效控

制,而自动信任协商正是为了弥补这个缺陷而被提出的。传统的自动信任协商模型对敏感信息并没有起到很好的保护作用,且默认访问控制策略有效,而实际应用中会出现无效的访问控制策略^[2],因此,对敏感信息保护和访问控制策略的有效性校验成为ATN研究中一个重要方向。

自动信任协商中,敏感信息的保护主要有以下3种方式:对资源内容敏感的保护、对资源拥有敏感的保护和对信息在非安全物理信道中传输时的保护^[3]。目前尚无一种自动信

收稿日期:2015-02-11;修回日期:2015-03-30。 基金项目:国家自然科学基金资助项目(61073042)。

作者简介:李健利(1963-),男,山东龙口人,副教授,主要研究方向:访问控制、自动信任协商; 谢悦(1989-),男,河北石家庄人,硕士研究生,主要研究方向:自动信任协商; 王艺谋(1990-),男,辽宁丹东人,硕士研究生,主要研究方向:自动信任协商; 丁洪骞(1990-),男,山东泰安人,硕士研究生,主要研究方向:自动信任协商。

任协商模型能够比较完善地同时对这 3 类敏感信息进行保护。此外,敏感信息保护模型协商效率和成功率较低,原因是存在无效的访问控制策略,因此,如何能够在保证较高协商效率和成功率的同时又能保护敏感信息成为本文研究的重点。

本文基于交错螺旋矩阵加密(Interleaved Spiral Matrix Encryption, ISME)算法,对资源内容敏感和非安全物理信道中敏感信息传输进行保护,并应用策略与证书相分离的思想对资源拥有敏感进行保护,同时为了进一步提高系统的协商效率和成功率,提出了 0-1 图策略校验算法,减少访问控制策略中无效策略的数量。

1 相关研究

本章首先综述国内外敏感信息保护的一些研究成果。主要从资源内容敏感信息保护,资源的拥有敏感信息保护和非安全物理信道中敏感信息传输这三方面进行描述。

对于资源内容敏感信息保护,国内外学者提出了很多方案,以下几类是其中典型代表。UniPro 模式是 Yu 等^[4]提出的一种应用在 ATN 中对资源(敏感证书与访问控制策略)进行保护的统一模式。UniPro 是在传统的自动信任协商研究的基础上,把策略看成最优先保护的资源,应用与保护资源相同的方法对策略进行保护,同时还可以对策略的暴露进行细粒度控制,明确区分了策略披露和策略满足这两个概念。雷建云等^[5]提出一种基于信任向量的敏感信息保护方案。此方案通过信任评估,可以做到有选择性地暴露证书中的敏感属性。策略图这一概念是由 Seamons 等^[6]提出的,目的是对访问控制策略中的敏感信息进行保护。策略图是一个有向无环图,资源 R 为其最终节点,其他节点由保护资源 R 的访问控制策略组成。优点是可逐步对访问控制策略进行披露;缺点是未涉及到证书中敏感信息的保护,在实际应用中有很大的局限性。

资源拥有信息敏感与资源内容敏感一样也是研究的热点。对这一类的敏感信息保护,国内外研究者也提出了很多方案。Seamons 等^[7]提出了对拥有敏感信息的不响应来保护敏感信息。它的中心思想是,访问控制策略与敏感属性相互独立,使它们之间没有明显的关联。策略数据库由 Irwin 等^[8]提出,主要是保护 ATN 中资源的拥有属性敏感。策略数据库的主要设计思想是把策略的披露和属性的拥有情况相分离,按照每个属性拥有敏感信息的不同,将其分配到不同的推理组件中,来防止对访问控制策略中拥有敏感信息属性的推理。访问控制策略是随机提取的,与所拥有的敏感信息并没有明显的关联,从而使敏感信息不至于通过访问控制策略而隐式地泄露,以达到保护敏感信息的目的。不过策略数据库还是有其不足,它还存在因为概率推理而使资源拥有敏感信息泄露的问题。虽然 Liu 等^[9]进行了改进,引入了关联检测器来检测用户从策略数据库中提取的访问控制策略与敏感信息是否有关联,提升了系统的安全性,但是引入关联检测器后会降低系统的协商效率。Liu 等^[10]提出了一种借助描述逻辑推理对协商者访问控制策略安全性进行分析的方法,从而保护访问控制策略中隐含的敏感信息。Kikuchi 等^[11]提出了完善的隐私保护模型,主要是通过协商双方互相学习来建立信任,协商中不交换访问控制策略和证书。但是本文对相互学习的描述并不清楚,而且对 ATN 的协商机制改动过大。

对非安全物理信道中的敏感信息保护,现在研究的还比较少。典型代表有李健利等^[12]提出的基于魔方算法的自动信任协商方案,该方案详细地阐述了如何对非安全物理信道中敏感信息进行保护。此方案的优点是可实现信息高速传输且不暴露证书和资源信息,但不足是没有考虑到对属性的内容敏感和拥有敏感的保护。

针对以上敏感信息保护方案的不足,本文提出了基于交错螺旋矩阵加密的自动信任协商模型。采用交错螺旋矩阵加密算法对敏感信息进行保护,同时针对该模型改进了传统的协商规则和协商协议。提出了 0-1 图访问控制策略校验算法来提高系统的协商效率和成功率。

2 交错螺旋矩阵算法设计

本章基于螺旋矩阵加密算法^[13]提出了一种加密效率更高、安全性能更好的交错螺旋矩阵加密(ISME)算法,来对自动信任协商中的证书和访问控制策略进行加密,生成的密文变换序列,可以使协商双方外其他第三方均不能截获证书和策略中的内容。

