基于有限自动机的RFID入侵检测

杨晓明[1,2]，张 翔[1]，王佳昊[1]，吴 劲[1]，秦志光[1]

(1. 电子科技大学计算机科学与工程学院 成都 611731; 2. 工业和信息化部电子第五研究所 广州 天河区 510610)

【摘要】利用RFID中间件的特点，加入入侵检测异常检测模块，通过对入侵者的攻击数据流与RFID系统内部的数据流进行对比后提取特征向量，并通过对入侵数据流对应子模块的归纳建立有限自动机，对有限自动机的归并来提高系统入侵检测的效率。此外，参照归并后的有限自动机对攻击进行分类，通过对攻击本质的分析与提取来检测一部分入侵检测自动机里没有相应的攻击。最后，对固定攻击比例的访问事件样本乱序进行试验，试验结果表示系统在3轮测试中均得到稳定的检测率。

关 键 词 攻击分类; 有限自动机; 入侵检测; RFID

中图分类号 TP393 文献标志码 A doi:10.3969/j.issn.1001-0548.2014.05.025

RFID Intrusion Detection with Finite Automation

YANG Xiao-ming[1,2], ZHANG Xiang[1], WANG Jia-hao[1], WU Jin[1], and QIN Zhi-guang[1]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731;
2. The fifth research institute of MII Tianhe Guangzhou 510610)

Abstract Based on the characteristics of RIFD middleware, the paper adds an intrusion detection system in RFID middleware to gather the feature vector from the comparison between intrusion data stream with RIFD internal data stream and establish finite automation according to intrusion data steam corresponding to sub-module. The efficiency of the intrusion detection system is improved via the consolidation of some of finite automation. Besides, the proposed system can achieve the classification of RFID attacks from finite automation, and even detect some unknown attacks through analyzing the nature of the attacks. By randomizing the order of access events which has mixed attack events in fixed proportion, the system can achieve stable detection rates in 3 rounds tests.

Key words attack classification; finite automation; intrusion detection; RFID

随着对RFID系统研究与使用的深入，其安全性也越来越受到人们重视。目前针对RFID系统的攻击主要有3类：1) 针对通信协议的攻击；2) 物理破解标签的攻击；3) 针对RFID上层应用的攻击。对于这些攻击，现阶段研究最多的是读写器与标签之间的通信协议，它具有典型的RFID通信特征[1]。

随着RFID标准协议的推出，协议中的漏洞亟待解决，越来越多的人尝试着通过改进协议解决其固有安全问题[2-3]。但是由于RFID的物理硬件的局限性和这些改进协议本身存在的一些问题，还没有一种改进协议能广泛的使用[4]。更换通信协议需要从硬件入手，必定导致新旧RFID系统兼容存在一定的困难，从而大幅度地增加更换安全协议的成本。

为了达到增强现有协议而无需大幅增加资金投入的目的，本文采取入侵检测办法，从分析入侵RFID系统的步骤入手。使用有限自动机分别描述每一种攻击，再通过不同的自动机合并模型状态，从而达到建立入侵检测模型的目的，使之能够对异常数据流模式进行检测与告警。

一般情况下，读写器收取的数据包是有序的，并且在同一个读写器覆盖区域内考虑只有一个攻击者尝试入侵。攻击者可以通过USRP、开源阅读器等设备监听无线信道中读写器和标签的正常通行，进行会话分析、篡改及注入等操作。

本文采用的技术能够有效覆盖DOS、标签信息泄漏及标签可追踪等主要攻击类型，并对一部分未知攻击能够根据攻击本质进行检测，具有良好的扩展性。

收稿日期：2013 – 07 – 05；修回日期：2013 – 12 – 17

基金项目：中央高校基本科研业务费(ZYGX2011J066)；四川省科技支撑计划(2013GZ0022)；国家自然科学基金(61003230)；新疆教育厅教育科学研究项目(XJEDU2013I28)

作者简介：杨晓明(1974 –)，男，博士生，高级工程师，主要从事信息安全方面的研究.

