RFID 生产线安全问题①

龚茜茹, 赵建超

(河南工业职业技术学院 计算机工程系, 南阳 473009)

摘 要: 使用攻击树模型, 对基于 RFID 的生产线系统安全问题做出了分析, 根据攻击树模式模型描述的问题, 给出了相应的安全策略. 采用定向法拉第网罩来解决标签读写安全问题; 采用 HASH 链来解决标签信息安全问题; 采用基于数字签名的双向认证系统来解决通信安全问题; 建立一个整体的信息安全管理体系来解决生产线整体的安全问题.

关键词: RFID; 安全; 攻击树; 数字签名; 生产线

Security Issues of RFID Production Line

GONG Qian-Ru, Zhao Jian-Chao

(Department of Computer Engineering, Henan Polytechnic Institute, Nanyang 473009, China)

Abstract: This article uses attack tree model to analysis the RFID-based production line system security issues; gives the corresponding security policy according to the questions described by the attack tree mode model. Directional Faraday net is used to solve the problem of the safety of the RFID reader. The HASH chain is used to solve the problem of the RFID information security. Mutual authentication system based on digital signatures is used to solve the communication security issues. An overall information security management system is established to solve the whole security issues of the production line.

Key words: RFID; safe; attack tree; digital signature; production line

由于 RFID 具有稳定性好、非接触识别、抗干扰能力强等特点. 随着 RFID 系统成本的进一步降低, 在制造业的应用得到进一步推广. 在汽车生产和销售领域, 同样得到了广泛的应用. 例如宝马公司在收到用户订单的时候, 会在汽车装配生产线上应用 RFID 完成该订单, 确保汽车的个性化装配任务在流水线上完成. 除此之外, 福特、丰田等公司也有自己的 RFID 生产线系统. 国内的某汽车生产厂家, 根据自己的实际情况, 设计了自己的 RFID 汽车生产线[1]. 但是, 由于 RFID 本身运算能力差, 在 RFID 的读写、数据交换、信息传输等环节, 存在很大的安全隐患[2].

1 系统结构

以汽车生产线为例, 某公司基于 RFID 的汽车生产线信息管理系统如图 1 所示.

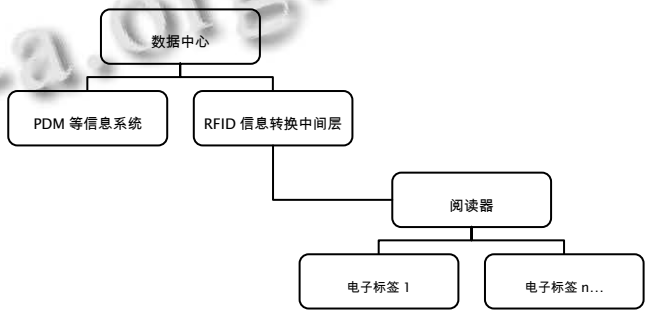

图 1 RFID 汽车生产线信息管理系统

从图中可以看出, 该系统分为四层组成. 位于最下面一层的为电子标签层. 电子标签贯穿于汽车生产的整个过程, 在车体和主要零部件上都部署有电子标

① 基金项目:河南省科技攻关计划项目(142102210556)
收稿时间:2014-04-17;收到修改稿时间:2014-05-08

签, 电子标签负责记录整车的生产信息, 包括主要部件的生产场地、生产日期, 重要环节的生产、检测过程等相关资料.

电子标签的数据, 必须经过相应授权的阅读器才能进行阅读, 不同的阅读器具有不同的权限, 能且仅仅只能阅读指定的电子标签. 中间件层主要实现数据格式的转化和车间质量监控系统. 为了提高系统的通用性, 该系统采用 B/S 模式. 阅读器的数据, 需要转化为标准的 XML 数据, 才能提交服务器. 而同样为了实现质量监控的快速反应, 车间设有及时监控系统, 即时反映生产环节的情况. 服务器保存有整个生产环节的信息, 可以实现与原来的信息管理系统无缝接轨[3].

