EPC 信息共享网络的隐私保护策略研究*

韩水华，杜超坎
（厦门大学管理科学系，福建，厦门 361005）

摘 要 安全和隐私是影响无线射频识别(RFID)技术在各个应用领域进一步发展的关键问题，目前尚没有人从管理、运作和技术等层面深入探究过来自供应链整个域上的安全和隐私风险。本文试图研究提出一个面向 EPC 信息共享网络的隐私保护策略框架，以解决 RFID 网络大规模部署所面临的各种访问许可与授权问题。首先分析了 EPC 网络信息共享的隐私保护需求，接着讨论了发现服务的访问控制框架，然后以一个典型的供应链 RFID 应用实例为背景，围绕用户端的访问控制和服务端的访问控制需求，分析了 EPC 发现服务应制定出的各种隐私保护策略。最后，针对这种复杂分布式安全策略管理问题，研究了其可能的实现机制。

关键词 EPC 网络，隐私保护，访问控制策略

中图分类号 TP309.2

1 介绍

安全和隐私是无线射频识别(RFID)领域广泛讨论的话题，不少学者已经对此进行了深入研究，并提出多种技术方案：(1)杀死标签；(2)电磁屏蔽；(3)有源干扰；(4)阻塞器标签；(5)可分离的标签；(6)散列锁定；(7)临时地址；(8)通用重加密[1]。但是，这些研究局限在一个相对狭窄范围，其关注点主要集中在前端问题上[2](见图 1)，例如，如何给标签增加额外的安全特性，如何进行通讯加密，以及如何解决用户访问钥匙的管理问题等[3,4]，这些问题的解决对于促进 RFID 技术的广泛采纳无疑是有帮助的。但是，不容忽视的是在数据采集后端存在的一系列安全隐患，事实上，企业所面临的最大风险可能来自更广泛的供应链网络。相对而言，适用单一组织的访问控制机制仅仅是安全的一小部分，目前尚少有人从管理、运作和技术等层面上深入探究过来自供应链整个域上的安全隐私威胁[5]。

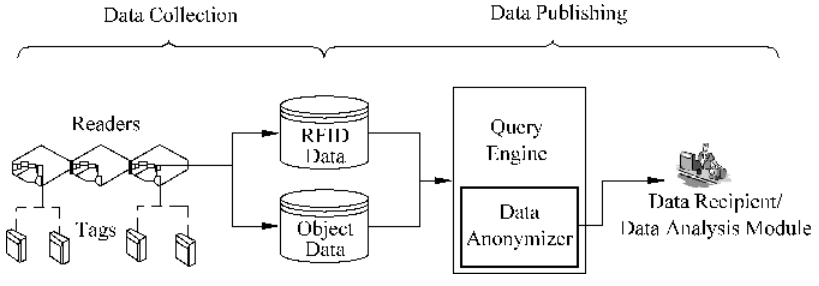

图 1 RFID 系统及其数据流管理

* 基金项目：国家自然科学基金项目(70971112)/福建省高等学校新世纪优秀人才支持计划(X04139)/福建省社科规划基金项目(2009B054)

通信作者：韩水华，男，1970 年出生，博士，厦门大学管理学院教授，e-mail：hansh@xmu.edu.cn

最近几年,有关 RFID 信息共享网络的安全问题开始引起有关人士的注意,NIST[6],BRIDGE[7]的报告证实 RFID 安全问题超出了单个实体保护的范畴。Garfinkel 等人[8]从多层次和跨组织域的角度,分析了 RFID 的隐私问题。R. Agrawal 等人[9]意识到 EPC 信息共享网络可能存在的隐私风险,并认为传统访问控制方法如访问控制列表(ACLs),选择访问控制(DAC)和强制访问控制(MAC),以及基于角色的控制策略(RBAC)可以派上用场;但这些方法应用于 EPC 信息共享网络控制,却存在诸多难点:例如在供应链的各个节点,RFID 标签数据粒度是可变的,可能从单品级—箱体级—托盘级演化,或者存在互为装配的关系,或者存在包装/分拆的关系,因而 RFID 数据的安全管理远比其他应用更复杂;同时供应链伙伴的合作关系也是动态的,信息发布方无法预知物品最终将送到哪一方的手中,使实现跨组织的共享数据管理面临很大的挑战[10];EPC 发现服务具有很特殊的一面,信息发布方和服务运营方是各自独立的,安全策略的制定和实施需要兼顾服务运营方和信息发布方的策略需求,事实上,两者的需求有时是相互矛盾的;EPC 信息的发布方,对其 EPC 相关数据在什么场合下可以被谁访问可能做出不同的决策,必须以细粒度的方式设置查询接口的访问控制。现有的研究成果不足以完全解决 RFID 的隐私与安全问题,相关文献也没有覆盖能适应大规模 RFID 网络部署的完整安全模型。基于此,本文从 EPC 网络的核心组件——发现服务出发,试图通过分析发现服务的访问控制策略来解决 EPC 网络的隐私保护问题,为 EPC 网络标准的完善提供有价值的参考。