1 相关知识及研究现状

1.1 RFID系统分层以及RFID中间件的特点

完整的RFID系统可以用逻辑分层的方式来研究，从下到上可以分为标签层、读写器层、RFID中间件层和上层应用层[5]。它们无论是在硬件还是软件方面都有很大的差异，其中的RFID中间件层相对于标签层和读写器层具有较强的计算和存储能力，能够进行比较复杂的运算。

1.2 有限自动机在入侵检测中的应用

有限自动机是计算理论中的一种基础理论计算模型，有着广泛的应用，其中模式匹配就是其重要应用之一。基于传统网络的入侵检测系统(network intrusion detection system, NIDS)大多采用模式匹配技术进行入侵检测[6]。其成熟的理论模型可以被有效地引入RFID通信过程的入侵检测技术中[7]。

1.3 RFID中间件的安全性研究

随着RFID系统安全逐渐被人们重视，RFID中间件的安全性作为RFID系统安全的重要组成部分也逐渐被大家考虑。有关RFID中间件的安全问题主要分为两类：1) RFID中间件自身的安全问题；2) 利用RFID中间件的相对优势来维护整个RFID系统的安全。

第一类安全问题通常划为传统软件安全问题，常用的解决办法是设置权限。在中间件与网络连接的地方使用一些安全措施防止网络的攻击；中间件与数据库连接的地方采用一些手段来保证数据的安全等[8]。第二类安全问题是RFID中间件从系统的局部到整体来维护系统安全[9]。文献[10]对基于上下文感知计算的方法进行了比较深入的研究，这样的系统能够很好地检测标签位置移动的异常行为，但针对不同的RFID应用场景需要不同的设定，普适性较差，而且对于针对标签敏感信息获取的攻击的检测能力较差。文献[11]提出了基于免疫和多Agent的入侵检测，该方法是基于数据挖掘方式，具有再学习的能力和较强的适应能力。但是由于RFID通信协议比传统网络的通信协议简单，现阶段针对单一协议的攻击数量有限，数据挖掘需要的训练集往往不够，而且由于是无线通信，通信双方存在不对称性，数据挖掘的特征提取存在一定的困难。文献[12]提出了在无线信道中抓取信号，对这些信号进行学习，设定门阀值，超过门阀值时定义为入侵行为，以此来标签拥有者是否改变。把信号存放在文件中，由于RFID系统的简单性和门阀值的设置难以掌握，同时大量规则比对将影响大规模的RFID系统的吞吐率，造成环境适应性和系统效率不能得到保证。文献[13]提出的基于*K*平均算法的RFID入侵检测，使用了数据挖掘中的聚类算法，在给定的数据集合中寻找同类的数据子集合，每一个子集合形成一个类簇，同类簇中的数据具有更大的相似性。但是该方法还是受到了RFID的限制，即训练集的稀缺难以得到适用性高的准则函数。

本文利用基于有限自动机的入侵检测解决第二类安全问题，专注整个RFID系统安全，即使只有少量的攻击样本也能建模，具有一定的普适性和较好的延展性。归并以后的有限自动机数目相对于数据挖掘产生的规则要少，使得整个RFID系统的通信效率得到提升。

2 基于有限自动机的RFID入侵检测

本文提出的入侵检测模块在RFID中间件层实现，具有较强的计算能力。通过监听读写器从信道中抓取的信息包与系统内部的信息包进行比较发现异常，送往检测模块，如果经过自动机模型匹配发现攻击则报告给处理模块并且系统进入下一轮的异常捕捉，如果不是入侵系统则进入下一轮的异常捕捉。图1所示是系统检测过程。

