自动信任协商中的推理攻击分析*)

杨秋伟　洪　帆　郑明辉　廖俊国
(华中科技大学计算机学院　武汉 430074)

摘　要　自动信任协商是陌生实体通过交替地披露属性证书建立信任关系的一种方法。主体拥有的不同属性之间可能存在着某种联系，某些属性的披露会导致其它敏感信息的泄露，即推理攻击。本文分析了属性间的线性关系，提出了属性敏感强度的概念，定义了属性敏感强度的偏序关系，在此基础上定义了自动信任协商系统抽象模型。针对几类推理攻击给出了相应的防御方案及其安全性分析。

关键词　信任证，自动信任协商，推理攻击，授权管理

The Analysis of Inference Attack in Automated Trust Negotiation

YANG Qiu-Wei　HONG Fan　ZHENG Ming-Hui　LIAO Jun-Guo
(Department of Computer Science, Huazhong University of Science & Technology, Wuhan 430074)

Abstract　Automated trust negotiation is an approach to build trust relationship between strangers by disclosing attribute credentials alternately. The attributes owned by principles are always relevant each other, so disclosing some attributes maybe induce leakage of sensitive information, namely inference attack. We give the definition and partial order of sensitivity intensity of private attribute, then an abstract automated trust negotiation model is proposed, which depicts relevancy not only between principles and attributes, but also between policies and attributes. As a result, several inference attacks in automated trust negotiation are discussed, then defense scheme and security analysis are presented.

Keywords　Credential, Automated trust negotiation, Inference attack, Authorization management

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和资源共享。由于主体数量庞大、运行环境动态分散以及访问控制自主性需求等特点，各主体往往隶属于不同的管理域，使得传统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。

1996 年，M. Blaze 等人首先提出了信任的概念[1]，将信任引入到授权管理中，并在此基础上开发了信任管理系统 PolicyMaker[1]和 KeyNote[2]。Winsborough 等人称这类信任管理系统为基于能力(capability-based)的授权系统[3]，它们仍需要请求方能够预先被服务方所熟知，无法与陌生方建立动态的信任关系。在文[4,5]中，Li Ninghui 等人提出了一种基于角色的信任管理框架(role-based trust-management framework，简称 RT)，RT 模型族中的授权依赖于主体属性，使得陌生方之间建立可能有效的信任关系。但是，陌生主体之间建立信任所依赖的属性信任证和访问控制策略中，都可能泄露交互主体的敏感内容以及资源拥有信息，并且主体间的信任关系常常是动态变化的。

为了解决以上问题，Winsborough 等人提出了自动信任协商[3](automated trust negotiation，简称 ATN)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”[3,6]。在自动信任协商系统中，主体拥有的不同属性之间可能存在某种关联，其中某些属性的披露会导致其他敏感信息的泄露，即存在着推理攻击。在已有的相关研究中[7~10]，并没有对 ATN 推理攻击给出有效的防御方案，敏感信息泄露问题依然存在。

本文首先分析了属性之间的线性关系，定义了隐私属性敏感强度，并给出了敏感强度偏序关系的形式化定义。基于敏感强度偏序关系给出了 ATN 抽象模型的定义，该模型不仅反映了主体与属性、属性与保护策略之间的关联，而且反映了不同属性之间的线性关系，这为解决推理攻击提供了有利的分析工具。最后，本文重点分析了自动信任协商系统中的几类推理攻击，并给出了相应的防御方案，这些防御方案的安全性也得到了详细分析。

本文其他部分的结构如下：第 1 节简要介绍 ATN 中解决的主要问题、属性确认策略以及 RT 语言；第 2 节定义了隐私属性敏感强度以及它的偏序关系，在此基础上给出了 ATN 抽象模型的形式化定义；第 3 节分析了自动信任协商中几类推理攻击，并给出防御方案和安全性分析；最后是全文的总结。

1　基本概念

1.1　自动信任协商

ATN 主要研究跨域的信任建立问题。它与传统的访问控制的主要区别在于协商双方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，通过逐步披露属性证书，最终建立信任关系，协商过程一般强调自动化，不需要或者需要少量的人工参与。