2 EPC 网络的发现服务

在供应链 RFID 应用的前期阶段,主要由大型零售商主导构建跟踪数据仓库,但因竞争零售商并不愿意将自己的数据存储在共享数据仓库中,供货商被迫将各自的 RFID 数据上载到送货的零售店,随着数据量的急剧上升,这对集中式数据仓库产生严重的约束。

为解决这一问题,EPCgloable 提出了一种对象域名服务(ONS)[11],其基本思路类似互联网的域名服务,当给定一个产品电子码(EPC),ONS 框架可以指向互联网(或者是企业内部网)的具体某一位置,并提供该特定物品的附加信息。一个典型的 EPC 网络是由几个模块构成的,其中 RFID 标签和读写器可以合并成一个识别系统(RFID System),其功能就是读取物品的 EPC 信息;RFID 中间件系统(RFID Middleware)主要用于初级处理和管理相应的数据,并与更高一层的系统交互作用;EPC 信息服务(EPC-IS)使得为信息服务请求提供产品相关数据成为可能,EPC 信息服务可以针对不同的信息请求作不同的数据处理,以满足用户与供应链伙伴交换相关的产品信息的需要;ONS 属于 EPC 网络的发现服务(Discovery Services),用于帮助用户对所需信息的服务器地址定位。图 2 给出了一个发现服务具体的执行步骤。

(1) 供应商供货时,在货物上贴上 EPC 标签,并将 EPC 在发现服务上注册,货物离开供应商仓库时,RFID 阅读器捕捉到该信息,并通过中间件传输到供应商的 EPC-IS,另外,EPC-IS 还存有 EPC 对应的产品相关信息。

(2) 当货物到达分销商的配送中心/仓库时,阅读器捕捉到该信息,并自动存储在分销商的 EPC-IS 中,同时分销商还将部分 EPC 事件信息(如地点,入库/出库时间等)发布到发现服务上。

(3) 当货物到达零售商的仓库时,执行步骤(2)相同的过程。

(4) 当供应链的实体需要查询产品的事件信息(如产品的运输情况或销售信息)和产品信息时,可以根据 EPC 在发现服务上查询到相关的信息,或通过发现服务的 ONS 来定位相应的 EPC-IS 网络地址,进而查询所需的信息。

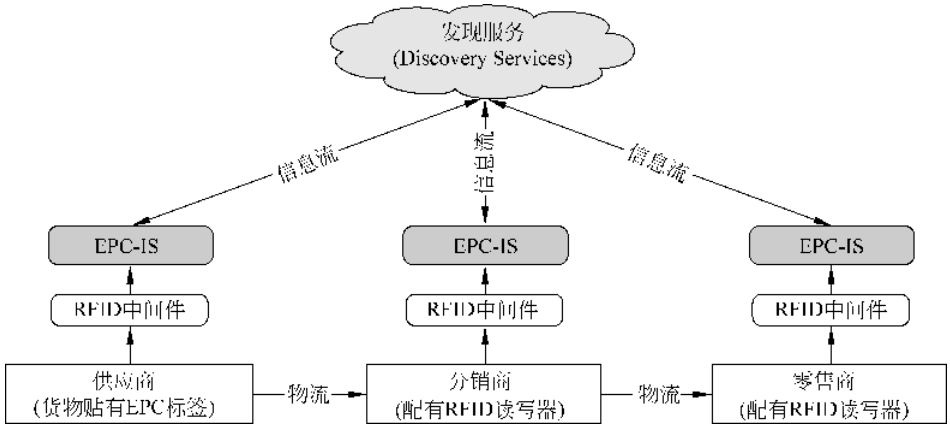

图 2　EPC 网络的信息共享模式

3　EPC 网络共享信息的隐私保护需求

由于供应链上的物品流动信息是企业重要的商业信息，企业一般不允许匿名访问 EPC-IS。因此，发现服务不可能像互联网的域名服务那样直接链接到 EPC-IS 的网络地址，只有当 EPC-IS 的拥有者决定在发现服务注册并发布 EPC 信息后，发现服务才可以链接到其 EPC-IS。此外，EPC-IS 的拥有者为了保护商业隐私信息，只允许受信任的合作伙伴访问其 EPC-IS。依据 EPC 信息共享和发现服务记录查询/发布过程，我们可以得到如下 EPC 信息隐私保护需求。

