基于RFID系统的安全性问题研究

史艳伟 张岩庆 刘克胜
(电子工程学院 合肥 230037)

摘 要 随着RFID技术的飞速发展与广泛应用,RFID系统的自身安全威胁及基于其的恶意代码也在快速发展。为了更好地对抗安全威胁和恶意代码,需要透彻地分析了解其原理。详细分析了当前RFID系统的自身安全问题及现有的攻击手段,给出了相应的防范措施;并根据RFID系统的特点,提出了基于RFID系统的恶意代码免疫模型。

关键词 RFID技术,恶意代码,免疫模型,安全,攻击
中图法分类号 TP391.44 **文献标识码** A

Study of Security Problem Based on RFID System

SHI Yan-wei ZHANG Yan-qing LIU Ke-sheng
(Electronic Engineering Institute, Hefei 230037, China)

Abstract With the rapid development and wide application of RFID technology, RFID system's security threats and malware of them also develop quickly. In order to prevent from them, we need to know their theories better. This paper particularly analyzed existing security problems and malware of RFID system, and gave some defense measures. At last, according to the characters of RFID system, the paper proposed a malware's immune model based on RFID system.

Keywords RFID technology, Malware, Immune model, Security, Attack

对于无处不在的网络来说,RFID(Radio Frequency Identification,无线射频识别)已经成为网络技术中的一种很重要的技术,该技术最早诞生于第二次世界大战,是战机的敌我识别(IFF)技术的发展[1]。随着该技术的不断创新和飞速突破,其已广泛应用到人类社会生活的各个方面,如物流和供应链管理、航空行李处理、文档追踪/图书管理、身份标识等。

一直以来,人们只是对使用RFID产生的个人和企业隐私及相关安全问题颇多忧虑,但是2006年荷兰研究人员通过实验证明了即使这种廉价芯片上的内存容量极小,RFID标签在病毒面前也是十分脆弱的。他们指出,RFID标签可能会感染上一种病毒,这种病毒可以传染并影响后台使用无线射频识别软件的数据库,并能轻易地向其它RFID标签传播[2]。为了更好地对抗这种基于RFID的恶意代码,本文对其传播方式进行了研究并给出了防范措施。

1 RFID相关知识

1.1 RFID技术

RFID系统主要由RFID标签(应答器)、RFID阅读器(询问器)、天线、计算机网络和最终处理RFID标签所携带信息的软件组成。其工作原理为:RFID标签首先进入RFID阅读器读写范围,标签信息被阅读器读取并交给RFID中间件处理,RFID中间件遵照协议,进行数据解析、ID验证、信息过滤等一系列的数据处理工作,然后将数据交付到后台系统。

依据内部电源的有、无,RFID标签分为被动式、半被动式(也称作半主动式)、主动式3类。一般来说,主动式标签拥有较长的读取距离和较大的内存容量用来储存读取器所传送来的一些附加讯息[3]。

1.2 基于RFID的安全问题

下面是对RFID中的数据安全的定义[4]。

• 存取数据受约束:读取和写入数据库的信息需要经过认证。

• 接入系统受约束:接入系统的所有设备必须经过认证并且是可信的。

• 系统是安全的,值得信赖的:最基本的一点是系统必须是安全可靠的。

RFID技术在安全和隐私方面存在缺陷,RFID系统的安全大多依赖于中间件的发展,也取决于RFID标签中包含的数据,这些数据可能会导致SQL注入攻击、拒绝服务攻击和缓冲区溢出等。

1.2.1 RFID安全威胁

(1)嗅探。任何对应的阅读设备都可能读取标签信息,阅读行为无需标签负荷知晓,并且可以远距离发生。

(2)跟踪。阅读器在特定地点可记录独特的可视标签识别器,然后与个人身份相联系。

(3)应答攻击。攻击者使用应答设备拦截、转发RFID查询[2]。

(4)拒绝服务。Denial of Service(DoS)阻止RFID系统正常工作,如信令拥塞会阻止射频波与标签之间的通信。

1.2.2 RFID风险

(1)数据读取出错。网络出错、中间件被病毒感染或数据

史艳伟(1985—),女,硕士生,主要研究方向为信息安全,E-mail:shiyw861163.com@yeah.net;张岩庆(1987—),男,硕士生,主要研究方向为信息安全;刘克胜(1968—),男,博士,教授,主要研究方向为信息安全。

