一般化 RFID 安全认证授权协议模型

王 涛
WANG Tao

华南师范大学 计算机学院,广州 510631
School of Computer,South China Normal University,Guangzhou 510631,China
E-mail:filion@tom.com

WANG Tao.General RFID authentication and authorization protocol model.Computer Engineering and Applications,2008,44(20):57-60.

Abstract: RFID is prevented from further usage by its security problems.A General RFID Authentication and Authorization Protocol Model(GRAAP Model) was introduced,an adjustment on the data access process of Seo's RFID four roles model was made to simplify the RFID application authentication process so as to satisfy the practical usage requirement,new roles(RFID tag manager,data owner,data carrier,data accessing entity,etc.) were introduced,as well as the basic structure,roles' responsibility and systematic protocol prototypes of this model.Comparing to the former RFID authentication protocol prototype,it is more flexible and can be the base of newer and more sophisticated managing,authentication and authorization protocols of RFID devices.
Key words: RFID;security model;identification authentication;security protocol

摘 要:RFID 技术安全性存在的问题阻碍了它的进一步应用。提出了一个一般化 RFID 安全认证授权协议模型,在 Seo 等提出的 RFID 四角色模型的基础上调整了系统读写过程以便简化 RFID 应用模型且更接近实用要求,并引入了 RFID 标签管理者、数据所有者、数据运载者和数据读取者等新角色,给出了新的 RFID 认证/授权模型的基本结构、角色职责和实现该模型的系统化协议原型。与之前的 RFID 认证授权模型相比更加灵活,可以在此基础上实现 RFID 设备之间更加多样的管理、认证、授权模式。
关键词:射频识别(RFID);安全模型;身份认证;安全协议
DOI:10.3778/j.issn.1002-8331.2008.20.017 **文章编号:**1002-8331(2008)20-0057-04 **文献标识码:**A **中图分类号:**TP309

1 RFID 安全及 RFID 认证协议研究现状

1.1 RFID 技术背景

无线射频识别技术(RFID)是自动数据识别技术的一种高级形式。RFID 技术的应用范围随着其软硬件的发展而不断扩展,包括供应链管理(物流\配送\仓储)、零售、畜牧、采矿、安全防盗、交通、体育运动、工业生产、产品防伪等许多方面都有应用[1],是现代高新数据处理技术的一种基础技术。而随着实际应用的展开,又提出了许多新的应用方式。目前美国使用的 E-Passport、香港的智能身份证,都是以 RFID 技术为基础实现的,将数据与人结合起来的一个最新的实例,甚至出现了在未来的欧元钞票上装入 RFID 芯片的方案。

1.2 RFID 中的安全问题

但随着 RFID 技术越来越广泛地应用,尤其是用于身份证明、货币电子化等领域之后,RFID 技术原有的安全问题变得越来越严重。RFID 广泛运用于门禁和安全系统(如汽车防盗)已经出现了安全问题;而且基于 RFID 技术的 E-passport(电子护照)应用于人的身份识别,包括美国使用的 E-Passport 同样存在安全问题[2]。

信息安全问题已成为制约 RFID 技术应用发展的一大因素[3]。RFID 技术采用无线数据交换,这是 RFID 技术的一大优势,但在安全方面这也是它的一大缺陷:攻击者不用接近 RFID 芯片就可把其数据读出。越来越多的 RFID 技术应用(尤其是涉及大量金钱、个人身份信息和国家安全的应用)都要求 RFID 技术在使用时可以提供令人放心的安全性。但可以说,目前的 RFID 安全问题仍然无有效的解决方法。

1.2.1 RFID 中的安全问题的集中表现

(1)芯片中数据的泄露;

(2)使用者隐私被泄露:芯片数据以及芯片出现位置都会反映使用者行为模式、生活习惯等;

(3)读卡器、芯片的数据传送泄露商业活动的相关信息;