*)国家自然科学基金(No. 60403027)、湖北省教育厅科学基金(No. Q200629001)资助。**杨秋伟**　博士研究生，主要研究领域为安全模型、信任管理模型；**洪　帆**　教授，博士生导师，主要研究领域为访问控制、网络安全；**郑明辉**　博士研究生，主要研究领域为现代密码理论与技术、网络安全；**廖俊国**　博士研究生，主要研究领域为安全模型。

在文[3]中，Winsborough 等人基于 P2P 的协作模式提出了自动信任协商的概念，并且定义了 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)。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"。本文中，资源的请求方被称为敌手，而资源提供方被称为挑战者。

在信任的协商过程中，访问控制策略、信任证通常携带着敏感信息，而对这些敏感信息进行保护，提供统一的敏感信息保护方案，迄今为止没有得到很好的解决。目前，针对典型的敏感信息泄漏问题包括多项技术，如 Ack、策略过滤、策略迁移[11]、隐藏证书[12]以及零知识证明等，这些技术都没有完全解决敏感信息泄露问题，这仍是一个有待解决的问题。

1.2 属性确认策略

信任协商系统中，资源是一些敏感信息的集合，不允许非授权访问。目前所研究的资源(包括访问控制策略和信任证)涉及的敏感信息有两大类[4]：(1)资源的内容敏感：访问控制策略以及信任证中的某些属性值内容是敏感的，不允许未授权地拷贝；(2)资源的拥有敏感：协商方的响应和信息流动可能隐式地披露其拥有某敏感信息这样的事实。

在传统的信任协商模式下，对隐私信息的保护是不够的，会出现敏感信息泄露的问题。特别地，当某个协商者不拥有某个属性(信任证)时，那么也将不拥有与之相关的访问控制策略。当收到敌手发送的属性披露请求时，挑战者的响应行为将区别于其他拥有该属性(信任证)的主体的响应行为。敌手可以通过观察这种行为之间的区别，而推断出是否主体拥有某个属性(信任证)。

为了解决以上问题，Winsboroug 等人[3]以 RT 为基础，引入属性确认策略(Attribute Acknowledgment Policy，简称 Ack Policy)的概念。它的基本思想是：对于一个给定的敏感属性，任意主体无论是否拥有该敏感属性，都披露相同的 Ack Policy，对手无法从披露的策略中判定主体是否拥有此属性。

1.3 RT_0 语言框架[4,5]

本文采用的都是 RT_0 语言框架下的策略语言。RT_0 是 RT(Role-based Trust-management)的基础，它主要用来定义角色。一个角色定义由两部分组成：头部(HEAD)与主体(BODY)，用谓词连接。按语义分类，它有 4 种类型：

类型 1：$A.r \leftarrow B$ 定义主体 B 是角色 $A.r$ 的成员。

类型 2：$A.r_1 \leftarrow B.r_2$ 定义角色 $B.r_2$ 的成员是角色 $A.r_1$ 的成员。

类型 3：$A.r_1 \leftarrow B.r_2.r_3$ 定义角色 $A.r_1$ 包含所有的角色 $X.r_3$，并且 X 是角色 $B.r_2$ 的成员，$B.r_2.r_3$ 是一个链接角色(linked role)。

类型 4：$A.r \leftarrow A_1.r_1 \cap A_2.r_2 \cap \cdots \cap A_k.r_k$，定义角色 $A.r$ 的成员包含了角色集$\{A_i.r_i\}$交集的所有成员。

2 隐私属性敏感强度

2.1 隐私属性敏感强度及其偏序关系

定义 1(隐私属性的敏感强度) 在信任协商系统中，为了防止资源的非授权访问而导致敏感信息的泄露，对这些敏感信息实施一些保护策略，而这些保护策略在敏感信息披露之前必须被满足。这些附加在属性上的保护策略集合记为 $policy(t)$，用来衡量对该属性的保护力度，也被称为隐私属性的敏感强度，简称敏感强度。

根据之前对敏感属性的分类，那么敏感强度也可以分为两类：拥有敏感强度和内容敏感强度，分别用 $policy_{Ack}(t)$ 和 $policy_{AC}(t)$ 来度量，并且 $policy_{Ack}(t) \cup policy_{AC}(t) = policy(t)$。