(1) 记录发布者的隐私

一个数据发布者将 EPC-IS 资源信息发布到发现服务后，他需要确定允许访问数据的对象。此外，记录发布者也需要创建访问控制策略，规定哪些用户访问哪些数据，这种安全和网络信息的公开需要以细粒度的方式进行控制，对于发现服务来说，当数据发布者发布访问控制策略后，发现服务只能将那些用于链接 EPC-IS 的信息向用户公开。

(2) 用户的隐私

当供应链的参与者通过发现服务查询信息时，除了必要的信息之外，发现服务不能将其他的信息透露给参与者。用户向发现服务提交的证书(如 ID 或角色信息)、查询信息以及用户网络地址信息，这些都是用户的隐私，发现服务需要确保这些信息不被窃取。

(3) 数据完整性要求

发现服务上的数据记录需要有明确的拥有者。除了数据发布者和拥有者外，其他参与者不能对数据进行任何修改，授权代理情况除外。此外，参与者不能以其他发布者的身份在发现服务上发布数据。发布者需要有可验证的权限来发布 RFID 数据。对于发现服务来说，在得到发布者的同意之前，记录不能被删除。例如，只有记录的发布者才能删除他们的数据，或者在发布者制定的策略中确定数据的过期时间。在某些情况下，发布者需要将数据的访问权限赋予其他参与者。这样，发布者就需要能够创建、修改、删除访问控制策略，以此控制其他参与者对他们数据的访问。

4　EPC 网络发现服务的隐私保护策略

EPC 网络发现服务的用户主要可以分为两种角色：一个是记录的发布者；另一个是记录的查询者。一般情况下，发现服务的每一个参与者(如供应链上的某个制造商或零售商)都会同时扮演双重

的角色,既是记录的发布者,也是记录的查询者。EPC 网络发现服务存储的资源也可以分为两种类型:第一种是连接各个 EPC-IS 的链接记录,这种记录可能也包含额外的 EPC 事件信息,如物品的出库/入库事件记录;第二种是访问控制策略,与其他的访问控制策略不同的是,根据策略来源的不同,可以将存储在发现服务的访问控制策略分成两种类型:其中一种类型是用户端策略,即记录发布者制定的策略,用来控制其他用户对他们记录的访问;另一种是服务端策略,包括用来限制用户发布记录和策略的访问控制策略等。

4.1 EPC 网络发现服务的访问控制模型

为实现上述的企业个性化隐私保护需求,发现服务应能够提供设定访问控制策略的途径,让企业设定 RFID 数据共享的对象和条件等约束条件。图 3 给出了 EPC 网络发现服务访问控制的基本框架。记录发布过程和记录查询过程可以归纳为以下几个步骤。

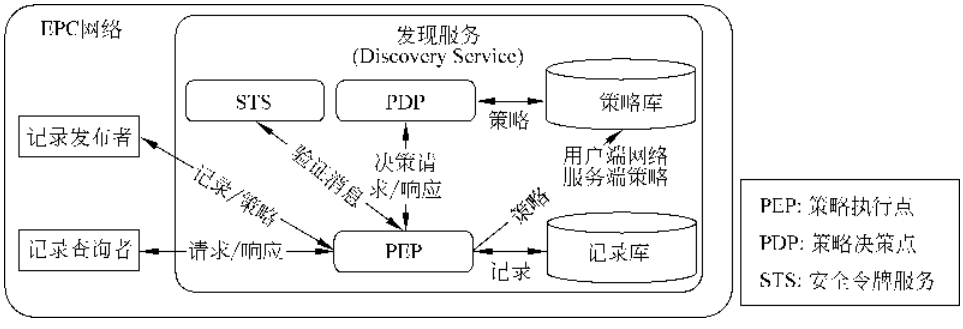

图 3 EPC 网络访问控制的基本框架

记录发布者发布过程:

(1) 记录发布者发布记录/策略时,首先会将自己 STS(安全令牌服务)颁发的安全令牌附加在请求消息中,然后通过网络发送到发现服务。

(2) 发现服务的 PEP(策略执行点)接收到请求消息后,抽取出消息中的安全令牌,将令牌传给发现服务的 STS,STS 利用记录发布者的公钥(在用户注册发现服务阶段获得)对令牌进行有效性验证,并将验证结果信息返回给 PEP。

(3) 若验证通过,PEP 向 PDP(策略决策点)发送一个决策请求,PDP 接到请求后,查询策略库,判断记录发布者是否有发布记录/策略的权限,生成一个策略授权决策,最后将决策返回给 PEP。

(4) PDP 接收到决策响应信息后,执行决策。

(5) 若决策的信息是"Permit",则将消息中包含的记录/策略信息,添加到相应的记录库/策略库;若决策信息是"Deny",则向记录发布者返回一个拒绝指令;若决策的信息是"Not Applicable",则向记录发布者返回一个错误指令。

记录查询者查询过程:

(1) 执行记录发布者发布记录的前 3 个步骤。

(2) 若验证通过,PEP 向 PDP 发送一个决策请求,PDP 接到请求后,查询策略库,接着 PDP 对所有匹配的访问控制策略(假设有多个匹配的策略)进行合并计算评测,生成一个策略授权决策,最后将决策返回给 PEP。

(3) 若决策的信息是"Permit",则从记录库中取出记录,经过签名、加密后通过网络返回给记录查询者;若决策信息是"Deny",则向记录查询者返回一个拒绝指令;若决策的信息是"Not Applicable",

则向记录发布者返回一个错误指令。

4.2 EPC 网络发现服务的访问控制策略

为了分析讨论 EPC 网络发现服务的访问控制策略，本文以一个典型的供应链 RFID 应用实例为背景，分析企业用户为保护信息隐私而需要制定的各种访问控制策略——用户端访问控制策略，以及 EPC 网络实际应用所需要制定的访问控制策略——服务端访问控制策略。

4.2.1 供应链 RFID 应用实例描述

图 4 描述了一个产品从制造商到零售商的流动过程，期间产品的运输通过制造商的物流提供商(MLP)和零售商的物流提供商(RLP)完成。另外，图 4 还有一个表示“监管者”的角色，在某些行业，如食物和药品行业，有很多的行规，那么可以预见当发生重大产品问题时，监管者很可能会直接查询产品的物流信息。

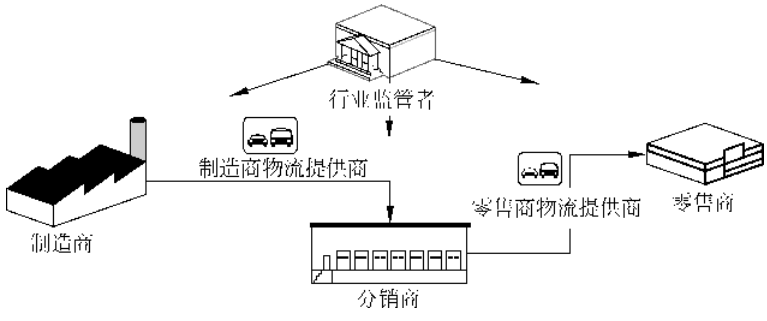

图 4 典型的供应链实例

虽然图 4 的信息只显示了单个的分销商和零售商，但是，在真正的供应链中，一般 MLP 会将产品配送给多个不同的分销商，直至多个零售商。例如，一个新的零售商可能会直接向分销商下订单，在这种情况下，产品的制造商很有可能并不知道它的产品已经输送到新的市场。这种供应链上的不确定性恰好验证了使用发现服务的必要性。在本实例中，假设制造商只与分销商建立直接合作关系，而与零售商没有建立直接的合作关系，分销商与制造商和零售商都有合作关系。

供应链企业利用 EPC 网络实现信息共享主要涉及以下几种应用需求。

(1) 物流提供商跟踪包装箱的使用情况，如果包装箱丢失了，可以查询到包装箱最后出现的位置。

(2) 允许制造商监控零售商销售的产品情况，例如，制造商可以知道是哪个零售商以及如何销售这些产品。制造商有各种合法的理由了解产品的销售信息，例如，如果制造商知道某一个区域的产品库存情况，那么它就可以针对该区域制定相应的广告方案。