(4)读卡器被欺骗,接收虚假、伪造数据的写入。

1.2.2 RFID 出现上述安全问题的原因

RFID 芯片计算及存储能力相对较差,无法提供加密及认证所需的计算能力。公钥密码算法为了达到一定的安全性,需要使用大数字(位数达到几十位到上千位的数字)运算。这当然要求有大量计算能力和存储空间,而这种计算能力的要求是一

基金项目:广东省自然科学基金 (the Natural Science Foundation of Guangdong Province of China under Grant No.06300905)。
作者简介:王涛(1975-),男,博士,讲师,主要研究领域为安全协议分析与设计、RFID 安全协议。
收稿日期:2007-10-09 **修回日期:**2008-01-23

般低成本 RFID 设备无法提供的。因此,RFID 环境中运行的安全协议和安全运算一般都是轻量级的(Lightweight),或者叫“低代价”(low cost)的,也即需要的计算代价和存储代价都是极低的。

没有好的安全体系以利用相对较小的计算能力实现加密\身份认证:目前,在 RFID 环境中,还没有提出可以实现完善的认证,同时又可以适应低成本 RFID 设备计算能力的方案。这也是为什么设计 RFID 安全认证协议十分困难的一个原因。

1.2.3 RFID 安全问题的研究内容和目前的一些解决方案

RFID 安全技术研究内容:使得 RFID 芯片的数据不会被恶意修改或被泄露到不应获得它的攻击者手里;使得 RFID 芯片不会向冒充的读卡器返回数据;使得 RFID 芯片的使用不会使得使用者的隐私和正当权益受到侵害;使得 RFID 读卡器不会被虚假(冒充的 RFID 芯片)数据欺骗。

目前 RFID 技术安全问题的解决方案分两大类:硬件物理解决方案;软件处理解决方案。硬件物理解决方案是利用电路[4]及通信频率控制[5]实现安全性。但由于技术难度\控制灵活性和频率范围限制等因素,这些硬件解决方案无法灵活使用。而基于 RFID 芯片简易计算能力实现的分布式安全访问协议等软件处理解决方案则有更多的优点,因此成为目前 RFID 安全控制技术研究的主流和热点。

1.2.4 现有的 RFID 安全控制协议方案

在周永彬等的综述性文章[6]中,介绍了一些 RFID 安全协议,但都有一定的缺陷,并且都无法提供比较通用的一般化认证协议。而最近 RFID 技术又出现了一些新的进展。其中一种思路是 Seo 等提出的、由中介设备协助 RFID 芯片进行认证工作[7]。虽然这一方案并不是一个通用化的 RFID 认证协议(每次读取都需要中介设备在场,这一点导致了这一模型不实用),但受这一方案启发,我们提出了一个一般化的 RFID 认证授权协议模型。

2 一般化的 RFID 认证授权协议模型

2.1 认证协议模型的目标

(1)可授权性:保证芯片的所有者可以管理对芯片的读取。

(2)保密性:保证 RFID 设备只能从芯片中读取被授权读取的数据。

(3)匿名性:保证芯片除了使用者的设备外,无法被追踪。

(4)可认证性:保证不同所有者的不同芯片可以互相区分;保证芯片在必要时可以证明其所有者是谁。

为了比较包括这里提出的协议模型在内的几个 RFID 数据存取协议模型的优劣,设想这一情况:顾客在超市购买商品,通过商品上的 RFID 标签进行结帐后,商家将不可再识别这些 RFID 标签(已经付费的商品商家不应该再可读取其数据),但顾客希望这些标签仍可被家里的 RFID 读写器(例如冰箱上的 RFID 读取器)识别,以便标记每种商品的购入日期(例如对新鲜食物可以自动提醒在保鲜期内食用),而邻居带进自己家里的类似商品信息则不会读取到自己家的系统中。这就要求 RFID 数据传输实现认证和授权:RFID 标签知道是什么样的读写器试图读取自己的数据,并根据该读写器的授权级别去提供相应数据。这一应用场景在后面简称为“RFID 授权读写模型场景”。