下面我们分析不同属性(信任证)的 $policy$ 之间的关系。在信任协商系统中，假定用户 u 拥有两个敏感属性，t_1 和 t_2，敌手可以通过获知 u 是否拥有 t_1 而推断出也是否拥有 t_2(例如，存在这样信任证 $A.r_1 \leftarrow B.r_2$，敌手可以通过获知用户 u 拥有属性 $B.r_2$ 而推理出用户 u 也拥有属性 $A.r_1$)。直观上来说，我们认为实施在 t_1 上关于拥有敏感的保护策略的保护力度必须强于 t_2，用户 u 必须严格规定 t_2 的 $policy_{Ack}(t_2)$ 被包含于 t_1 的 $policy_{Ack}(t_1)$ 中，因为只有在敌手获知用户 u 是否拥有 t_1 的同时，也必须使得 t_2 的 $policy_{Ack}$ 被隐式地满足了，从而防止了非授权的信息泄露。

由以上分析可以看出，在一般的信任协商系统中，属性的敏感强度通常具有线性关系。为此，我们引入了属性敏感强度的偏序关系来刻画属性之间敏感强度的线性关系。考虑到 $policy_{Ack}$ 和 $policy_{AC}$ 的相似性，本文仅仅对 $policy_{Ack}$ 之间的线形关系进行形式分析，$policy_{AC}$ 也可以进行类似分析。

定义 2 任意两个属性 t_1 和 t_2，如果 $policy_{Ack}(t_1) \supseteq policy_{Ack}(t_2)$，则称 t_1 的拥有敏感强度不比 t_2 的低，t_2 的拥有敏感强度不比 t_1 的高，记为 $t_1 \geqslant t_2$。如果 $policy_{Ack}(t_1) \supseteq (policy_{Ack}(t_2)$，$policy_{Ack}(t_2) \supseteq policy_{Ack}(t_1)$ 都不成立，则称 t_1 和 t_2 的拥有敏感强度不可比。对任意两个属性 t_1 和 t_2，$t_1 \geqslant t_2 \Leftrightarrow policy_{Ack}(t_1) \supseteq policy_{Ack}(t_2)$。

下面，我们对 $\geqslant$ 的语义进行分析。$t_1 \geqslant t_2$ 体现了敌手为了获知挑战者是否拥有属性 t_1 比获知挑战者是否拥有 t_2 而满足如下几种可能的需求：(1)需要满足更多的保护策略；(2)需要披露更多的属性；(3)要求更多的服务请求响应被完成。数学概念上来说，$\geqslant$ 是一种偏序关系，具有自反、可传递和反对称的特性：

1)属性的保护策略继承是自反的，因为一个属性继承它自己的保护策略；

2)传递在这样的上下文中是一个很自然的需求；

3)反对称排除相互继承的属性，因为这些相互继承的属性是多余的，而且容易出现逻辑错误。

假设信任协商系统中有如下几个信任证：$D.r_4 \leftarrow A.r_1$，$D.r_4 \leftarrow B.r_2$，$E.r_5 \leftarrow C.r_3$，$B.r_6 \leftarrow D.r_4$，$B.r_6 \leftarrow E.r_5$。那么，这些属性敏感强度的直接偏序关系为：$D.r_4 \geqslant A.r_1$，$D.r_4 \geqslant B.r_2$，$E.r_5 \geqslant C.r_3$，$B.r_6 \geqslant D.r_4$，$B.r_6 \geqslant E.r_5$。通过"$\geqslant$"的可传递性还可以推出：$B.r_6 \geqslant A.r_1$，$B.r_6 \geqslant B.r_2$，$B.r_6 \geqslant C.r_3$。图 1 即为这些属性的敏感强度偏序关系结构图。一般概念理解，敏感强度高的属性出现在关系图的顶部，敏感强度低的属性出现在关系图的底部。