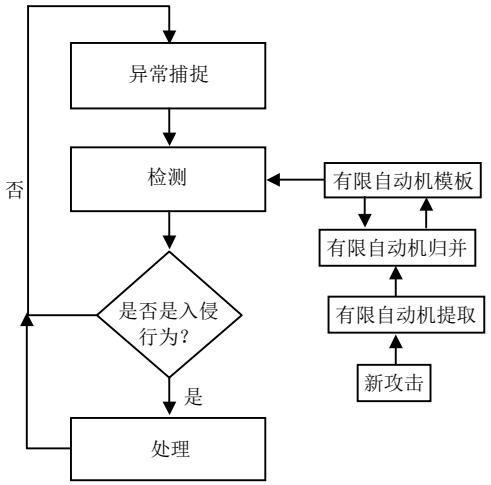

图1 RFID入侵检测流程

对于新出现的RFID攻击类型，可以图1所示的流程提取该攻击的有限自动机，然后提交给有限自动机归并模块，该模块将尝试新RFID攻击的有限自动机与系统已有的RFID攻击有限自动机模板进行归并并且返回给有限自动机模板模块。

3 入侵检测模块设计

3.1 入侵检测模块的逻辑位置

入侵检测模块的位置处于RFID中间件层，RFID

中间件需要接收读写器层识读的数据，经过处理给上层的应用提供统一接口，图2是其在整个RFID系统中的逻辑位置。由处于中间件层中的入侵检测模块和处于读写器层的监视读写器(可能有多个)构成。监视读写器类似于攻击者监听设备，不发射任何信息，只收集信道中的信息。它被用来收集无线信道里的信息，并将信息与系统内部的信息进行对比，如果不符合则产生了异常。通过预设的攻击模型对异常集的分析可判断系统是否受到攻击。

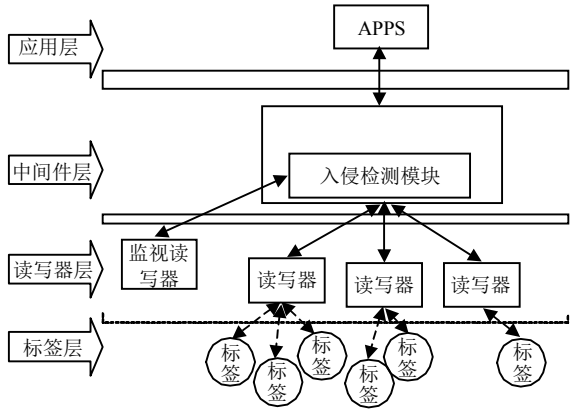

图2　入侵检测模块逻辑位置

检测的具体流程如图3所示，信道的数据流和系统数据流综合以后提取异常，然后根据时间顺序形成异常特征组，异常特征组将与多个检测自动机匹配攻击模型，检测入侵行为。

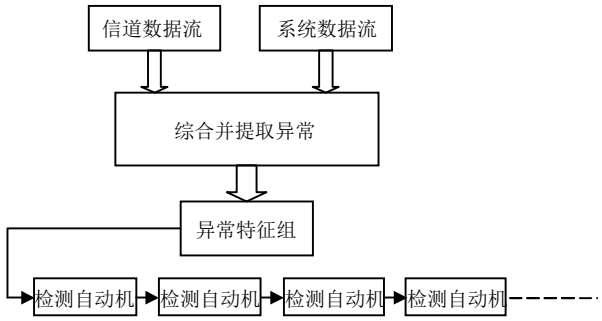

图3　信道异常检测流程图

3.2　入侵检测特征向量的抓取

本文提出的入侵检测系统的关键是利用有限自动机构造异常行为的模型。本文首先选取其中的一些子攻击类型进行分析，通过描述其有限状态机行为过程建立攻击模型，然后再对多个自动机模型进行归并，最后提取出具有一定通用性和覆盖率的RFID系统攻击模型。

本文通过RFID读写器的命令和标签是否有回应，来推测标签的状态。由异常检测获得的异常可以由特征向量表示：<Command，Status，Timestamp>其中Command命令是读写器发出的命令，Status表示标签可能的状态，Timestamp时间戳是监听读写器监听到命令的时间先后情况。

本文定义开始节点到节点i的深度就是最短到i的路径经历过的节点数。将特征向量根据时间戳排序可以形成异常向量表。有限自动机的状态在状态节点的深度上保持标签可能的状态的一致性，但不同的节点深度也可能是一样的标签可能状态。标签可能的状态和收到的命令共同决定自动机状态，通过不同的读写器命令来进行状态转移。状态转移的路径表示同一命令或者同一类型的命令(即能使标签达到同一状态的命令)。