这里介绍双螺旋矩阵。以四阶矩阵为例,传统的螺旋矩阵如图 1 所示,是一个称螺旋状态的矩阵,它的数字由第一行开始到右边不断变大,向下变大,向左变大,向上变大,如此循环。双螺旋矩阵如图 2 所示,它与传统的螺旋矩阵不同,它的数位是分奇数位和偶数位,所有的奇数位构成一个螺旋矩阵,同理所有的偶数位也构成一个螺旋矩阵。双螺旋矩阵与传统的螺旋矩阵相比拥有更强的灵活性,规律更加地隐蔽,密钥相对传统螺旋矩阵加密也更长;同时奇偶双螺旋,不必遵循传统螺旋矩阵数字的变化规律,数字通过奇数和偶数分别制定变换顺序如图 2 所示,在不造成奇偶冲突的情况下可以在矩阵的最外层四个角选取任意的起点。

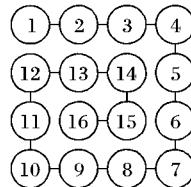


图 1 螺旋矩阵

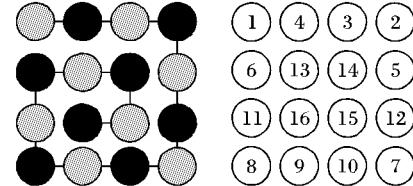


图 2 交错螺旋矩阵

2.1 ISME 加密算法

本节对双螺旋矩阵加密算法进行具体的描述,解密算法为其逆过程这里不再描述,加密过程如下。

输入:访问控制策略(Access Control Policy, ACP)或证书中敏感属性(Certification Letter Sensitive Attributes, CLSA)。

输出:访问控制策略密文序列(ACiphertext_Seq)或证书中敏感属性密文序列(RCiphertext_Seq)。

步骤 1 把 ACP 或 CLSA 转换为一串长度有限的二进制数。

步骤 2 把二进制数分成长为 $(4 \times n)^2$ 如 $4/16/64\cdots$,

n 的取值为 $1/2, 1, 2, \dots$ 。首先 $b_1 = x_1 * y_1$, x_1 是二进制长度划分的块数, y_1 是块的长度, 长度取值为 $(4 \times n)^2$, 如式(1):

$$b = \sum_{i=1}^m b_i \leq \sum_{i=1}^m (x_i * y_i); i \in (4 \times n)^2, n = 1/2, 1, 2, \dots \quad (1)$$

步骤 3 分割好的二进制串按密钥中的 z (一个六位的二进制数) 安排从二进制的最高有效位 (Most Significant Bit, MSB) 到最低有效位 (Least Significant Bit, LSB) 进行排列。

步骤 4 把 $(4 \times n)^2$ 的矩阵分割成 2×2 的矩阵, 位数不够的补零, 并按列读出。

步骤 5 把读出的二进制数按读出先后顺序排好, 生成密文。

2.2 算法密钥设计

对于一个对称加密算法, 密钥的设计无疑是非常重要的。

在 ISME 中密钥是一系列的三元组 (x_i, y_i, z_i) , x_i, y_i 决定如何把二进制数划分成矩阵, y_i 表示矩阵的容量, x_i 表示这样大小的矩阵个数, 其关系必须满足式(1), 公式中, b 表示明文的大小。 z_i 是一个 6 位的二进制数, 如表 1 所示, 它的选择要注意奇偶选择起点的互斥性, 左上角与右下角互斥, 右上角与左下角互斥。

表 1 密钥说明

奇数位	摆放次序	偶数位	摆放次序
第 1 位	奇数摆放次序	第 4 位	偶数摆放次序
第 2,3 位	摆放的起点	第 5,6 位	摆放的起点

3 ISMATN 模型基本概念

ISMATN (Interleaved Spiral Matrix Automated Trust Negotiation) 是一个基于交错螺旋矩阵加密算法的 ATN 协商模型, 它可以对敏感信息进行有效的保护。该模型的主要组件有访问控制策略库 (Access Control Base, ACB)、策略迁移器 (Strategy Transfer Device, STD)、策略校验器 (Strategy Validator, SV)、证书库 (Certificate Repository, CR) 和加解密器 (Encryption/Decryption Device, E/DD), 并且 ISMATN 模型有自己的访问控制策略格式和证书格式。

DHMATN 模型的协商过程如图 3 所示, 在协商开始时, 双方开始披露各自的访问控制策略, 访问控制策略中可能隐性的包含敏感信息, 因此包含敏感信息的访问控制策略进入到策略迁移器 (STD), 进行策略迁移。迁移后的策略由于是新生成的策略, 就必须验证这一策略的有效性, 若没有通过则需重新进行迁移, 这样保证访问控制策略的有效性, 使协商更好地进行。验证后的策略进入到加解密器 (E/DD), 生成访问控制策略密文序列进行交换, 满足后双方披露证书, 证书直接进入 E/DD, 生成资源密文序列, 进行交换直到协商成功。