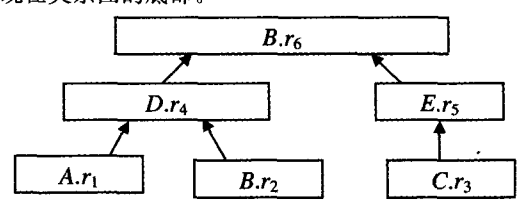

图 1 属性敏感强度偏序关系图

2.2 基于敏感强度偏序关系的 ATN 抽象模型

在前面的部分，我们讨论了隐私属性的敏感强度，并定义

了属性敏感强度的偏序关系。下面将给出基于属性敏感强度偏序关系的 ATN 抽象模型的定义。

定义 3 基于敏感强度偏序关系的 ATN 抽象模型有如下组件：

• U：主体集；T：属性集；P：策略集；S：(信任协商)会话集；

• $UT \subseteq U \times T$，建立 U 到 T 的关联，指定哪些主体拥有哪些属性；

• $PT \subseteq P \times T$，建立 P 到 T 的关联，使用哪些策略保护哪些属性；

• $user: S \to U \times U$，是将每个会话映射到两个协商者(资源提供者，资源请求者)的函数；

• $policy: T \to 2^P$，将每个属性映射到一个策略集合。$policy(t_i) \subseteq \{p \mid (\exists p'' \leqslant p)[(p, t_i'') \in PT]\}$。

• $attribute: S \to 2^T$，将每个会话映射到一个属性集合。$attribute(s_i) \subseteq \{t \mid (\exists t' \geqslant t)[(user(s_i), t') \in UT]\}$。信任协商会话 s_i 需要满足的策略集合为 $\bigcup_{t \in attribute(s_i)} \{p \mid (p, t) \in PT\}$。

• $TOH \subseteq T \times T$，建立 T 关于拥有敏感强度的偏序关系(偏序关系采用"$\geqslant$"，若 $t_1 \geqslant t_2$，称 t_1 是 t_2 的父属性，即 t_1 的拥有敏感强度不弱于 t_2 的拥有敏感强度，而 $policy_{Ack}(t_1) \supseteq policy_{Ack}(t_2)$)。

• $TCH \subseteq T \times T$，建立 T 关于内容敏感强度的偏序关系(偏序关系采用"$\geqslant$"，若 $t_1 \geqslant t_2$，称 t_1 是 t_2 的父属性，即 t_1 的内容敏感强度不弱于 t_2 的内容敏感强度，而 $policy_{AC}(t_1) \supseteq policy_{AC}(t_2)$)。

该模型中用户可以为他具有的属性或其下级属性建立一个会话，协商双方需要满足的策略包括在该会话中激活属性所具有的保护策略以及下级属性所需要满足的保护策略。如果在属性的保护策略继承时限制继承的范围，则可建立私有策略及其私有子偏序关系。当然，并不是所有的属性之间都保持着严格的层次关系。

3 推理攻击分析

3.1 信任协商系统的推理攻击及其安全性

信任协商安全面临的一类主要问题就是推理攻击，是指敌手对某个挑战者提出某些属性查询请求，得到相应有返回信息，然后从这些返回结果中推导出一些该用户本来无权访问的信息。有推理攻击企图的人必须依靠某些共享信息以及个人的经验和知识来分析得到的数据，并从中找到感兴趣的信息(包括一些主体根本没有意识到的、潜在的敏感信息)。

推理攻击可以是敌手通过信息之间本身存在的逻辑关系推理出敏感信息，也可以基于社会知识或者专业知识在看起来毫无联系的信息之间找出逻辑上的联系，从而推理出敏感信息。如果敌手能从查询的响应结果中推理出未经授权的敏感信息，那么就认为存在推理攻击问题。攻击的过程如下：敌手首先确定希望推理出的信息；接着判断进行推理所需的信息，据此构造若干个查询；然后向挑战者发送查询请求，得到挑战者返回的结果；分析所得到的查询响应，推理出所需的敏感信息。例如，如果敌手获知信任证 $A.r_1 \leftarrow B.r_2$ 存在，那么 $B.r_2$ 的满足会暗示着 $A.r_1$ 的满足。

定义 4(信任协商系统的安全性) 对于所有可能的关联(用户与属性之间的关联、属性与策略之间的关联)，任意敌手在满足敏感信息的保护策略以前，不能通过挑战者在此之前的响应推理出任何的敏感信息，那么就称该信任协商系统是安全的。