传输时信号中断等都可发生导致统计数据不精确。

(2)商业情报泄露。攻击者非法访问 RFID 系统获取商业敏感信息。

(3)个人隐私暴露。通过跟踪驻留在商品中的标签获取顾客的住址及一些个人信息。

(4)外部风险。RFID 系统与外部网络连接时对这些网络的攻击会间接或直接威胁到 RFID 系统。

1.2.3 RFID 通信相关的安全问题

标签阅读器有两种通信方法:通过因特网协议(IP)传输数据和通过低功率无线电(radio frequency,RF)提供并收集发送或到达标签的数据,这两种方法都存在一些安全问题。

(1)通过 IP 传输数据

未经授权接入网络是重要的安全威胁,应该防止任何恶意设备接入网络。使用 SSL 和 SSH 等技术可以确保网络安全,这些技术关闭了一些可以被攻击者恶意利用的端口以确保系统更安全。较多的安全工具和较高的技术标准,使得该通信方式相对来说比较安全。

(2)通过低功率 RF 提供和收集数据

这种方法在空中进行,会导致一些严重的威胁:

· 未授权标签接入(导致嗅探)。所有的标签在理论上都应先通过 RFID 阅读器的认证再被读取。但是标签内的漏洞使假冒的阅读器可以读取标签内的完整信息,并向标签内写入任意恶意数据,甚至可以终止或毁坏标签。由于标签可以在 RFID 阅读器范围内的任何地方被读取,因此它可以用来盗取数字护照[2]。

· 克隆标签(导致欺骗)。克隆标签是原始标签的未授权复制品,阅读器会以为其是原始的标签而阅读它,因而可以非法地接入阅读器。克隆标签会注入错误的或恶意的数据到系统,破坏系统和系统内数据的完整性,Johns Hopkins University 和 RSA Security 展示了该攻击[5]。

· 信道攻击(导致重放攻击)。目前最大的安全威胁是恶意设备在标签和阅读器之间偷听它们的通信,并伺机窃取口令和其他敏感信息,这同时会导致中间人攻击事件。

2 基于 RFID 的攻击

2.1 缓冲区溢出

缓冲器溢出是最常见的一种软件攻击。缓冲区溢出是指当计算机向缓冲区内填充数据位数时超过了缓冲区本身的容量,溢出的数据覆盖在合法数据上。

缓冲器溢出是指入侵者直接(如用户输入)或间接(通过环境变量)地输入数据,该输入数据大于内存中分配给缓冲区的长度,使之溢出并覆盖在合法数据上。程序控制数据在内存中的位置通常与数据缓冲区相邻,缓冲区溢出使程序随意执行代码。RFID 标签缓冲区溢出将危及中间件后台系统安全,标签数据一般少于 1024bit,但 150—15693 中"write muhiple blocks"命令允许标签重复发送同一数据模块,最终填满应用层缓存。

2.2 SQL 注入

SQL 注入是由应用程序数据库层的安全漏洞导致的,它是一种利用 Web 站点通过伪造请求者的输入来改变后台 SQL 语句的攻击技术。在 RFID 系统中,这种漏洞常见于中间件。SQL 注入有几种方法,包括不正确过滤换码符和不正确的类型转换。

中间件读取来自 RFID 阅读器的数据,因为不涉及到数据库,故无法对数据库进行任何有意义的攻击。例如,一个人要进入某个房间,就需要通过认证,RFID 标签包含了这个人的 ID 号和姓名,中间件会用 SQL 查询语句来进行认证,查询返回非空值,这个人就可以进入房间。攻击者可以使用不正确过滤换码符来进行 SQL 注入,使得查询结果总会返回一个非空值;这还会导致拒绝服务攻击,即 SQL 查询时删除查询表使得没有人可以通过认证。当该数据库和网络或因特网连接时更危险,特别是 SQL 语句通过 Web 站点和 URLs 执行时。

2.3 基于 RFID 的蠕虫

蠕虫是利用应用程序中的安全缺陷通过网络进行自我传播的程序。蠕虫不需要人为地去主动传播,通常有负载来执行诸如删除文件、通过 email 传递信息、插入软件代码等工作,最常见的负载是在受感染的主机上开后门,以方便攻击者以后进入该计算机系统。