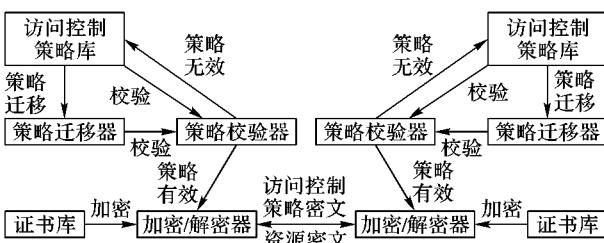


图 3 ISMATN 模型

3.1 访问控制策略格及证书格式

这里设计了一种新的访问控制策略格式, 其式如下: $\text{acp} = (\text{holder}):(\text{recipient}):(\text{item}):(\text{op}):(\text{value}):(\text{notBefore}):(\text{notAfter})$ 其中: holder 是指策略的持有者, 即资源持有方; recipient 是策略的接受者; item 是属性项; op 指操作符如: $\text{op} \in \{<, >, \leq, \geq, \in, \notin, \subset, \not\subset, \subseteq, \not\subseteq, =, \neq\}$; value 是属性值用来判断数字证书的属性值是否符合要求; notBefore 和 notAfter 表示是策略的有效期, 其结构如图 4 所示。

策略拥有者(holder)	策略接受者(recipient)
属性项(attribute)	比较谓词(op)
属性值(value)	
策略有效期(notBefore,notAfter)	

图 4 基于属性的元策略格式

ISMATN 的证书中每个属性都被加密, 并且根据属性敏感度的不同分别使用了不同的加密密钥, 因此, 证书格式为“主体 + 属性 + 属性密钥标志位”, 属性密钥标志位附加在证书的扩展项中。flag 作为属性密钥标志位记录了此密钥能够解密哪些敏感属性。

3.2 ISMATN 描述

ISMATN 与传统的协商模型不同, 增加了策略校验器、策略迁移器以及加解密器, 其模型如图 3 所示。

以下对加解密器模块加以具体描述。

1) 加密器 (ED)。加密函数 $\text{DP}_e(\text{key}, R)$, 表示在提供资源的一端利用密钥 key, 把资源 R 加密。

这里的资源 R 可理解为证书中敏感信息以及扩展项中的 flag。此过程采用两次加密, 首先, 生成一个或多个 (x_i, y_i, z_i) 的三元组作为密钥, 其中: $x_i, y_i, z_i \in \{0, 1\}^m$ (其选择必须满足上文介绍的原则), m 表示 z_i 中的 0, 1 不止一个。然后, 用密钥对资源 R 进行加密, 其加密表达式为:

$$\text{RCiphertext_Seq} = \text{DP}_e(\text{key}_1, R)$$

此后, 对第一次加密密钥 key_1 进行第二次加密, 此密钥是协商开始之前协商好的, 这里记为 key_2 , 其加密表达式为:

$$\text{RCiphertext_Seq} = \text{DP}_e(\text{key}_2, \langle \text{DP}_e(\text{key}_1, R), \text{key}_1 \rangle), \text{尖括号表示有多项需要加解密的内容, 此处是第一次加密后的密文序列及 key}_1$$

生成 ACiphertext_Seq 比较简单, 直接加密, 其加密表达式:

$$\text{ACiphertext_Seq} = \text{DP}_e(\text{key}, \langle \text{user}, \text{Policy} \rangle)$$

表示用密钥 key 对 user 和 Policy 加密。其中: user 是密文接收方, 即访问控制策略的接受方不是访问控制策略的发送方; Policy 是访问控制策略。

2) 解密器 (DD)。解密函数表达式 $\text{DP}_d(\text{key}, \text{RCiphertext_Seq})$, 在资源接收端用密钥 key 进行密文解密恢复资源 R。

对资源 R 的密文序列进行解密, 表达式为: $(\text{RCiphertext_Seq}, \text{key}_1) = \text{DP}_d(\text{key}_2, \text{RCiphertext_Seq}), R = \text{DP}_d(\text{key}_1, \text{DP}_d(\text{key}_2, \text{RCiphertext_Seq}))$ 。

对于解密 ACiphertext_Seq , 直接利用解密函数 DP_d , 即 $\text{Policy} = \text{DP}_d(\text{key}, \text{ACiphertext_Seq})$

此外, 为了保证系统 ISMATN 的一致可靠性, 在这里规定系统函数约束条件。函数 $\text{STD}(\text{parameter}), \text{SV}(\text{parameter})$, $\text{parameter} \in \{\text{ACP}\}$, 策略密文序列:

$$\text{ACiphertext_Seq} = \text{DP}_e(\text{key}, \langle \text{user}, \text{Policy} \rangle)$$

资源密文序列:

$RCiphertext_Seq = DP_e(key_2, \langle DP_e(key_1, R), key_1 \rangle)$ 解密后的密文序列:

$$R = DP_D(key_1, DP_D(key_2, RCiphertext_Seq))$$

$$Policy = DP_D(key, ACiphertext_Seq)$$

加密函数 DP_e 与解密函数 DP_D 之间满足:

$$\langle user, Policy \rangle = DP_D(DP_e(key, \langle user, Policy \rangle))$$

最后,在第一次加密中,为了保护证书中的敏感信息,把证书中的属性由不同的密钥加密,同时又因为密钥的选择是由访问控制策略决定的,因此,如果 $Policy_1$ 与 $Policy_2$ 是不同的两个策略且分别对应两个密钥 key_1 和 key_2 ,则任何满足不同策略的用户,都不能分辨 $RCiphertext_Seq_1$ 与 $RCiphertext_Seq_2$,其中: $RCiphertext_Seq_1 = DP_e(key, \langle DP_e(key_1, R), key_1 \rangle)$, $RCiphertext_Seq_2 = DP_e(key, \langle DP_e(key_2, R), key_2 \rangle)$ 。