本文接下来的部分将对 RT_0 语言框架下的几种推理攻击类型进行分析，并给出了相应的解决方案。在 RT_0 语言框架下我们保持着如下两个假设：

1)类似于 $A.r_1 \leftarrow u$ 类型的信任证只能被主体 u 自己保存，证书的分布式查找无法直接获知这样的信任证。

2)其它类型的信任证，如 $A.r_1 \leftarrow B.r_2$，$A.r_1 \leftarrow B.r_2.r_3$，$A.r \leftarrow A_1.r_1 \wedge A_2.r_2 \wedge \cdots \wedge A_k.r_k$，任意主体能动态获取这些类型的信任证。

3.2 $A.r_1 \leftarrow B.r_2$ 类型的推理攻击

3.2.1 正向推理攻击

1)正向肯定推理攻击：敌手通过获知主体拥有 $B.r_2$ 能推断出主体同样拥有 $A.r_1$。

2)正向否定推理攻击：当敌手得知仅仅只有这样的一个证书定义 $A.r_1$，那么敌手通过获知主体不拥有 $B.r_2$ 能推断出主体也不拥有 $A.r_1$。

防御方案：所有主体在制定关于属性拥有敏感的保护策略的时候，使得 $B.r_2$ 拥有敏感强度高于 $A.r_1$，$B.r_2 \geqslant A.r_1$，即 $policy_{Ack}(B.r_2) \supseteq policy_{Ack}(A.r_1)$。

防御方案的安全性分析：

1)正向肯定推理攻击：因为 $B.r_2$ 的拥有敏感强度大于 $A.r_1$，即使敌手通过获知挑战者拥有 $B.r_2$，从而根据 $A.r_1 \leftarrow B.r_2$ 推理出挑战者也拥有 $A.r_1$，但敌手满足 $B.r_2$ 的保护策略的同时也隐式地满足了 $A.r_1$ 的保护策略，这并没有违背授权的信息流动的前提，信息泄露没有发生。

2)正向否定推理攻击：该推理通常不成立。因为除了用户 u，其它用户无法直接获知 u 是否拥有 $A.r_1 \leftarrow u$ 这样的信任证。即使敌手得知 u 不拥有 $B.r_2$，而 $policy_{Ack}(B.r_2) \supseteq policy_{Ack}(A.r_1)$，我们也认为 $A.r_1$ 的保护策略被隐式地满足了，披露 u 没有 $A.r_1$ 的事实也是可取的。

3.2.2 反向推理攻击

1)反向肯定推理攻击：当敌手得知仅仅有这样的一个证书定义 $A.r_1$，敌手通过获知主体拥有 $A.r_1$ 能推断出主体同样拥有 $B.r_2$。

2)反向否定推理攻击：敌手通过获知主体不拥有 $A.r_1$ 能推断出主体也不拥有 $B.r_2$。

防御方案：所有主体在制定关于属性拥有敏感的保护策略的时候，使得 $B.r_2$ 的拥有敏感强度高于 $A.r_1$，$B.r_2 \geqslant A.r_1$，即 $policy_{Ack}(B.r_2) \supseteq policy_{Ack}(A.r_1)$。当敌手请求挑战者披露 $A.r_1$ 时，挑战者披露 $B.r_2$ 的保护策略。

防御方案的安全性分析：

1)反向肯定推理攻击：该推理通常不成立。因为一个用户无法获知是否用户拥有 $A.r_1 \leftarrow u$ 这样的信任证。即使敌手得知 u 拥有 $A.r_1$，敌手也无法判断 u 拥有 $A.r_1$ 是基于 $A.r_1 \leftarrow u$ 的推理，还是基于 $A.r_1 \leftarrow B.r_2$ 的推理，这两者是不可区分的。

2)反向否定推理攻击：因为挑战者披露 $B.r_2$ 的是的保护策略，那么又可以分为以下三种情况：

a)$B.r_2$ 的保护策略没有被满足，同时 $A.r_1$ 的保护策略也没有被满足。挑战者不会披露是否拥有 $A.r_1$，这样的反向推理不成立。

b)$B.r_2$ 的保护策略没有被满足，但 $A.r_1$ 的保护策略被满足了。挑战者可以披露拥有 $A.r_1$ 这样的事实，而不拥有

$A.r_1$ 这样的事实是不能被披露的。披露拥有 $A.r_1$，敌手也许会接下来进行反向肯定推理攻击，此类问题在前面已经得到了分析和讨论；披露不拥有 $A.r_1$ 将会导致敌手推断出主体也不拥有 $B.r_2$，泄露了敏感信息，在我们的安全性定义下，这将是不被允许的。当然，这样的处理将可能会导致某些信任协商的失败。

c) $B.r_2$ 的保护策略被满足，因为 $policy_{Ack}(B.r_2) \supseteq policy_{Ack}(A.r_1)$，所以 $A.r_1$ 的保护策略也被满足了。用户是否拥有 $A.r_1$ 和 $B.r_2$ 的事实都是可以披露的。