(3) 分销商、零售商需要查询产品的主数据信息，如产品的名称、型号、重量等。

(4) 支持物品级的产品召回应用。在供应链流动的产品中很有可能存在劣质产品，在特别的情况下，制造商需要对这些劣质产品进行精确定位进而召回产品。

(5) 行业监管者也可能需要对劣质产品进行跟踪。在这种情况下，就需要一个特殊的策略让供应链的实体访问 EPC 数据。

从以上实例描述可以发现，有些应用需求是检验供应链的运转是否正常，而其他的应用需求则是检查供应链的哪一个环节出现了问题。“例外情况”的例子如：定位丢失的包装箱，或者实现物品级的产品召回。这些应用可以产生很大的商业利益，不过有时候也会不受企业欢迎，企业一般不会将自己重

要的商业信息轻易和其他企业共享。基于此原因,企业有必要制定自身的信息共享访问控制策略。

4.2.2 用户端访问控制策略

发现服务用户端的访问控制策略是完全由发现服务的用户——企业——制定的,用以限制其他企业对其 RFID 数据的访问,以保护企业重要商业信息的隐私。以下分别分析制造商、分销商和零售商的 RFID 数据访问控制策略。

MLP 为制造商运送产品,且运送产品的包装箱是由 MLP 提供的,为了便于 MLP 跟踪托盘和装卸包装箱,制造商应该给予 MLP 托盘和包装箱的信息访问权限,但是对于包装箱所包含的产品,MLP 无须了解其相关的信息,这样,制造商限制 MLP 访问有关产品的信息。该访问控制策略可由图 5 表示的 RFID 数据特点中的容器关系来说明。

分销商是制造商的最终客户,两者之间存在合作关系,分销商除了需要访问托盘和包装箱信息外,也需要通过查询产品的主数据信息(如产品的名称、型号、重量等)来对产品进行分类以便销售给零售商。另外,对于一些特别的产品,如食品,分销商还需要了解产品的每一个物品的有效期等信息。这样,分销商可以查看托盘、包装箱和产品信息。

当分销商把产品转销给零售商时,产品从分销商到零售商的物流是由 RLP 提供的,且在运输时装载产品的托盘也是由 RLP 提供的,这样 RLP 不需要从制造商那获取相关信息,而是从分销商那查询托盘和包装箱的相关信息。

当产品到达零售商后,与分销商一样,零售商需要了解产品的主数据信息,但是制造商与零售商没有建立合作关系,甚至制造商根本不知道零售商的存在,这样,制造商不可能让零售商访问任何信息。

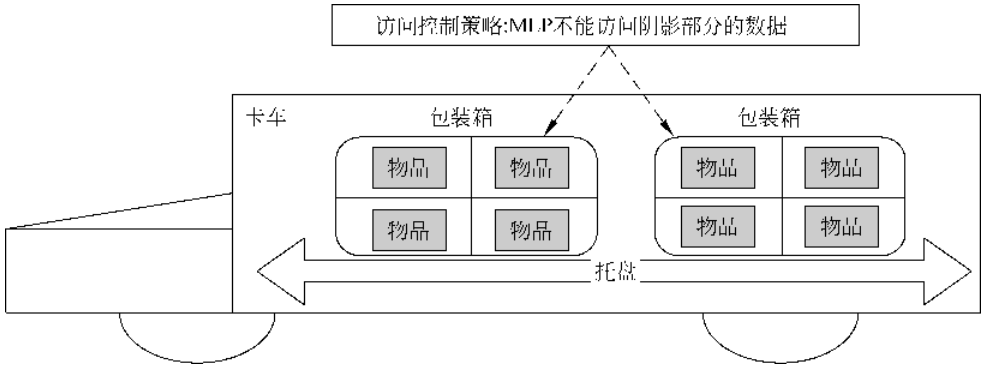

图 5 基于 RFID 容器关系特点的访问控制策略

经过以上分析,归纳得到制造商的各个访问控制策略:

(1) MLP 只能访问托盘和包装箱信息。

(2) 分销商可以查看托盘、包装箱和产品的信息。

(3) RLP 无法访问任何信息。

(4) 零售商无法访问任何信息。

分销商的访问控制策略:

(1) 制造商拥有托盘、包装箱和产品数据的访问权限。

(2) MLP 只能访问属于自己的托盘和包装箱信息。

(3) RLP 只能访问属于自己的托盘和包装箱信息。

(4) 零售商可以访问产品的物品级数据和包装箱信息。

零售商的访问控制策略：

(1) 制造商无法访问任何信息。

(2) 分销商可以查看托盘、包装箱和产品信息。

(3) MLP 没有信息访问权限。

(4) RLP 可以访问托盘和包装箱信息。

假设有一个装载产品的托盘，托盘上有 2 个包装箱，每个包装箱中有 4 件产品，其各自标识的 EPC 码如表 1 所示。

表 1 对象的产品电子码(EPC)

对 象	EPC	
托盘	urn:epc:pat:gid:6.141.10.1	
箱子	urn:epc:pat:gid:6.141.11.1	urn:epc:pat:gid:6.141.11.2
单品	urn:epc:pat:gid:6.141.12.1	urn:epc:pat:gid:6.141.12.5
	urn:epc:pat:gid:6.141.12.2	urn:epc:pat:gid:6.141.12.6
	urn:epc:pat:gid:6.141.12.3	urn:epc:pat:gid:6.141.12.7
	urn:epc:pat:gid:6.141.12.4	urn:epc:pat:gid:6.141.12.8

这样，对于“MLP 只能访问托盘和包装箱信息”的策略可以用 XACML[12] 描述，如下所示：

```
<Policy policyId="MLPAccessPolicy">
  <Rule RuleId="1" Effect="Permit">
  <!--MLP 只能访问托盘和包装箱信息-->
  <ResourceMatch
    MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-is-in">
      <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#anyURI AttributeId="urn:
        oasis:names:tc:xacml:1.0:resource:resourceid"/>
    <!--托盘 EPC 码-->
    urn:epc:pat:gid:6.141.10.1
      </AttributeValue>
      <AttributeValue DataType=http://www.w3.org/2001/XMLSchema#anyURI AttributeId="urn:
        oasis:names:tc:xacml:1.0:resource:resourceid"/>
    <!--包装箱 EPC 码-->
    urn:epc:pat:gid:6.141.11.[1-2]
     </AttributeValue>
    <ResourceAttributeDesignator
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>
    </ResourceMatch>
  </Rule>
</Policy>
```

由于制造商很可能根本就不知道 RLP 和零售商的存在，因而，制造商的“RLP 无法访问任何信息”和“零售商无法访问任何信息”两个访问控制策略其实可以不用额外设定，只要制造商不为他们设定“允许访问”的访问控制策略，RLP 和零售商就无法访问制造商的 RFID 数据。

4.2.3 服务端访问控制策略

发现服务的管理者在制定访问控制策略时，还需要考虑以下几种应用需求。

(1) 为了保护已存在数据的安全和隐私,发现服务的管理者需要制定一些管理规范,例如,规定只有发现服务的合法注册者才能访问发现服务的资源。

(2) 为了保证用户发布的记录/策略的规范性,发现服务的管理者需要对每一位用户发布的记录/策略进行管理控制。

(3) 当出现产品召回等紧急事件时,需要有特别机制以满足紧急事件的信息查询需求。

(4) 行业组织或政府监管部门在某些情况下,需要对产品的信息进行跟踪审核,以及监督问题产品的回收等。这些规定需要在 EPC 网络发现服务上制定相应的策略。

(1) 发现服务基本的访问控制策略

发现服务需要设定一些基本的访问控制策略,例如,只允许注册用户访问存储在发现服务上的记录,或者允许记录的发布者访问自己发布的记录等。利用 XACML 策略描述语言描述主要代码如下所示:

```
<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyId="urn:plicyid:10.Discovery.1"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
    <Rule RuleId="NonSubscriberDenyRule" Effect="Deny">
<!--任何对象对任何资源执行任何动作之前必须先满足是发现服务注册用户的条件-->
    <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
    <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
      <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
       AttributeId="group"                    Issuer="admin@discovery.com"/>
      </Apply>
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
       Subscriber
       </AttributeValue>
     </Apply>
     </Condition>
     </Rule>
</Policy>
```