3.3 ISMATN 协商规则

本节介绍 ISMATN 模型的协商规则,这里的协商规则就是阐述加密函数 DP_e (解密函数 DP_D 类似)如何对复合策略进行处理。

1) 元策略用最简单表示方法。

$$ACiphertext_Seq = DP_e(key, \langle user, Policy \rangle)$$

其中: key 是加密密钥,尖括号中是加密的信息。

2) 若 $P = P_1 \wedge P_2$:

$$ACiphertext_Seq = DP_e(key, \langle user, P \rangle) =$$

$$DP_e(key, \langle DP_e(key, \langle user, P_1 \rangle), user, P_2 \rangle)$$

对复合“与策略”进行的加密表示,是从左向右依次对策略加密。

3) 若 $P = P_1 \vee P_2$:

$ACiphertext_Sequence = DP_e(user, P) = DP_e(key, \langle DP_e(key, \langle user, P_1 \rangle), DP_e(key, \langle user, P_2 \rangle) \rangle)$ 对复合“或策略”加密,首先平行加密 P_1 与 P_2 ,最后再对此两项加密。因为“或策略”一项为真即可满足策略,因此要最后进行联合加密。

4) 若 $P = MofN(2, P_1, P_2, P_3, P_4)$:

$$ACiphertext_Seq = DP_e(key, \langle user, P \rangle) = DP_e(2, DP_e(key, \langle user, P_1 \rangle), DP_e(key, \langle user, P_2 \rangle))$$

“可满足策略”与“或策略”类似。

3.4 ISMATN 协商协议及应用

本节通过一个场景实例来具体地阐述 ISMATN 的协商协议和实际中如何对敏感信息进行保护。

例如某保密组织(Security Organization, SO)中资料室的开放只针对 SO 的高层管理人员和保密室的主管,普通的组织成员需要时必须向组织申请。其他非组织成员必须满足与 SO 是项目合作关系并且得到保密室主管授权,以及是 SO 主负责的项目,这 3 个条件中的任意两个,才可以对保密室的资料进行查阅。

上述场景可以用如下策略进行描述, $P = (T_1 \vee T_2) \vee (T_3 \wedge T_4) \vee MofN(2, T_4, T_5, T_6)$ 。证书集合 $Trusts = \{T_1, T_2, T_3, T_4, T_5, T_6, T_7, T_8\}$,其表示如下: $T_1 = \{user_name\} : SO : (Top_manager, age. 45) : '!' = \{user, role = age. 45, Top_manager\}$,后面的证书简单表示为: $T_2 = \{user, role = age. 37, Director\}$, $T_3 = \{user, role = age. 26, staff\}$, $T_4 = \{user, role =$

$Director \ empower\}$, $T_5 = \{user, role = cooperate\}$, $T_6 = \{user, role = Project\}$, $T_7 = \{user, role = SO\}$, $T_8 = \{user, role = data\}$ 。

ISMATN 的协商过程如图 5 所示。

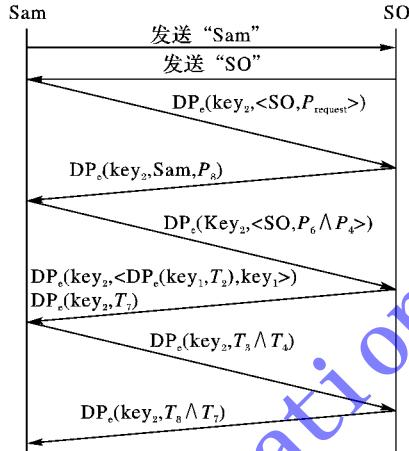


图 5 ISMATN 协商过程

1) 证书及访问控制策略准备阶段。

资源请求方证书集合 $T_{Sam} = \{T_3, T_4, T_6\}$, 服务方证书集合 $T_{SO} = \{T_2, T_7, T_8\}$, 访问控制策略为: $P_{request} = T_8 \wedge T_7$, $P_8 = T_3 \wedge T_4$, $P_6 = T_7$, $P_4 = T_2$ 。

2) 身份确定及密钥协商阶段。

此阶段,双方先互相交换自己的身份和加密密钥 key_2 (此密钥是对证书第二次加密密钥)。

3) 策略披露阶段。

此阶段会涉及到对非安全物理信道中敏感信息的保护和资源的拥有敏感信息保护。

首先,资源请求方 Sam 发出请求 $ACiphertext_Seq = DP_e(key_2, \langle SO, P_{request} \rangle)$, 服务方 SO 收到访问控制策略密文序列对其进行解密, $P_{request} = DP_D(key_2, ACiphertext_Seq)$, 服务方根据 Sam 的请求披露自己的访问控制策略 P_8 , $ACiphertext_Seq = DP_e(key_2, \langle Sam, P_8 \rangle)$, Sam 收到后解密 $P_8 = DP_D(key_2, ACiphertext_Seq)$, 解密后的内容是要求 Sam 披露 T_3 和 T_4 ,但是 T_3 和 T_4 是敏感证书,而且保护证书 T_3 的 P_3 中有属性拥有敏感信息需要系统对这一敏感信息进行保护。

P_3 的内容是: Sam 属于某保密组织 SO 的成员,拥有 SO 为其颁发的证书 T_3 ,如果只是拟定 T_3 的访问策略 P_3 ,其他方在向 Sam 请求 T_3 时, Sam 披露策略 P_3 或不响应时都会使其他方知道 Sam 是否拥有 T_3 ,因此,需要把 T_3 的访问控制策略迁移到证书 T_6 ,生成新的访问控制策略 P_6 。凡是新生成的策略都要进行策略的有效性验证,合格后 Sam 披露 $P_6 \wedge P_4$, $ACiphertext_Seq = DP_e(key_2, \langle SO, P_6 \wedge P_4 \rangle)$ 。SO 解密 $P_6 \wedge P_4 = DP_D(key_2, ACiphertext_Seq)$, $P_6 \wedge P_4$ 的内容是要求对方披露证书 T_2 和 T_7 ,此时的 T_2 和 T_7 是非敏感的,双方开始交换证书,策略交换阶段结束。