RFID 蠕虫[6]利用 RFID 在线服务的漏洞进行传播,不需要用户做任何事情(如扫描 RFID 标签),其传播开始于 RFID 蠕虫通过网络第一次发现 RFID 中间件服务器并感染时。RFID 蠕虫也可以通过 RFID 标签进行传播,感染了蠕虫的 RFID 中间件会利用标签上的漏洞感染 RFID 标签。这个漏洞使新的 RFID 中间件服务器远程下载并执行某个文件,该文件会和标准恶意代码使用同样的方法感染 RFID 中间件。

2.4 基于 RFID 的病毒

与 RFID 蠕虫依赖于 RFID 系统与网络的相连不同,RFID 病毒是不需要连接网络,只要利用基于 RFID 的漏洞便可以独立复制自身代码到新的标签的程序,RFID 病毒可能带有负载也可能没有。使用新感染的 RFID 标签时,标签会感染其他的 RFID 系统(假设使用相同的软件系统);被感染的 RFID 系统感染其他的 RFID 标签,这些标签再感染另外的 RFID 系统,如此循环感染以传播病毒。

2.5 基于 RFID 的碎片式恶意代码

恶意代码给 RFID 应用系统的使用者带来了很大的威胁,但这些代码也存在着一些问题,如受 RFID 标签内存大小限制,某些恶意代码由于体积太大而无法完整地放入标签内;标签中完整的恶意代码很容易被受害者及防护软件发现等。为了解决这些问题,文献[7]提出了基于 RFID 的碎片式恶意代码,该方法是先根据恶意代码的总大小及每个 RFID 标签的可用空间大小把恶意代码等分为若干碎片,并依次将其放入 RFID 标签内。而在中间件处,碎片数据会变成 SQL 查询语句的格式被提交给数据库服务器,这些碎片存储在数据库的一个单独的表中,而这个表必须在所有的碎片被 RFID 阅读器读取之前创建,为此必须准备一个专门的标签来创建这个表;再准备一个单独的标签用于存储包含碎片合并和触发机制的数据,一旦该标签被读取,所有的碎片将被合并为一个单独的可执行文件——攻击者创建的恶意代码,并触发该可执行文件。

3 基于 RFID 系统的恶意代码免疫模型

当前,针对 RFID 系统的恶意代码的检测模型还较少,且大都基于传统的特征码检测,检测效率低,不能很好地对抗当前基于 RFID 系统的恶意代码攻击。为此,本文提出了基于 RFID 系统的恶意代码免疫[8]模型。

3.1 防范措施

为应对基于 RFID 的攻击，有两部分需要增加防御机制，即中间件和数据库，这两部分是 RFID 系统的主要组成部分。对此，Rieback 提出了一系列针对 RFID 恶意代码的防御措施[2]，它们同样对碎片式攻击有效，这些防御措施包括：

- 检查中间件代码；
- 锁定用户账号；
- 关闭或删除不必要的属性；
- 通过禁止向 SQL 语句里复制数据和一条语句只允许查询一次来避免 SQL 注入；
- 限制或阻止函数获得当前的查询来阻止病毒传播；
- 关闭 SSI，避免基于网络的攻击；
- 严格地检查缓冲区边界，阻止缓冲区溢出。

3.2 免疫模型的安全策略

本文根据 RFID 系统各个部分的特点，给出了针对各个部分的相应的安全策略。

(1)RFID 标签

RFID 标签是用来存储数据的，很少包含 SQL 语句，可以禁止在 RFID 标签内使用 SQL 语句，而应该在中间件使用 SQL 语句。设计 RFID 标签时，在标签内建立一种安全机制，当用户写入数据时该机制对写入的数据进行检查，若为 SQL 语句格式则报警并提醒该格式不被允许，否则数据是安全的。同时也要确保标签内没有包含十六进制数据，因为恶意代码很可能会被转换为十六进制存放于标签内。

(2)RFID 标签与阅读器

利用 RFID 标签进行碎片式攻击时，一般攻击者会选择使用自己的标签，这样便于向标签内存储攻击者构建的数据。为了防止这种未经许可的标签接入 RFID 阅读器进而攻击数据库服务器，应加强 RFID 标签和阅读器之间的认证。可以利用密码技术中的签名机制，使标签带有特殊的签名，当标签进入阅读器可读取的范围后，阅读器首先读取该标签的签名，确认为正确的签名后再读取其他数据，过程如图 1 所示。