2 安全威胁的攻击树模型

Bruce Scheier 提出一种信息安全的分析方法[4], 它采用树型结构用来模拟攻击, 树的每一条路径, 代表一种攻击方法(如图 2 所示). 该模型的每个叶子代表一个攻击行为, 树的根表示攻击的最终目标. 模型中叶子的关系为“与”和“或”两种, “与”表示两片叶子相互依赖, 必须同时完成才能到父节点. “或”表示为两片独立的叶子, 都能独立通往父节点.

电子标签的信息位于整个系统中, 攻击树模型如下: 攻击者采用非授权读写器获得 RFID 信息, 或截获系统通信过程, 或者竞争对手进行系统渗透, 直接在服务器中获取信息, 或者内部人员在管理系统上提取信息. 攻击模型的生成树描述如图 2 所示.

G0:窃取 RFID 标签信息
OR G1: 直接读取数据
AND G11:确定 RFID 的频段
AND G12: 确定标签的激活能量
AND G13: 确定标签的协议
OR G2: 读写器攻击
OR G21:通过伪造冒充合法读写器获取标签信息
OR G22:合法读写器上获得标签信息
　OR G3: 服务器
　OR: 通信过程截获
　OR: 冒充合法用户获取信息
　OR G4: 信息管理系统各个授权环节

图 2　攻击描述

从图中可以看出, 到达根 G0 可以经由四条分支的任一分支即可, 每条分支又有不同的子分支组成. 那么窃取 RFID 标签信息可以通过四种方法, 完成任意一种方法即可达到目的. 这样, 攻击者只根据上图, 找到任意一条可以到达根节点的路径即可. 可以把上述攻击图像化, 如图 3.

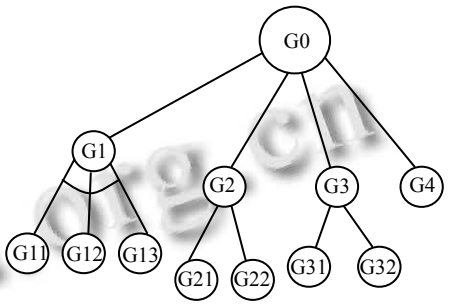

图 3　攻击树模型

经过分析, 可以到达根节点的路径有以下 6 条:

第一条, {G11,G12,G13,G0};第二条: {G21, G0};第三条: {G22, G0};第四条: {G31, G0}; 第五条: {G32, G0}; 第六条: {G4, G0}.

3 安全策略设计

3.1 路径 1 安全设计: 定向法拉第网罩

对于第一条路径来说, 主要为最底层的通信问题. RFID 协会专家组(RFID ExpertsGroup)针对底层通信, 包括电子标签本身、标签到阅读器无线通信安全, 制订了相应的安全规范(AIM REG 314). 规范中的方法包括: 杀死(Kill)标签、主动干扰、阻止标签、法拉第网罩等. 杀死(Kill)标签原理是使标签彻底销毁, 任何读写器都不能对该标签进行后续的跟踪, 这显然不符合需求. 主动干扰标签频谱的信号是一种屏蔽标签的方法, 可是在汽车生产线这种大规模使用电子标签的系统中无法使用, 否则会出现非法干扰, 严重的时候使得整个系统的其他电子标签无法工作. 阻止标签是在系统中设置一个特殊的阻止标签, 使用干扰防碰撞算法来实现, 这个标签对非法阅读器应答为相同的数据, 从而保护标签. 由于阻止标签会带来整个系统大幅度的成本上升, 因此不能采用. 法拉第网罩的工作原理就是电磁波屏蔽, 即使用金属材料的容器装置电

子标签, 这样外部的阅读器信号将无法进入法拉第网罩, 从而无法激活电子标签[5].

根据本条路径的实际情况, 安全设计如下:

确定 RFID 的频段. 工作频率选择是 RFID 安全设计中的一个很重要的问题. 频段不同, RFID 具有各自优缺点, 主要是标签的性能和价格. 根据实际情况, 选择超高频(UHF)的 RFID, 这种标签, 穿透能力较差, 可以使用法拉第网罩来进行完全屏蔽. UHF 电子标签可以选择如下: 长 13.5 厘米、宽 2.5 厘米, 频率 915MHz, 合 EPC global Class1 Generation2 标准.