综上所述,此阶段通过对策略的加解密,有效地保护了非安全物理信道中敏感信息保护,并且在涉及到属性拥有敏感信息时,应用策略迁移理论,对其进行保护。

4) 证书交换阶段。

此阶段双方开始证书交换,本阶段同上阶段一样,全部证书交换都采用了加密,保护了非安全物理信道中敏感信息的

传输,同时,应用了二次加密机制,对资源的内容敏感进行了有效保护,具体过程如下。

SO 根据 $P_6 \wedge P_4$ 披露其证书 T_2 和 T_7 ,由于 T_2 中包含有对协商方 Sam 的敏感信息,因此 T_2 证书需要进行二次加密,对其中的“年龄”和“职务”使用不同的密钥加密,根据协商方提供的策略来判断证书中那些属性是不敏感的,从而确定 key₁。

二次加密后的序列为: RCiphertext_Seq = DP_e(key₂, ⟨DP_e(key₁, T₂), key₁⟩)。T₇ 中不包含对 Sam 的敏感信息直接加密即: RCiphertext_Seq = DP_e(key₂, T₇)。Sam 收到证书后,进行解密 $T_7 = DP_D(RCiphertext_Seq)$, T₂ 比较复杂要由里向外逐次解密, $T_2 = DP_D(key_1, DP_D(key_2, RCiphertext_Seq))$ 。这里由于 key₁ 只是对敏感信息“职务”加密而“年龄”是由其他密钥进行保护,因此协商方是无法解密“年龄”这个敏感属性。后面的证书交换按照策略披露序列倒序进行,直到协商成功,其中涉及的证书加密过程同上。

通过上述的应用实例可知,本模型利用了加密,保护了证书中的内容敏感信息以及不安全物理信道中信息的传输,其中保护内容敏感信息还应用到了二次加密机制。利用策略迁移器,保护了访问控制策略中拥有属性敏感。由此可知,ISMATN 模型可以有效地对三类敏感信息进行保护。

4 0-1 图策略校验算法

本章具体对 ISMATN 模型中策略校验器的内置算法 0-1 图策略校验算法进行描述。首先,说明出现无效访问控制策略的原因;随后,给出对访问控制策略的分类,提出 0-1 图策略校验算法;最后,对本文算法进行可靠性完备性证明。

4.1 策略的分类

在自动信任协商系统中,造成出现无效策略的原因主要有以下几个方面:

- 1) 角色职能互斥导致的无效策略;
- 2) 策略语言的局限性;
- 3) 策略描述不当导致策略无效;
- 4) 内容冲突导致无效策略。

以下是策略具体分类。

定义 1 有效策略。数学形式化表示为: $P_{\text{复合}} = f(p_1, p_2, \dots, p_n)$, 中除了 $p_1 = p_2 = p_3 \dots p_n = \text{false}$, 其余的 $2^n - 1$ 个指派 $p_i (i = 1, 2, \dots, n)$ 时, $P_{\text{复合}}$ 不永为 true 也不永为 false。

定义 2 矛盾策略。数学形式化表示为: $P_{\text{复合}} = f(p_1, p_2, \dots, p_n) \equiv \text{false}$, 无论 $p_i (i = 1, 2, \dots, n) = \text{true}$ 或者 $p_i (i = 1, 2, \dots, n) = \text{false}$ 。

定义 3 永真策略。数学的形式化定义如下:已知一个由 n 个元策略构成的集合,拥有 2^n 个不同的指派,赋值给 $P_{\text{复合}} = f(p_1, p_2, \dots, p_n) \equiv \text{true}$ 。

4.2 0-1 图策略校验算法

0-1 图策略校验算法,是通过 6 个策略基本分解规则,对一条访问控制策略进行分解。基本分解规则如图 6 所示,图中起始节点为要校验的复合策略,每条边上的值是对其头节点的赋值,终节点是复合策略的真值假设。真值假设是决定策略图如何构成的最初步骤。校验时对策略先假设 T 没矛盾再假设 F,若都无矛盾则为有效策略。如果 T 有矛盾则为矛盾策略,F 有矛盾则为永真策略。

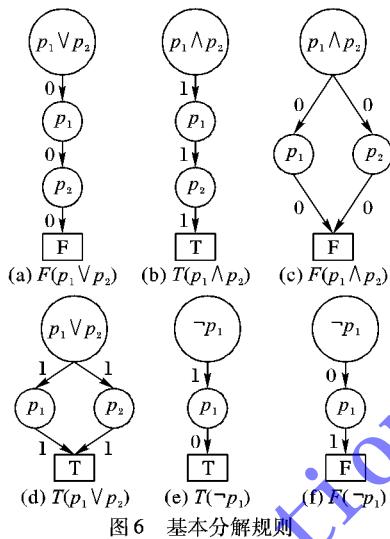


图 6 基本分解规则

为了更好地说明 0-1 图策略校验算法,下面列举 3 类策略的实例。

例 1 校验策略 $p_1 \vee (p_2 \wedge \neg p_3)$ 的种类。

首先对策略进行真值假设 $T(p_1 \vee (p_2 \wedge \neg p_3))$, 应用 0-1 图分解算法构成 0-1 校验图。如图 7 所示, 遍历图中的每一条路径, 没有发现路径中存在任何的矛盾, 并且也没有一条路径上的赋值全为 false, 因此这条策略为有效策略。