2.2 现有的 RFID 安全协议模型

现有的 RFID 安全协议模型有三个参与者:RFID 标签 T(Tag),RFID 标签读写设备 R(Reader),后端服务器 S(Server)。其中前两者完成 RFID 远程数据读写工作,后端服务器进行数据存储和查找等复杂数据处理工作。这种模型在本文后面简称为“简单 RFID 数据读取模型”,其工作过程如图 1 所示。

这种模式是最早出现的、相对简单的 RFID 应用模式,也是目前主流的 RFID 应用模式,但这一模型已经越来越不适用于 RFID 标签的管理和应用,因此这其中没有任何授权和认证,从而存在安全问题。例如,RFID 标签无法被管理和控制,因为 RFID 读取设备是读取数据的,它当然希望读取的数据越多越好;而 RFID 标签数据的所有者(即 RFID 标签所依附的物品的所有者,如商家、顾客等),虽然希望对数据的存取进行管理,但无法管理,因为在这一模型中能够对 RFID 标签进行读写的只有 RFID 读写设备,而这些设备不是标签所有者可以控制的。

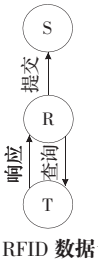

图 1 简单 RFID 数据读取模型

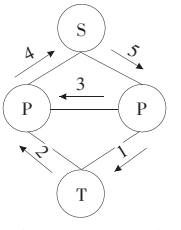

图 2 SALK 模型

2.3 SALK 安全认证协议模型

在 Seo 等的模型中(后面简称为 SALK 模型),增加了一个角色——代理 P(Proxy),这一角色负责与 R 进行认证工作,并负责对 T 进行管理。这一模式提高了对 T 的管理能力,使得即使 T 计算能力不强也可以进行认证和授权管理。但这一模式要求每次 T 与 R 之间的 RFID 读写操作都要有 P 的参与,在 P 通过 R 将 T 传递的数据转移给 S 并分析后,R 才能获得它被授权访问的数据,每次的 RFID 读写都要完成认证和授权两种操作。其处理模式如图 2 所示。

实际上,RFID 技术要实现的就是 RFID 标签与读写器之间的快速、远程数据交换,这是 RFID 技术的优势。如果每次读写都要经过复杂的数据交换和处理过程(从图 2 中 1 至 5 的全部步骤完成后,才完成一次 R 与 T 之间的数据交换),并且要求一个额外设备 P 进行 RFID 标签的数据处理,这一方面降低了可以应用的领域,另一方面也会使应用更加复杂、成本更高(P 本身就是一个 RFID 读写器)。因此,这一模型并不实用。

2.4 本文提出的认证授权协议模型

虽然 SALK 模型存在问题,但代理这一新角色的引入给我们解决前述简单 RFID 模型中 RFID 标签无法管理的问题带来了新的思路。基于此,提出新的 RFID 数据读写模型(称为 GRAA 模型,General RFID Authentication and Authorization Model)。如图 3 所示。在这个模型中,有4 个角色,它们的职责如下:

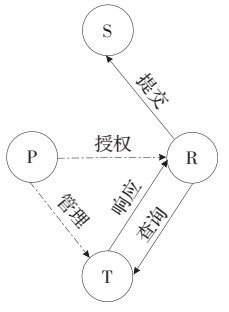

图 3 本文提出的模型

(1)RFID 数据运载者 T

T 是 RFID 数据标签芯片,是运载 RFID 数据的实体,与物品进行物理连接(例如粘贴在物品上)。

(2)RFID 芯片管理者 P

P 是 T 的管理者(这里,P 同样是一个 RFID 读写器)。为实现对 T 的管理功能,P 本身应该具有一定的数据计算和存储能力。一个 P 可以管理多个 T。P 对 T 的管理职责如下:

①P 可修改 T 的管理者:即可以转让 T 给其他代理 P′来管理。

②P 可以确定 T 的使用者:T 的使用者一般是 RFID 读写器 R。

③P 可以修改 T 的数据:对 T 的全部或部分数据拥有全部或部分修改权限。

④P 可以对 T 的使用者进行授权:授权给 T 的使用者读取或修改 T 的全部或某些数据的权利。当然,P 授予使用者的权限不应该多于 P 本身所拥有的权限。

而 P 与 T 的数据管理关系可能有如下情况(可根据这两种不同的关系设计不同的 RFID 安全协议):

①T 仅负责运载 RFID 数据,它本身不知道所运载数据的内容,或不能对所运载的数据进行修改;P 负责进行数据授权和认证管理外,也负责数据的生成和修改(即 P 是 T 上数据的唯一所有者,T 只是运载者);

②P 只负责对 T 数据读取的授权和认证管理,而不管理 T 上的数据。这样 T 是 T 上数据的所有者和运载者,而 P 只是认证和授权读取的管理者。

(3)RFID 数据读取者 R

R 是 RFID 读写器,也是标签 T 的使用者,R 向 T 提出数据读取或写入要求,T 根据对 R 的授权执行或拒绝这些要求。

(4)RFID 数据使用者 S

S 则是后端服务器,与前述模型中的功能一致。

2.5　本文的模型与其他模型的比较

与 SALK 模型相比,P 只在授权时参与;而单次 RFID 数据读写只需在 R 与 T 之间进行,无需 P 的参与。因此,本模型在实现效率、成本、使用灵活性方面都要远远优于 SALK 模型。

如果不需要 P,则这一模式与"简单 RFID 模型"一样。

P 的实现方式也可以十分灵活,例如在上面的"RFID 授权读写模型场景"中,可以由超市的 RFID 读写器提供 P 的功能,把这些商品标签 T 的管理者由超市 RFID 读写器转移为家里的 RFID 读写器(这时 P 和 R 的功能重合了),以便生成可以在顾客家里的 RFID 设备读取数据的授权。而如果对超市商家的诚信没有把握,则可以由第三方提供自助的代理实现上述授权,而顾客自己没有必要购买一个 RFID 读写设备实现 P 的功能。

3　模型工作协议原型

为实现上述模型,定义相应的协议原型如下。

3.1　管理权确认/转移协议原型

协议目标:本文模型实现的基础,是 P 与 T 之间建立管理与被管理的关系,而这种关系的建立有两种情况:(1)T 是空白标签,没有任何管理权的设定,而 P 通过写入管理权数据确认管理权;(2)T 原来属于 P,P 通过管理权转移协议将管理权转交给 P′,从此 T 由 P′管理。而对应这两种情况,分别有管理权确认协议和管理权转移协议。

3.1.1　管理权确认协议原型

协议过程:

(1)P 将自己的保密信息进行运算,生成查询字符串 qm;

(2)P→T:query-manager,qm,NP;

(3)T 将收到的 qm 与自己存放的 P 保密信息进行运算,如果证明 P 是自己的管理者,则返回 YES,如果是其他管理者,返回 no,如果没有管理者,则返回 NULL;

(4)T→P:query-manager-yes/no/null;

(5)如果 P 收到是"是"或"否",则协议结束,如果是 NULL,表示现在没有管理者,则继续。P 根据自己的保密信息,计算出访问自己下属标签所需要的访问验证串 AVS;

(6)P→T:cmd-confirm-management,F(AVS),NP;

(7)T 收到 F(AVS),计算出 P 的特征串,将 P 的特征串和自己的访问验证串保存下来。

由于这一过程中,T 的计算能力不强,T 与 P 之间没有任何认证机制,这一协议的大多数步骤应该在保密的\安全的信道上进行,例如可在电磁屏蔽的房间内进行 P 与 T 的远程 RFID 读写,或者如果 T 有外部线路接口,也可以通过物理线路连接进行安全的数据读写。

3.1.2　管理权转移协议原型

协议过程:

(1)未来的管理者 P′利用计算自己的保密信息计算 AVS′;

(2)P′→P:F(AVS′);

(3)P 将自己的保密信息进行运算,计算 F(AVS);