RFID 天线的设计是另外一个重要的问题, 实际上, 如何有效利用天线进行标签屏蔽和实现有效覆盖, 是 RFID 技术研究的一个重要方向[6].

可以在指向阅读器的位置, 使用定向天线来解决这个问题, 典型的天线频率范围为 902~928Mhz, 尺寸为长 21 厘米、宽 21 厘米, 厚 6.5 厘米. 同时使用定向法拉第网罩进行屏蔽(只在指定放行电磁波). 这样能够有效避免多个方向的安全防护问题, 可以低成本的实现物理层防护.

3.2 路径 2、3 安全设计: HASH 链

对于路径 2 来说, 只要对标签信息进行加密, 那么攻击人即使获得标签信息, 也无法还原标签内容. 采用匿名 ID 、重加密方案等公钥加密技术, 攻击者者即使在消息传递过程中截获标签信息也不能获得标签的真实 ID. 公钥加密的计算量, 通常大约为对称加密的 1000 倍, 公钥的计算负载超出了标签的能力, 将导致整个系统成本的增加, 在汽车生产线这种大规模的 RFID 应用肯定是不合适的.

可以采用 Hash 锁来对标签的信息进行单向加密[7], 由于 Hash 函数很容易实现, 因此成本很低. RFID 卡的序列号在全球具有唯一性, 在生产过程中已被固化, 是该标签的身份标志. 阅读器 B 系统中保存需要读取的标签访问密钥 K, 并保存 HASH 后的 HASH 值(HID), 其中 HID =Hash(K). 该值具有唯一性, 并与标签 A 的 ID 一一对应.

验证过程如下:

A 在激活后会发送 HID 作为响应, HID 一个 HASH 值, 即使此时被截获, 也不能得到 K 值.

B 同样也无法通过解密 HID 得到密钥 K, 只能通过数据库中查找对应 HID 对应的密钥 K, 标签 A 可以通过 Hash(K), 用来验证 B 的身份, 然后发送标签真实信息给阅读器. 由于无法通过 Hash(K)来还原出 K, 因此, B 的身份得到验证.

在安全需要更高的部门, 如汽车产品质量溯源等部门, 可以采用 Hash 链来解决.

3.3 路径 4、5 安全设计: 基于数字签名的双向认证系统

对应路径 4、5 的安全设计来说, 如果仅仅为了保证数据通信的安全, 可以采用 VPN 来实现, VPN 是一种非常成熟的数据保密通信方式, 在 B/S 模式下有非常成熟的技术方案. 但是 VPN 没有数字签名, 无法实现产品质量监控, 因此无法直接采用. 考虑到电子标签信息量很小, 公钥加密对系统影响很小, 因此采用基于数字签名的双向认证系统, 如图 4.

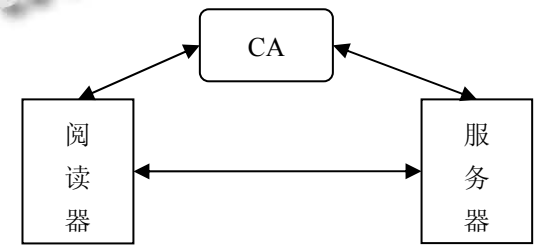

图 4 基于数字签名的双向认证系统

假定阅读器为 X, 服务器为 Y, CA 中心为 A. 系统运行时, X、Y 分别从 CA 中心申请了自己的证书, 证书的公钥信息 EKUx、EKUy 保存在 CA 中心, 在阅读器上保存私钥 EKRx, IDx 为阅读器的编号, 服务器 Y 上保存私钥 EKRy,M 为阅读器读到的电子标签信息.

认证过程过程如下:

X->Y: IDx||EKRx[IDx||EKUy(EKRx[R])|| R]

当 X 需要连接服务器的时候, 首先使用 Y 的证书对随机数 R 进行加密, 并添加随机数 R 和自己的 ID 号码, 然后用自己的私钥 EKRx 对消息进行加密, 形成一个经过签名且保密的消息.

Y 收到消息后, 与 CA 中心联系, 获得 X 的公钥 EKUx 后, 完成服务器对阅读器的签名验证. 验证成功后, 将将随机数 R 签名后重新发送给 X.