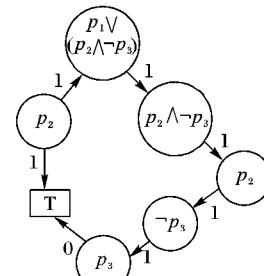


图 7 策略 $T(p_1 \vee (p_2 \wedge \neg p_3))$ 的 0-1 图

例 2 校验策略 $p_1 \vee \neg p_1$ 的种类。

首先对策略进行真值假设 $F(p_1 \vee \neg p_1)$, 应用分解规则构成 0-1 图如图 8 所示。通过图 8 可知其所有路径均产生矛盾,由此可以判断此策略无论如何赋值都不会满足假设的赋值,因此,可知道此策略为永真策略。

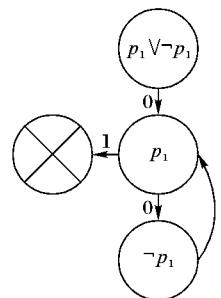


图 8 策略 $F(p_1 \vee \neg p_1)$ 的 0-1 图

例 3 校验策略 $p_1 \vee \neg p_1$ 的种类。

策略 $p_1 \wedge \neg p_1$ 的真值假设为 $T(p_1 \wedge \neg p_1)$, 构成的 0-1 图如图 9 所示。可以发现其所有路径都存在矛盾,所以说明无论怎么赋值其结果都不会为真,策略为矛盾策略。

综上所述策略校验的算法步骤如下。

输入: $Policy(f, P_{\text{复合}})$, 真值假设 T/F, 其中 $P_{\text{复合}}$ 是由元策略 $p_i (i = 1, 2, \dots, n)$ 用 \wedge 或 \vee 复合而成。

输出: 0 为有矛盾, 1 为无矛盾。

步骤 1 复合策略 $P_{\text{复合}}$ 转化成析取范式或合取范式的形式, 形如 $(p_1 \wedge p_2) \vee (p_3 \wedge p_4) \vee (p_5 \wedge p_6)$ 或 $(p_1 \vee p_2) \wedge (p_3 \vee p_4) \wedge (p_5 \vee p_6)$ 。

步骤 2 对复合策略进行真值假设, 例如假设策略 $T(p_1 \wedge p_2)$ 或 $F(p_1 \wedge p_2)$ 。

步骤 3 应用 6 种分解规则对 $P_{\text{复合}}$ 进行策略分解, 使之构成一个 0-1 图。

步骤 4 对构造好的 0-1 图的每一条路径进行遍历, 检测路径中是否存在矛盾。

步骤 5 对结果进行判断, 如果赋值 T 或 F 都不存在矛盾路径且在赋值 T 时不存在赋值全为假的情况, 则为有效策略。如果赋值 F, 所有路径都存在矛盾则为永真策略; 如果赋值 T, 所有路径都存在矛盾则为矛盾策略。

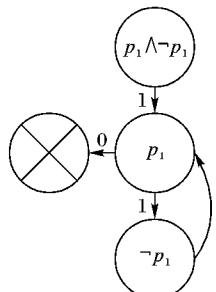


图 9 策略 $T(p_1 \wedge \neg p_1)$ 0-1 图

4.3 策略校验算法可靠完备性证明

为证明算法的可靠完备性, 这里首先证明一个引理, 其内容和证明过程如下。

引理 1 设 0-1 策略图 G , f 是与到最后的终点相一致的赋值, 则存在一条路径 S , 对这条路径上所有的元策略进行赋值的结果与 f 是一致的。

证明 应用数学归纳法, 首先, 通过假设可知 f 是与最后的终点相一致的赋值, 例如 $F(p_1 \vee p_2)$, 则 $f(p_1) = 0$ 且 $f(p_2) = 0$, 一定与 0-1 图中的一条路径相一致。现假设图 G_n 中的路径 S_n , S_n 路径上的值与 f 是相一致的。如果图 G_{n+1} 是由图 G_n 扩展而来, 而路径 S_n 暂不扩展, 令 $S_{n+1} = S_n$ 。如果现在扩展 G_n 到 G_{n+1} , 则路径 S_n 中要在图的最后增加一个节点和一条赋真值的边 R , 由归纳假设可知新增的边 R 的值与 f 是一致的, 因此, 可知 f 必与 S_n 中的路径扩展相一致, 即 S_{n+1} 。

定理 1 矛盾策略可靠性。证明如果策略 P 是矛盾策略, 即以策略 P 为起点(真值假设 $T(P)$) 构成的 0-1 策略图最后到达终点的所有可达路径都是矛盾路径, 那么命题 P 是永假的。

证明 应用反证法进行证明, 假设命题 P 不是永假。又根据题设, 策略 P 的真值假设为 $T(P)$, 且存在一组指派 f , 使命题 P 赋值为 T。以下两种情况下称命题指派 f 与策略 P 的真值假设相一致, 如 $T(P)$ 则 $f(P) = 1$, 或者 $F(P)$ 则 $f(P) = 0$ 。根据引理 1 可知, 一组指派赋给 P , 若 P 是图的起点, 那么这组指派必与这图中的一条路径上的所有元策略赋值相一致, 然而遍历图可知并不存在满足这种条件的路径(因为每条路径都会存在 $P_i = 0$ 且 $P_i = 1$ 这种矛盾的情况), 因此, $T(P)$ 不可