3.3　RFID入侵检测有限自动机的构造

有限自动机M由一个五元组构成：$M=(K,\sum,\delta,q_0,F)$，其中，K是状态的有限集合；$\sum$是有限输入字母表；δ是$K*\sum$的K的一种映射；q_0是初始状态，$q_0\in K$；F是结束状态集合，$F\subseteq K$。若当自动机处于状态q，并且发生了a状态以后，M转换状态到p，则记为$\delta(q,a)=p$。

下面是一个攻击者在没有被LOCK的用户区上读写标签信息的例子，由监听读写器抓取的攻击者的异常行为如表1所示。

表1　在未被LOCK的存储区读写标签攻击的抓包情况

命令	标签可能的状态	时间戳
开始	未上电	1.0
Query	Reply/arbitrate	1.5
Ack	Acknowledge	2.7
Query	Reply/arbitrate	3.5
Ack	Acknowledge	4.5
Req_RN	Open/secured	6.1
Read	Open/secured	7.0
Write	Open/secured	9.2
Query	Reply/arbitrate	10.1

表1按监听读写器抓包的时间戳排序，从表中提取异常集合的主要步骤：<开始,没上电,1.0>到<Query,Reply/arbitrate,1.5>到<ACK,Acknowledged,4.5>完成第一个子步骤，即完成攻击者读写器对标签的盘存阶段命令集。然后是<Req_RN,open/secured,6.1>,<Read,Open/secured,7.0>。根据对于入侵主线的描述可以构建有限自动机：$M=(K,\sum,\delta,q_0,F)$，$K=\{s_0,s_1,s_2,s_3,s_4,s_5\}$，$\sum=\{r_0,r_1,r_2,r_3,r_4,r_5,r_6,r_7\}$，其中，$r_0$表示query类型的命令；$r_1$表示ACK类型的命令；$r_2$表示Req-RN类型的命令；$r_3$表示读写类型的命令；$r_4,r_5,r_6,r_7$表示重复接到与已经到达的标签可能状态相同的命令(如在s_2的状态下接收到了r_4)，它们不能改变标签的可能状态；$F=\{s_4,s_5\}$。

映射$K_x\sum_>K$为$\delta(s_0,r_0)=s_1$，$\delta(s_1,r_0)=s_1$，

$\delta(s_2, r_0) = s_1$ ， $\delta(s_1, r_1) = s_2$ ， $\delta(s_2, r_2) = s_3$ ，
$\delta(s_3, r_3) = s_4$ ， $\delta(s_3, r_3) = s_5$ ， $\delta(s_2, r_4) = s_2$ ，
$\delta(s_3, r_5) = s_3$ ， $\delta(s_4, r_6) = s_4$ ， $\delta(s_5, r_6) = s_5$ ，
$\delta(s_4, r_7) = s_5$ ， $\delta(s_5, r_7) = s_4$ 。

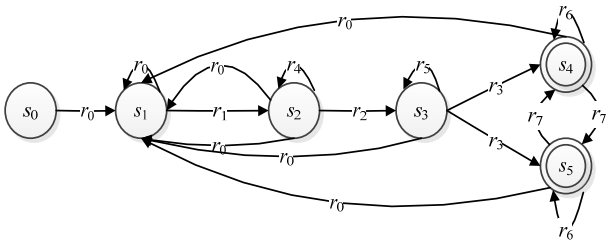

图4 在没有被LOCK的用户区上读写标签信息的攻击

图4为各状态的有限自动机，其中的各个状态的含义为： s_0 为开始状态，标签未上电； s_4, s_5 是结束状态，表明攻击者已经开始读写标签； s_1 是标签接到Query类的命令，可能处于Reply或者arbitrate的状态； s_2 是标签接收到ACK类型的命令，可能处于Acknowledge状态； s_3 是标签接收到Req_RN类型的命令，可能处于Open或者secured的状态。