(2) 用户记录发布控制策略

由于发现服务上存储的记录为多方拥有和控制,设计发现服务的访问控制是一个复杂的难题。难点在于在数据记录的发布者将数据记录放到发现服务进行共享的同时,还要保护数据的机密性,防止非授权的用户查看或非法修改数据记录。这样,我们需要对发布者制定访问控制策略的范围进行限定,即他们只能给自己的数据记录制定访问控制策略。这种限定可以通过给每一个资源(如发现服务中的每一条记录)附加一个“owner”属性来实现。在用户发布访问控制策略时,发现服务先对策略中的记录与记录的“owner”属性进行校验,以判断用户是否拥有特定记录的策略设置权限。用 XACML 描述用户记录发布控制策略主要的代码如下所示:

```
<Policy PolicyId="ServicePolicy2">
<!--用户发布访问控制策略之前需要先进行策略记录"owner"属性校验-->
<Rule RuleId="PolicyPublishRule" Effect="Permit">
  <Target>
    <Actions>
    <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
```

```
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Policy publish
            </AttributeValue>
  <ActionAttributeDesignator DataType=http://www.w3.org/2001/XMLSchema#string
    AttributeId="ServerAction"/>
  </ActionMatch>
 </Actions>
</Target>
<!--需要满足条件"校验通过"-->
<Condition>
  <Apply unctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        Policies have been Checked
      </AttributeValue>
    </Apply>
  </Condition>
 </Rule>
</Policy>
```

(3) 应急策略

在供应链中,常常会有紧急的事件发生,比如当某产品发生质量问题时,需要对产品实行召回,在召回的过程就需要利用发现服务来对有质量问题的产品进行跟踪和召回。如果要对产品在整个供应链的范围内进行跟踪,就需要有特殊的权限来访问供应链信息,这样就需要一种应对这种突发事件的应急策略。

实现这种紧急访问控制方案的一个方法是,让数据的拥有者或受信任的第三方动态地调整访问控制策略。如果这种紧急事件发生的频率很低,这种方法还是比较合适的,但是如果这种事件发生的频率比较高,那么策略管理的负担就会很大,而且也可能引起机密数据的泄露,因而,我们需要寻找一种自动的机制来应对这种紧急事件。

可以这样定义紧急事件:发布一个安全令牌,声明某个紧急事件已经发生。我们可以设想一个紧急事件的权威机构,当某个事件满足供应链定义的紧急情况时,它负责令牌的发放。利用这种令牌,访问者可以激活存储在发现服务上的应急策略,进而访问数据,另外还可以对这种令牌进行有效期设置,规定它在某个时间段内才能使用。

(4) 行业监管策略

在很多行业中,发现服务可能会强制执行一系列的访问策略。这种强制的策略可能由发现服务的用户共同制定,或来自行业的约束,或者出于监管部门管理的需要。例如,这种策略或许是声明所有发布者在发布记录之前都应该对记录进行电子签名,或声明这种策略不允许被删除,或声明审计员可以访问所有的数据等。尽管发布者可以对其数据的访问进行控制,但是发布者的策略却不允许覆盖发现服务制定的这种强制执行的策略。解决这种策略的冲突,可以给策略赋予不同的优先级,级别高的策略可以覆盖级别低的策略,见图 6。

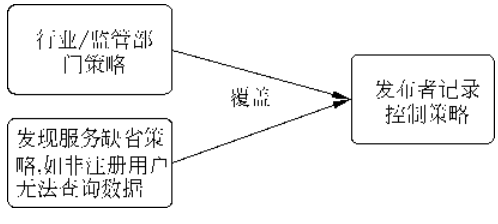

图 6 策略优先级

在 XACML 策略描述语言中,没有一个专门的元素<Precedence>来表示策略的优先级,因而利用现有的 XACML 语言表示访问控制策略的优先级还需要采用特别的办法。

我们知道 EPC 码[11]能够唯一标识实体,EPC 码的不同区域代表不同的含义,可以参考 EPC 码的编码方

式来设定访问控制策略的ID值,进而设定策略的优先级。设定策略ID——"policyId"的通用格式:

urn:policyid:Precedence.PublishId.SerialNumber

其中,Precedence为策略的优先级,PublishId为策略发布者的发布ID(可以为用户的ID或发现服务的ID、行业监管者的ID),Precedence和PublishId在用户注册阶段由发现服务统一分配,SerialNumber是策略的序列号,可以由系统自动生成。由三个部分组成的"policyId"不仅可以唯一标识策略,也可以表示策略的优先级信息。三个数据域的位数可以结合实际需求进行设定。