能通过分解规则构成一个完整的 0-1 图, 因此假设不成立。

定理 2 矛盾策略完备性。证明如果命题 P 是永假, 那么策略 P 是矛盾策略, 即以策略 P 为起点(真值假设 $T(P)$) 构成的 0-1 策略图最后到达终点的所有可达路径都是矛盾路径。

证明 已知命题 P 是永假, 则对每个赋值 f , $f(P) = 0$ 。假设已经通过分解规则构建了一个 0-1 图 G 。如果 G 存在一条非矛盾的路径 S , 由引理 1 可知一个赋值 f 与这条路径上的元策略赋值一致, 因此也就与 $T(P)$ 相一致, 这就得出一个指派使得 $f(P) = 1$, 这与 P 是永假相矛盾, 因此, 策略 P 是矛盾策略, 即以策略 P 为起点(真值假设 $T(P)$) 构成的 0-1 策略图最后到达终点的所有可达路径都是矛盾路径。

定理 3 永真策略可靠性。证明如果策略 P 是永真策略, 以策略 P 为起点(真值假设 $F(P)$) 构成的 0-1 策略图到达终点的所有可达路径都是矛盾的, 则命题 P 是永真的。

证明 用反证法, 假设命题 P 不是永真, 根据题设策略 P 的真值假设为 $F(P)$, 且存在一组指派 f , 使命题 P 的赋值为 F。根据引理 1 中的叙述可知, 一组对 P 的指派, 如果以 P 为图的起点, 那么图中一定存在一条路径, 其边对元策略的赋值与这组指派相一致。但是通过遍历图可知并不存在一条这样的路径, 每条路径中都存在 $P_i = 0$ 且 $P_i = 1$ 这种情形, 因此 $F(P)$ 不可能构成一个完整的 0-1 图, 假设不成立。

定理 4 永真策略完备性。证明如果命题 P 是永真的, 那么策略 P 是永真策略, 即以策略 P 为起点(真值假设 $F(P)$) 构成的 0-1 策略图到达终点的所有可达路径都是矛盾的。

证明 已知命题 P 是永真, 则对于其所有的指派 f , $f(P) = 1$ 。假设已经应用分解规则构成了一个 0-1 图 G 。若 G 中存在一条非矛盾的路径 S , 由引理 1 可知会存在一个 f 和 P 中的所有元策略一致, 即和 $F(P)$ 相一致, 这样可得出一个赋值使得 $f(P) = 0$, 这与 P 是永真矛盾, 因此, 策略 P 是永真策略, 即以策略 P 为起点(真值假设 $F(P)$) 构成的 0-1 策略图到达终点的所有可达路径都是矛盾的。

5 仿真和分析

本章主要是通过实验对 ISMATN 模型的各项协商指标进行验证。主要是通过 ISMATN 与传统的自动信任协商模型进行对比实验体现本模型在安全方面的优势。

本模型的实验仿真平台应用了 Trust Builder2 这款自动信任协商的开源软件。数据绘图部分采用 Matlab2012 处理。

此次实验是把 ISMATN 与传统的信任模型作对比, 除了协商的成功率和效率这两个系统指标外, 也要对系统的安全性进行对比, 一个协商系统的安全性好坏主要从其在协商时暴露的敏感信息条数决定的。

为方便统计, 本实验规定协商双方的证书库中的证书都为 20 个, 访问控制策略库中的策略数也规定为 100, 做 10 次实验每次 50 次协商, 矛盾策略是 3% 的增加, 永真策略不予考虑。

图 10 可知当矛盾策略不存在时, ISMATN 模型的协商成功率提高不明显, 但随着矛盾策略在访问控制策略库中不断增加, 两者的差异逐渐显露出来。原因是策略变得复杂, 对两模型的协商成功率都有影响。但是 ISMATN 模型虽有下降却仍保持较高协商成功率, 而传统模型受影响较大。ISMATN

模型利用式(2)可知平均协商成功率 0.822, 而传统信任协商模型的平均协商成功率为 0.675。

$$\bar{S} = \left(\sum_{i=1}^n S_i \right) / n \quad (2)$$

$$\bar{E} = \left(\sum_{i=1}^n E_i \right) / n \quad (3)$$

其中: S_i 是第 i 次协商成功率, n 是协商总次数, \bar{S} 是平均协商成功率; E_i 是第 i 次的协商效率, \bar{E} 是平均协商效率。

从图 11 中可以看到在矛盾策略不存在时传统的自动信任协商的协商效率明显高于 ISMATN, 原因是传统自动信任协商中证书内容都是用明文进行传输, 并不涉及加密, 而 ISMATN 要对敏感信息进行加密。然而, 随着矛盾策略数量增加, 协商时间升高协商效率下降。主要原因是无效策略导致的证书死锁和回环策略依赖造成证书交换的死循环。反观 ISMATN 通过策略校验, 去除了无效策略保持了较高效率, 虽然在检测访问控制策略时会花费时间, 但每次协商所涉及策略较少, 因此, 要比协商失败省时间。ISMATN 模型利用式(3)可知平均协商时间为 6.61 s, 传统自动信任协商模型平均协商时间为 6.86 s。