3.4 RFID攻击模型的归并

由于标准协议的漏洞很多，如果需要串行的套用入侵检测有限自动机将带来较大计算复杂度和时延。因为简单串行套用这些模型则需要建立多进程或者多线程，上下文的频繁切换将导致较大的系统资源消耗，所以将一系列的有限自动机归并起来是一种有效的解决办法。

通过一系列的有限自动机的归并还将带来两点优势：1) 通过对归并完成的有限自动机进行分析提取出某些攻击专门针对有限自动机中的某一个或者若干个节点来采取行动，可以对RFID入侵行为进行分类分析，降低分析难度并提高模型对攻击行为的识读率。2) 通过尝试提取一些攻击的共同特征，判断分析潜在未知威胁，降低攻击漏报率。

本文根据RFID系统的特点提出了适用于RFID系统入侵检测的有限自动机归并算法。算法如下：

1) built old_set //建立旧节点集
insert (all nodes ∈ old state automaton) into old_set
//有序插入所有的节点到集合
for all nodes ∈ old_set do
if(*i*<*j* && node(*i*).timestamp > node(*j*).timestamp)
exchange(node(*i*),node(*j*))
end if
end for
2) built new_set //建立新节点集合
insert old_set(first) into new_set,
delete(old_set(first))
3) tryget (old_set(first)) //取节点
if(node(first) exist)
node(first) = old_set(first)
delete(old_set(first))
do step 4)
else
do step 6)
end if
4) for all node(*j*) ∈ old_set do //相似节点合并
if(similar (node(first), node(*j*)))
merge(node(first), node(*j*))
do step 3)
else
do step 5)
end if
end for
5) for all node(*j*) ∈ old_set //没有相似节点
if(node(first).state == node(*j*).state)
insert node(first) into same_list _of(node(*j*))
do step 3)
end if
end for
insert node(first) into (last_list + 1)
do step 3)
6) set all road belong to same node same number
//指向自身的路径设置为相同的标号
7) output new_set

4 攻击分类与潜在威胁的预测

4.1 基于有限自动机归并的RFID攻击

对于一些攻击合并到上述的自动机具有一定难度，如DOS攻击、堵塞信道、或者发送Qurey、QueryAdjust、QueryRep命令使得读写器与标签通信中断，标签返回仲裁状态等。然而其他一部分的攻击可以通过3.4节所述的RFID入侵检测有限自动机归并原则进行归并。

表2 部分RFID攻击

攻击标号	攻击名称或者攻击描述	最终状态
1	复制标签的PC/EPC	s_2
2	标签的仿冒	s_2
3	暴力破解ACCESS密码	s_4
4	使用ACCESS密码LOCK住标签	s_6
5	标签没有被LOCK时，尝试读写标签	s_7
6	入侵者LOCK以后，尝试读写标签	s_7
7	向标签写入特定的数据实现跟踪	s_8

表2给出了一部分的RFID攻击以及它在自动机中的最终状态，将它们进行归并后得到有限自动机，下一节将对该有限自动机分析归类并且讨论它的延展性和攻击预测能力。

图5表示归并以后的RFID入侵检测有限自动机。该有限自动机是由表2的各种攻击经过3.3节的有限自动机构造然后经过3.4节的适用于RFID系统入侵检测的有限自动机归并算法归并得出。其中 $M'=(K',\Sigma,\delta,q_0,F')$，$K'=\{s_0,s_1,s_2,s_3,s_4,s_5,s_6,s_7,s_8\}$，$\Sigma=\{r_0,r_1,r_2,r_3,r_4,r_5,r_6,r_7\}$，$F'=\{s_2,s_4,s_6,s_7,s_8\}$，$s_0$ 表示初始状态，标签未上电；s_1 是标签接到query类的命令，可能处于Reply或者arbitrate的状态；s_2 是标签接收到ACK类型的命令，可能处于Acknowledge状态；s_3 和 s_5 表示标签接收到Req_RN命令，可能处于open或者secured状态；s_4 表示接收到Access命令进行密码验证；s_6 表示攻击者采用LOCK命令尝试锁标签，标签可能处于secured状态；s_7 表示通过锁或者直写在标签中加入特定的信息；s_8 为读写标签，标签可能在Open或者secured状态。