3.3 $A.r_1 \leftarrow B.r_2.r_3$ 类型的推理攻击

$A.r_1 \leftarrow B.r_2.r_3$ 类型的推理攻击：敌手首先查询所有的 $B.r_2 \leftarrow X$，再查询主体是否拥有 $X.r_3$，同样存在着向前和向后两类推理攻击。

防御方案：所有主体在制定关于属性拥有敏感的保护策略的时候，使得 $X.r_3$ 的联合拥有敏感强度高于 $A.r$，即 $policy_{Ack}(X.r_3) \supseteq policy_{Ack}(A.r)$。当敌手请求挑战者披露 $A.r$ 时，挑战者披露 $policy_{Ack}(X.r_3)$ 的保护策略。

防御方案的安全性分析：因为这种类型首先需要查询所有的 $B.r_2 \leftarrow X$，在我们之前的假设前提下，这样的信任证只能被主体 X 保存，其他主体需要获知这样的事实，需要满足该信任证件的保护策略，这对于敌手来说本身就是一个复杂问题。并且，推理攻击最后可规约为形为 $A.r$ 与 $X.r_3$ 之间的推理攻击，那么此类推理攻击的防御方案安全性分析与 $A.r_1 \leftarrow B.r_2$ 类型的推理攻击防御方案安全性分析相似，可进行类似分析。考虑篇幅问题，这里不赘述。

3.4 $A.r \leftarrow A_1.r_1 \wedge A_2.r_2 \wedge \cdots \wedge A_k r_k$ 类型的推理攻击

此种类型的推理攻击依旧分为正向推理攻击和反向推理攻击两种：

1)正向推理攻击。敌手通过获知主体是否同时拥有 $A_1.r_1, A_2.r_2, \cdots, A_k.r_k$ 推断主体是否拥有 $A.r$。

2)反向推理攻击。当敌手得知仅仅有这样的一个证书定义 $A.r$，敌手通过获知主体是否拥有 $A.r$ 推断主体是否同时拥有 $A_1.r_1, A_2.r_2, \cdots, A_k.r_k$。

防御方案：所有主体在制定关于属性拥有敏感的保护策略的时候，使得 $A_1.r_1, A_2.r_2, \cdots, A_k.r_k$ 的联合拥有敏感强度高于 $A.r$，即 $\bigcup_{i=1,\cdots,k} policy_{Ack}(A_i.r_i) \supseteq policy_{Ack}(A.r)$。当敌手请求挑战者披露 $A.r$ 时，挑战者披露 $\bigcup_{i=1,\cdots,k} policy_{Ack}(A_i.r_i)$ 的保护策略。

防御方案的安全性分析：

1) 正向推理攻击：因为 $\bigcup_{i=1,\cdots,k} policy_{Ack}(A_i.r_i) \supseteq policy_{Ack}(A.r)$，而我们的策略是只有敌手满足了 $\bigcup_{i=1,\cdots,k} policy_{Ack}(A_i.r_i)$ 才能披露主体是否同时拥有 $A_1.r_1, A_2.r_2, \cdots, A_k.r_k$，在此之前敌手无法得知主体是否拥有 $A.r$ 这样的事实，所以信息泄露得到有效防止。

2)反向推理攻击：$A.r \leftarrow A_1.r_1 \wedge A_1.r_2 \wedge \cdots \wedge A_k.r_k$ 类型的反向推理攻击与 $A.r_1 \leftarrow B.r_2$ 类型的反向推理攻击相似，可以做类似的安全分析，这里不进行赘述。