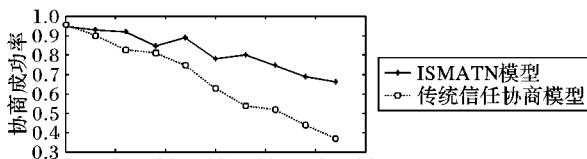


图 10 两种模型的协商成功率对比

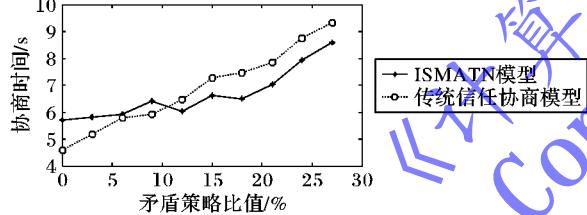


图 11 两种模型的协商效率对比

系统的安全性是否好主要是由协商中敏感信息披露的数量来决定的。协商中敏感信息披露得越多其系统的安全性被认为是越低下。如图 12 所示是 20 次信任协商中两个模型的敏感信息披露情况。传统的信任协商模型因为缺乏敏感信息保护机制, 证书交换中披露的敏感信息较多, 特别是在协商失败的情况下, 敏感信息保护不足为系统带来的危害更大; 而 ISMATN 则因为拥有比较完善的敏感信息保护机制, 因此在 20 次信任协商中敏感信息的披露较传统协商平均减少了 15.2 条。

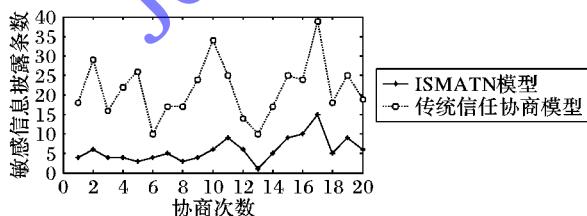


图 12 两种模型的敏感信息披露数量对比

6 结语

本文主要是针对自动信任协商中敏感信息保护及访问控制策略进行研究。为了保护敏感信息本文提出了 ISMATN 协商模型, 其能够在 3 种情况下有效地对敏感信息进行保护, 分

别是非安全物理信道中敏感信息传输的保护、资源内容敏感的保护和资源拥有敏感的保护, 同时为了提高 ISMATN 模型的协商成功率和效率, 在 ISMATN 中引入了策略校验器。策略校验器的内置算法是本文提出的 0-1 图策略校验算法, 此策略校验算法可以对无效策略进行检测, 减少访问控制策略库中无效策略数量, 提高协商效率和成功率。

参考文献:

- [1] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation [C]// DISCEX'00: Proceedings of the 2000 DARPA Information Survivability Conference and Exposition. Piscataway: IEEE, 2000: 88–102.
- [2] LI C. Study on several problems of authorization conflict in access control [D]. Wuhan: Huazhong University of Science and Technology, 2012. (李赤松. 访问控制中授权一致性问题的研究[D]. 武汉: 华中科技大学, 2012.)
- [3] LIAO Z, JIN H, LI C, et al. Automated trust negotiation and its development trend [J]. Journal of Software, 2006, 17(9): 1933–1948. (廖振松, 金海, 李赤松, 等. 自动信任协商及其发展趋势[J]. 软件学报, 2006, 17(9): 1933–1948.)
- [4] YU T, WINSLETT M. A unified scheme for resource protection in automated trust negotiation [C]// Proceedings of the 2003 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2003: 110–122.
- [5] LEI J, YU H, JIANG T, et al. Sensitive information protect scheme in automated trust negotiation [J]. Journal of Wuhan University of Technology, 2012, 34(3): 137–140. (雷建云, 余涵, 蒋天发, 等. 自动信任协商中的敏感信息保护方案[J]. 武汉理工大学学报, 2012, 34(3): 137–140.)
- [6] SEAMONS K E, WINSLETT M, YU T. Limiting the disclosure of access control policies during automated trust negotiation [C]// Proceedings of the 2001 Network and Distributed System Security Symposium. Berkeley: USENIX Association, 2001: 25–32.
- [7] SEAMONS K E, WINSLETT M, YU T, et al. Protecting privacy during on-line trust negotiation [C]// Proceedings of the Second International Workshop on Privacy Enhancing Technologies, LNCS 2482. Berlin: Springer, 2003: 129–143.
- [8] IRWIN K, YU T. Preventing attribute information leakage in automated trust negotiation [C]// Proceedings of the 12th ACM Conference on Computer and Communications Security. New York: ACM, 2002: 36–45.
- [9] LIU B, LU H. An ontology-based trust negotiation framework in advanced communications and computing environments [J]. Journal of Internet Technology, 2009, 10(5): 559–564.
- [10] LIU X, TANG S, HUANG Q, et al. An ontology-based approach to automated trust negotiation [J]. Computer Standards & Interfaces, 2013, 36(1): 219–230.
- [11] KIKUCHI H, PIKULKA EW T. Perfect privacy preserving in automated trust negotiation [C]// Proceedings of the 2011 IEEE International Conference on Advanced Information Networking and Applications. Piscataway: IEEE, 2011: 129–134.
- [12] LI J, HUO G, LIU B, et al. Sensitive information transmission scheme based on magic cube algorithm in automated trust negotiation [J]. Journal of Computer Applications, 2011, 31(4): 984–988. (李健利, 霍光磊, 刘博, 等. 基于魔方算法的自动信任协商敏感信息传输方案[J]. 计算机应用, 2011, 31(4): 984–988.)
- [13] PAUL M, MANDAL J K. A novel symmetric key cryptographic technique at bit level based on spiral matrix concept [EB/OL]. [2014-12-20]. <http://arxiv.org/pdf/1305.0807.pdf>.