(4)P→T:cmd-change-manager(all-cover.或 half-cover),F(AVS),F(AVS′),NP;

(5)T 将收到的 F(AVS)与自己存放的 P 特征串进行运算,如果证明 P 是自己的管理者,则从 AVS′计算 P′的特征串。注意,这里可以用 all-cover.或 half-cover 参数控制是否要用 AVS′替换原来的验证字符串 AVS,如果替换,则 T 无法再被 R 访问,R 要访问 T,要向 P′重新申请访问授权。

3.2　管理权释放\标签失效协议原型

协议目标:当标签 T 不再使用时,P 可以释放 T 或使 T 失效(两者的区别是:前者使 T 无管理者,但必要时通过管理权确认协议还可再次被某个 P 管理使用;后者则使 T 永远失效,不能再被使用)。无论是释放还是失效,都可以命令 T 清除 T 中的所有有效数据。

协议过程:

(1)P 利用计算自己的保密信息计算 AVS;

(2)P→P:cmd-release-manager(release 或 invalid),F(AVS);

(3)T 将收到的 F(AVS)与自己存放的 P 特征串进行运算,如果证明 P 是自己的管理者,则执行释放或失效操作。注意,这里用 release 或 invalid 参数,可以控制释放 T 或使 T 失效。

3.3　授权协议原型

协议目标:P、R 之间相互认证后,R 向 P 请求对 P 所管辖的标签 T 的权限,P 进行授权。由于 P 和 R 都可以看成高性能计算设备,它们之间可以进行基于公钥密码算法和数字证书上的复杂认证过程。

协议过程:

(1)P←→R:P 与 R 之间的互相认证过程,这可以采用现有的成熟安全协议进行,不在本文讨论范围之内,这里略去;

(2)R→P:cmd-auth-request,NR;

(3)P 根据业务要求,判断是否同意,如果同意,则给 R 赋予相应的授权级别 I,并根据自己的保密信息,计算出 R 的授权串 AP-R-I;

(4)P→R:H(cmd-auth-request,NR),ENC(PKR,AP-R-I),A(IDR)=F(IDR,AP-R-I)。AP-R 为 P 给 R 读取所有 P 管理的标签授予 I 级权限。注意,R 应无法从 A(IDR)中提取出,也无法修改 A(IDR)以获得更高的权限级别。

以后,R 可以通过 AP-R-I 对标签 T 进行访问,而不必每次都经过 P 的认证和授权。

3.4 普通读写协议原型

协议目标:R 向附近的标签 T 发送处理请求(读取或写入),T 判断其是否为有效用户。如是,则根据 R 从 P 处所获得的授权,提供符合其授权级别的数据给 R;如否,则拒绝提供数据。

协议过程:

(1)R→T:F(IDR),NR;

R 向 T 发送查询请求,要求提供数据。其中,IDR 为 R 的标识符;

(2)T 收到 IDR,(根据 T 自己 PINT 码信息)构造一个查询回复串 Rr,返回给 R;

(3)T→R:Rr,NR;

(4)R 收到 T 的返回串 Rr,经过和自己所掌握的授权串 A(IDR)计算,算出一个访问串 V,其中包含了 T 的 PIN 码和访问授权级别 I(但注意 R 无法从 V 中计算出 T 的 PIN 码和授权级别 I);

(5)R→T:V,NR,cmd;

(6)T 收到 V,跟自己的访问验证串 AVS 进行运算,算出 PIN 码和授权级别 I;根据 PIN 码判断,这次访问是对自己的合法访问;根据授权 I,执行 cmd 所标明的操作(读取或修改数据)。