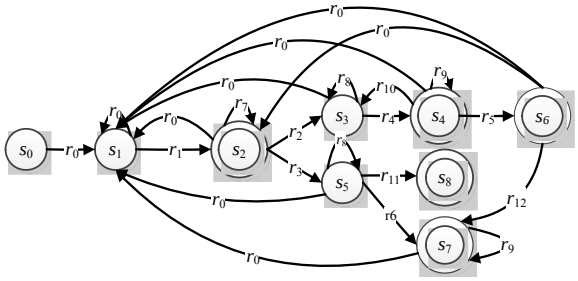

图5　一部分攻击归并后的有限自动机

4.2　RFID攻击分类

4.2.1　RFID攻击分类的原则

通过对RFID入侵检测有限自动机的归并，根据攻击对于RFID系统的危害程度不同及攻击围绕的攻击节点不同两个原则进行分类。

1) 从有限自动机的执行深度情况来判断。2) 这是分类的主要依据，观察有限自动机，不同种类的攻击围绕着不同的核心围绕节点，它的同类型的攻击跟它的核心围绕节点是相同的。

4.2.2　对于上述归并后的自动机的攻击分类

由图5所示的自动机使用4.2.1中攻击分类的原则对攻击进行分类。

1) 以获取标签的PC/EPC为主的攻击，它们围绕着节点s_2来实施，对应表2中的标号1、2。此类攻击容易实现，对RFID系统危害程度相对较小。

2) 针对没有LOCK的RFID系统，对应表2中标号5、7，此类攻击是在第一类攻击的基础上尝试着读写标签，常常围绕着节点s_5和s_7来实施，相对于第一种具有较强的破坏性，要应对此类攻击，需要对标签的敏感信息存储地方进行LOCK。

3) 围绕着标签的ACCESS密码来进行的，对应表2中标号3、4、6，这类攻击对于RFID系统具有非常强的破坏性，其核心是围绕着s_4和s_6节点来进行的，在尝试LOCK权限以后可能会采取一些读写措施来验证ACCESS密码的正确性。

4.3　模型的延展性

对于新出现的攻击类型，可以通过上述同样的方法建立其有限自动机模型，然后采取3.5节的算法将新的有限自动机尝试与系统中的几个自动机进行合并，给新产生的攻击进行分类。

由于RFID攻击多种多样，很难把现有的攻击全部涵盖完，而且随着RFID安全技术研究的深入，还将出现更多新的RFID攻击，直观地进行攻击特征识别是一项工程浩大的工作。但是本文提出的基于有限自动机的入侵检测系统，可以通过了解入侵的实质来对异常行为集进行检测。这样不但可以在攻击样本较少时建立入侵检测模型，而且还可通过模型检测具有相似特征的未知攻击。针对RFID系统中的异常行为，本文的有限自动机模型检测方法具有良好的适用性。

5　仿真实验分析

本文使用基于UDP协议的局域网通信完全仿真ISO18000-6C协议，采用3轮实验，每轮2 000次访问事件，每一次检测前对访问事件顺序乱序。攻击事件约占总体事件比重的40%，其中，DOS攻击(D)约占41%，围绕读写操作(RW)约占21%，监听攻击(L)约占14%，尝试暴力破解密码(P)约占5%，尝试改变标签内容(C)约占19%。检测结果如表3所示(攻击类型用上面的简写代替)。

表3　检测测试结果

(序号)漏/误检率/%	总体	D	RW	L	P	C
(1)漏检	21.1	7.44	2.79	100	6.25	11.3
(1)误检	5.38	8.19	1.19	0	6.25	5.68
(2)漏检	20.0	5.95	1.78	100	0	8.52
(2)误检	5.50	9.56	3.57	0	0	4.54
(3)漏检	22.2	9.56	2.38	100	6.25	10.8
(3)误检	4.63	7.44	0	0	0	6.81