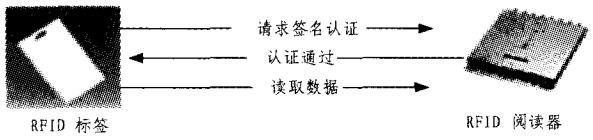

图 1 RFID 标签与阅读器的认证过程

(3)RFID 阅读器

RFID 阅读器创建一个标签 ID 不需要太多的字节。统计阅读器创建一个标签 ID 需要的字节数，归纳总结后取最大值作为阅读器读取标签内数据的上限，当阅读器读取的数据超过该上限或要读取整个 RFID 标签时提示报警。

(4)中间件和数据库

尽可能地只使用一个中间件和一个脱离其他系统的数据库，这样可以防止恶意代码向其他系统传播。若要与网络连接，应在可控的环境下进行。当从 RFID 数据库合并数据并通过网络传递到另一个数据库时，应配置防火墙使数据只在数据库之间传输，当然，手动传输(如通过 U 盘)会更安全。一般来说，RFID 标签内的正常数据不需要合并为可执行文件，因此，应该屏蔽掉 RFID 数据库内的 shell 命令等类似功能的命令。

3.3 恶意代码免疫模型

根据以上的安全策略，本文设计了基于 RFID 系统的恶意代码免疫模型。该模型分固有免疫系统和适应性免疫系统两部分，固有免疫系统主要用来检测数据是否合法，且是否为恶意代码；适应性免疫系统是针对一些恶意代码特征码库中没有的数据进行检测的，在检测过程中使用了行为检测方法，其模型如图 2 所示。

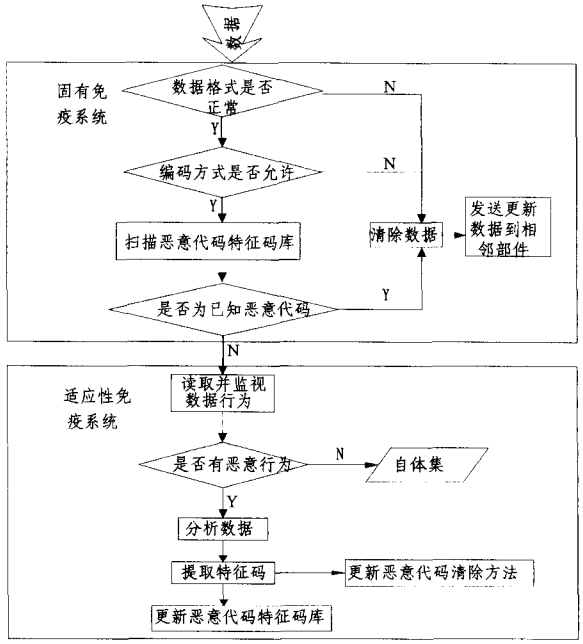

图 2 基于 RFID 系统的恶意代码免疫模型

结束语 随着 RFID 技术理论的成熟和应用的推广，RFID 系统将逐渐渗透到人们的生活当中并给人们带来极大的便利，但是由此带来的安全问题也不容小觑，各种针对 RFID 的恶意代码将扑面而来，防不胜防。本文详细分析了基于 RFID 系统的各种安全问题及可能存在的各种攻击手段，并给出了相应的防范措施；最后根据 RFID 应用系统的特点，提出了基于 RFID 系统的恶意代码免疫模型，它对有效检测当前针对 RFID 系统的恶意代码具有一定的意义。

参 考 文 献

[1] 张秋剑. RFID 系统环节的攻击与威胁的分析及解决方案的设计[D]. 上海：上海师范大学，2010：1-3

[2] Rieback M，Crispo B，Tanenbaum A. Is your cat infected with a computer virus [J]. IEEE Percom，2006

[3] 射频识别[EB/OL]. http://zh. wikipedia. org/wiki/RFID，2011-08-23

[4] Karygiannis T，Eydt B，Barber G. Guidance for Securing RFID Systems [J]. National Institute of Standards and Technology，2007：7-30

[5] Bono S C，Green M，Stubblefield A. Security Analysis of a Cryptographically-enabled RFID Device[C]//14th USENIX Security Symposium. 2005

[6] Sulaiman A，Mukkamala S，Sung A. SQL infections through RFID [J]. J Comput Virol，2008，4：347-356

[7] Shankarapani M K，Sulaiman A，Mukkamala S. Fragmented malware through RFID and its defenses [J]. J Comput Virol，2009，5：187-198

[8] 杨海东，杨春. RFID 安全问题研究[J]. 微计算机信息，2008，24：238-240