例外情况:当 T 为空白标签时,上述过程无法完成。

注意:这里只是给出协议原型,没有给出具体实现;上述各协议中的同名临时值表示一个在该协议中有效的局部变量,也即各个协议中的同名临时值不是同一个值。

3.5 性能和应用场景分析

这一模型可以适应 RFID 标签计算和存储能力很低的情况,因为标签本身只是执行一些很简单的运算,只需要存储很简单的数据值。真正的认证和授权工作涉及大量的计算和存储,则由芯片管理者 P 来完成。P 可能是一个 RFID 读写器或一个可直接连接 RFID 芯片 T 的设备(如手机、PDA 或 PC 等)。它可以与想读取 T 上数据的 RFID 读写器 R 直接通过 P 与 R 之间后台网络中的安全信道利用传统加密、认证方法进行认证和授权,从而解决了 RFID 芯片计算/存储能力不足导致无法完成认证和授权的问题。但这种 P 与 R 之间的认证和授权只有一次。在之后 R 读取 T 上数据的授权认证是在每次读取时进行,只涉及 R 和 T,不必像 SALK 模型一样每次都要求 P 协助进行认证,因此保证模型运作效率较高。

但这里也没有规定实现存取控制等的具体方式,例如,如果 T 有自己的计算能力和存储能力,它可以自己进行授权管理和控制,有自己的授权访问列表等,而 P 只进行管理权的转移和控制等。

因此,本模型是非常灵活的,可以基于本模型根据具体环境去设计和实现适应于特定应用方案的认证\授权协议。

4 结束语

本模型明确提出了:在 RFID 应用模型中,应该有一个设备角色,它代表物理物品的所有者对物品的 RFID 标签进行管理,对 RFID 标签的读写访问、授权、认证等进行统一控制;但它只应该进行总体认证和授权关系确定这两项工作,不应每次都参与 RFID 数据读写。它的出现可以实现 RFID 数据提供方(标签)和数据使用方(读写器)在计算能力上的平衡,从而解决之前困扰 RFID 安全认证协议实现上的问题(标签计算能力不足的问题)。

随后提出的协议原型,则是建立了在这个一般化 RFID 认证授权模型中实现 RFID 标签管理\认证\授权\读写的一般过程模型和数据模型,为以后 RFID 认证授权模型设计和实现进行准备。

参考文献:

[1] 游战清,李苏剑.无线射频识别技术(RFID)理论与应用[M].北京:电子工业出版社,2004.

[2] Juels A,Molnar D,Wagner D.Security and privacy issues in E-passports[C]//Proceedings of IEEE SecureComm,2005:23-29.

[3] 半导体咨询事业部. 中国 RFID 市场现状与发展前景研究报告[R].赛迪顾问股份有限公司,2005.

[4] Juels A,Rivest R L,Szydlo M.The blocker tag:selective blocking of RFID tags for consumer privacy[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security.[S.l.]:ACM Press,2003:45-51.

[5] RSA Security.Securing RFID tags from eavesdropping[R].RSA Security,2004.

[6] 周永彬,冯登国.RFID 安全协议的设计与分析[C]//中国科学院软件研究所 2005 中国计算机大会论文集,2005:94-99.

[7] Seo Youngjoon,Asano Tomoyuki,Lee Hyunrok,et al.A lightweight protocol enabling ownership transfer and granular data access of RFID tags[C]//Proceeding of Symposium on Cryptography and Information Security(SCIS'07),2007.

(上接 56 页)

[3] 段海滨.蚁群算法原理及其应用[M].北京:科学出版社,2005:238-244.

[4] 梁文,罗文坚.基于生态捕食模型的多目标优化问题求解算法[J].中国科学技术大学学报,2005,35(3):360-366.

[5] 万旭,林健良,杨晓伟.改进的最大-最小蚂蚁算法在有时间窗车辆路径问题中的应用[J].计算机集成制造系统,2005,11(4):573-576.

[6] 丁建立,陈增强,袁著祉.遗传算法与蚂蚁算法的融合[J].计算机研究与发展,2003,40(9):1351-1356.

[7] Bullnheimer B,Hartl R,Strauss C.An improved ant system algorithm for the vehicle routing problem[J].Annals of Operation Research,1999,89(13):319-328.

[8] Brysy O,Dullaert W.A fast evolutionary metaheuristic for the vehicle routing problem with time windows[J].International Journal of Artifical Intelligence Tools,2002,12(2):143-157.