3.5 概率推理攻击

概率推理攻击：虽然不同属性之间不存在着严格的逻辑推理关系，但是敌手基于社会知识或者专业知识在看起来毫无联系的信息之间找出逻辑上的联系，从而推理出敏感信息。例如，用户拥有某个城市图书馆图书证(library_card)这样的信任证，那么敌手能够拥有较大概率断言用户也是城市居民(citizenship)。

防御方案：对于不同属性之间的概率推理攻击，所有主体在制定关于属性拥有敏感的保护策略的时候，可以根据已有的社会知识或者专业知识，将存在类似概率推理的属性建立私有关系。例如，让 library_card 的拥有敏感强度高于 *citizenship*，$policy_{Ack}(library\_card) \supseteq policy_{Ack}(citizenship)$，默认 $library\_card \geqslant citizenship$，其他处理根据具体案例归类于以上几类推理攻击的某一类。

防御方案的安全性分析：因为这种类型的推理攻击最后可规约为前面讨论过的几类推理攻击的某一类，那么此类推理攻击的防御方案安全性分析与其它几种类型的推理攻击防御方案安全性分析相似，可进行类似分析，这里将不进行赘述。

总结 自动信任协商技主要研究跨域的隐私保护、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。在自动信任协商系统中，主体拥有的不同属性之间可能存在某种关联，某些属性的披露会导致其他敏感信息的泄露，即存在着推理攻击。在已有的相关研究中，并没有对 ATN 推理攻击的有效防御方案。

本文首先定义了隐私属性敏感强度及其偏序关系“$\geqslant$”，基于这种偏序关系给出了 ATN 抽象模型的定义，该模型不仅反映了主体与属性、属性与保护策略之间的关联，而且反映了不同属性之间的线性关系，这为解决推理攻击提供了有利的分析工具。自动信任协商系统中的几类推理攻击在本文中得到了详细的分析，相应的防御方案及其安全性也得到了详细描述。本文对如何防止 ATN 系统的敏感信息泄露进行了研究，这为在商业中实施 ATN 系统提供了必要的理论依据，并且也为保证 ATN 系统的安全性提供了途径。

参 考 文 献

1 Blaze M, Feigenbaum J, Lacy J. Decentralized trust management. In: Dale J, Dinolt G, eds. Proceedings of the 17th Symposium on Security and Privacy. Okaland: IEEE Computer Society Press, 1996. 164～173

2 Blaze M, Feigenbaum J, Keromytis A D. Keynote: trust management for public-key infrastructures. In: Christianson B, Crispo B, William S. et al. eds. Cambridge 1998 Security Protocols International Workshop. Berlin: Springer-Verglag, 1999. 59～63

3 Winsborough WH, Seamons KE, Jones VE. Automate trust negotiation. In: DARPA Information Survivability Conf and Exposition, 2000. 88～102

4 Li Ninghui, Mitchell JC, Winsborough WH. Design of a role-based trust management framework. In: Proceedings of IEEE Symposium on Security and Privacy, 2002. 114～130

5 Li Ninghui, Winsborough WH, Mitchell JC. Distributed credential chain discovery in trust management. In: Proceedings of the 8th ACM Conference on Computer and Communications Security, 2001. 156～165

6 李建欣，怀进鹏，李先贤. 自动信任协商研究. 软件学报，2006，17(1)：124～133

7 Winsborough WH, Li Ninghui. Protecting sensitive attributes in automated trust negotiation. In: Proceeding of ACM Workshop on Privacy in the Electronic Society, 2002. 102～113

8 Yu T, Winslett M. A Unified Scheme for Resource Protection in Automated Trust Negotiation. In: IEEE Symposium on Security and Privacy, 2003. 245～257

9 Bradshaw R W, Holt J E, Seamons K E. Concealing Complex Policies with Hidden Credentials. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004. 245～253

10 Irwin K, Yu T. Preventing Attribute Information Leakage in Automated Trust Negotiation. In: Proceedings of the 12th ACM Conference on Computer and Communications Security, 2005. 36～45

11 Yu T. Automated trust establishment in open systems. Illinois: University of Illinois, 2003

12 Frikken K, Atallah M, Li J. Hidden Access Control Policies with Hidden Credentials. In: Proceedings of the 3rd ACM Workshop on Privacy in the Electronic Society, 2004. 130～131