5 结论

发现服务是EPC网络的核心组成部分,并且是实现供应链各企业信息共享和构建物品跟踪网络的关键服务,为了管理存储在发现服务上的记录和策略并满足供应链EPC网络应用的各种需求,发现服务的管理者也要制定访问控制策略。与传统的访问控制机制不同的是,保护企业隐私的访问控制策略主要是由企业自己来制定的,而发现服务只作为策略的执行者。企业通过发现服务发布RFID数据记录进行数据共享的同时,也要提交自定义的访问控制策略来保护数据隐私。同时,为了管理存储在发现服务上的记录和策略,并且为了满足供应链EPC网络应用的各种需求,发现服务的管理者也要制定访问控制策略。我们把发现服务的访问控制策略分为两种类型:用户端策略和服务端策略。基于供应链RFID应用实例,并结合RFID的数据特点和企业用户隐私保护需求,我们得到用户端的各种访问控制策略;同时在实例基础上,根据EPC网络的实际应用需求提出了四种服务端的访问控制策略。

参考文献

[1] Juels A. RFID security and privacy: A research survey[J]. IEEE Journal on selected area in communication,2006,24(2): 381-394.

[2] Fung C,Cao M,Desai B,Xu H. Privacy protection on RFID data[C]. 24th ACM SIGAPP Symposium on Applied Computing,March 8,2009,Hawaii,U. S. A.

[3] Molnar D & Wagner D. Privacy and security in library RFID: Issues, practices, and architectures[C]. ACM Conference on Computer and Communications Security,2004: 210-219.

[4] Zhang X L,King B. Security Requirements for RFID computing systems[J]. International Journal of Network Security,2008,6(2): 214-226.

[5] Han S H,Chu C H,Liu Z Y. Security and Privacy threat in RFID Traceability. Network[J]. Journal of Southeast University(English Edition),2008,24(6): 132-135.

[6] Karygiannis T et al. Guidelines for Securing Radio Frequency Identification (RFID) Systems[M]. Special Publication,National Institue of Standards and Technology,2007: 80-98.

[7] Aigner M. et al.,D-4. 1. 1: Security Analysis[M],Ilic A ed.,Building Radio Frequency Identification for the Global Environment(BRIDGE),2007.

[8] Garfinkel S L,Juels A & Pappu R. RFID privacy: An overview of problems and proposed solutions[J]. IEEE Security & Privacy Magazine,2005,3(3): 34-43.

[9] Agrawal R,Cheung A,Kailing K et al. Towards traceability across sovereign,distributed RFID database[C]. Proc. 10th International Database Engineering & Applications Symposium,New Delhi,India,2006.

[10] Ilic A,Michahelles F,Fleisch E. The Dual ownership model: Using Organizational Relationships for Access Control in Safety Supply Chains[C]. IEEE International Symposium on Ubisafe Computing, Ontario,

Canada,2007.
[11] EPCglobal. EPC Tag Data Standards Version 1. 1 Rev. 1. 240[EB/OL]. http:// www. epcglobalinc. org/standards/tds/tds_1_1_rev_1_27-standard-20050510. pdf,2005.
[12] OASIS. XACML v3. 0 Administration Policy Version 1. 0[EB/OL]. http://www. oasis-open. org/committees/download. php/31747/xacml-3. 0-core-wd-10. zip,2006.

Policy-based Privacy Protection for EPC Information-Sharing Network

HAN Shuihua & DU Chaokan
(School of Management,Xiamen University,Fujian,Xiamen 361005)

Abstract Security and privacy has been a significant factor for further development of RFID technology,currently rarely has explored security and privacy risks in depth over the entire supply chain domain from the management,operational and technical levels. Here we are trying to propose a policy-based privacy protection framework for EPC network system,aiming at addressing many typical access control requirements for a large scale RFID Network deploymen. We first analyze the information-sharing model of EPC Network,then propose a basic access control framework of Discovery Services. After that,taking a RFID application in the supply chain for example,we analyze various access control policies of Discovery Services both in client-side and in service-side. Finally, we analyze a potential implementation and considerations over the manageability of complex distributed security policies.

Key words EPC network,Privacy Protection,Access Control

作者简介

韩水华,男,1970 年生,博士,厦门大学管理学院教授。主要研究方向:电子商务与信息系统。
杜超坎,男,1984 年生,厦门大学管理科学与工程硕士生。