Y -> X: EKRy[IDx||EKUx(EKRy[R])|| R]

X 得到消息后, 会用 Y 的公钥证书对消息进行解读, 将 R 值与发送成功的 R 进行比较, 从而完成整个身份验证过程.

身份认证成功后, 双方可以使用自己的签名发送消息.

3.4 路径 6 安全设计: 建立一个整体的信息安全管理体系

路径 6 为信息管理系统各个授权环节, 只要这个环节能够获取信息. 包括 ERP、PDM 等. 在这些系统技术安全防范中, 都有一套成熟的方法. 由于这个系统环节众多, 因此, 必须建立一个整体的信息安全管理体系保障汽车生产线 RFID 信息安全.

汽车企业普遍建立了 ISO9001 质量管理体系或者类型的质量管理体制, 在汽车制造企业应用 RFID 信息管理系统, 完全可以在 ISO9000 的基础上再进行重构.

该模式基本过程如下:

制订安全方案: 根据每个部分的安全需要, 建立与信息安全规定、信息安全处理过程、权限、授权流程.

企业实施: 企业的各个部门实施安全方案.

安全督察: 有独立的第三方对安全进行评估和督察.

再改进: 对安全漏洞进行再改进.

4 安全系统总体设计

针对安全策略的研究, RFID 生产线的安全整体设计如图 5.

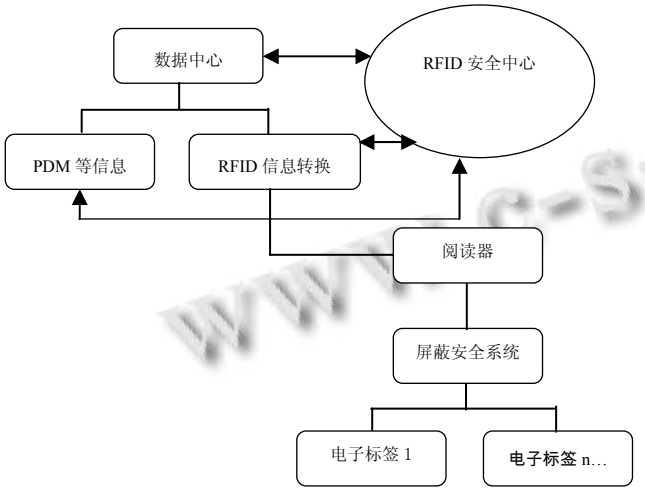

图 5 RFID 生产线的安全整体设计

从图 5 中可以看出, 在电子标签和阅读器中, 增加了屏蔽安全系统, 保证了标签的读写安全. 增加了 RFID 安全中心, 该安全中心与原有数据中心, PDM 等原有信息系统, RFID 信息转换中间层进行连接. RFID 安全中心处理有关 RFID 的安全问题, 具备 CA 认证和产品 HASH 信息处理功能. 对 PDM 等原有信息系统提供权威的 RFID 生产线安全查询, 对生产线的生产过程提供权威的安全信息处理.

5 结语

生成树模型成功描述了 RFID 生产线的安全问题. 但是, “三分技术, 七分管理”, 由于 RFID 技术刚刚在生产线上得到大规模的应用, 其安全问题尚未引起足够的重视. 因此, 需要在安全管理上更进一步下功夫, 才能保证系统的安全.

参考文献

1 倪霖.基于 RFID 的汽车生产线信息集成模式及关键技术研究[博士学位论文].重庆:重庆大学,2010.

2 Muir S. RFID security concerns. Library Hi. Tech., 2007, 25 (1): 95−107.

3 李文川.汽车制造企业 RFID 采纳过程模型及应用问题研究[博士学位论文].重庆:重庆大学,2011.

4 Schneier B. Attack trees: Modeling security threats. Dr Dobb’s Journal, 1999: 21.

5 彭志威,杜江,张建.RFID 的安全与隐私.中兴通讯技术,2007,13(4):28−33.

6 朱正.射频识别技术频率选择的一些考虑.中国电子商情(RFID 技术与应用),2006,(2):52−54.

7 丁振华,李锦涛,冯波.基于 Hash 函数的 RFID 安全认证协议研究.计算机研究与发展,2009,46(4):583−592.