从表3可以看出，该系统对于只监听的攻击无能为力，但对于其他的攻击检测效果较好。其中对于DOS攻击的检测存在一定的漏检率并且根据访问事件的不同顺序存在一定的波动，这是因为不同的组合顺序可能漏检的数量不同。对于尝试改变标签能容的攻击存在一定的漏报率，对于其他的攻击，它能起到较好的检测效果。

对于总体攻击的检测，漏检率趋于21%，误检率趋于5%。可见样本集一定时，虽然漏检率和误检率出现小幅度的波动，但大体上趋于稳定。

6 结 论

本文在RFID中间件层设计实施了RFID入侵检测系统的实现过程，说明了RFID入侵检测系统的模型构造方法和适用类型。定义了异常行为并采用<Command,Status,Timestamp>三元组对RFID系统行为进行样本分析。通过对标签可能的状态进行判别，建立了RFID入侵检测有限自动机，然后采取适用于RFID入侵检测有限自动机的归并算法建立攻击检测模型。通过对RFID攻击的建模和归并分析，对RFID环境下的攻击行为进行了分类。本文的方法具有良好的可行性和适应性，能够对未知的RFID攻击建立一定的检测能力。

由于RFID环境受到较多的物理环境限制，对RFID攻防技术的研究目前还处于起步阶段，本文主要基于信息安全理论提供了一个基于有限状态机模型的攻击建模与异常检测系统建立方法。对于该领域的研究还有待进一步深入开展。

参 考 文 献

[1] VAN DEURSEN T, RADOMIROVIĆ S. Algebraic attacks on RFID protocols[C]//Proceedings of the Third IFIP WG 11.2 International Work Shop on Information Security Theory and Practice. Smart Devices: Pervasive Systems, and Ubiquitous Networks. Berlin: Springer, 2009: 38-51.

[2] MITROKOTSA A, RIEBACK M R, TANENBAUM A S. Classifying RFID attacks and defenses[J]. Information Systems Frontiers, 2010, 12(5): 491-505.

[3] FU Y, ZHANG C, WANG J. A research on denial of service attack in passive RFID system[C]//Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference on. [S.l.]: IEEE, 2010: 24-28.

[4] VAN DEURSEN T, RADOMIROVIC S. Attacks on RFID protocols[EB/OL]. (2008-07-12). http://eprint.iacr.org/ 2008/ 310.

[5] JUELS A. RFID security and privacy: a research survey[J]. Selected Areas in Communications, IEEE Journal on, 2006, 24(2): 381-394.

[6] VASILIADIS G, ANTONATOS S, POLYCHRONAKIS M, et al. Gnort: High performance network intrusion detection using graphics processors[C]//Recent Advances in Intrusion Detection. Berlin: Springer, 2008.

[7] 单征, 刘铁铭, 楚蓓蓓. 基于网络状态的入侵检测模型[J]. 信息工程大学学报, 2002, 3(3): 9-14.
DAN Zheng, LIU Tie-ming, CHU Bei-bei. Intrusion detection model based on network state[J]. Journal of Information Engineering University, 2002, 3(3): 9-14.

[8] 张烨. RFID 中间件安全解决方案研究与开发[D]. 上海: 上海交通大学, 2007.
ZHANG Ye. Research and development for RFID middleware security solution[D]. Shanghai: Shanghai Jiaotong University, 2007.

[9] THAMILARASU G, SRIDHAR R. Intrusion detection in RFID systems[C]//Military Communications Conference. [S.l.]: IEEE, 2008.

[10] 廖宇俊. 基于上下文感知计算的RFID中间件安全决策技术研究[D]. 上海: 上海交通大学, 2009.
LIAO Yu-jun. Research on security decision-making technology of RFID middleware based on context-aware computing[D]. Shanghai: Shanghai Jiaotong University, 2009.

[11] 郭建华, 杨海东, 邓飞其. 基于免疫和多Agent的RFID入侵检测模型研究[J]. 计算机工程与应用, 2009, 45(35): 94-98.
GUO jian-hua, YANG Hai-dong, DENG Fei-qi. Study on intrusion detection model for RFID system based on immune and multi-Agent[J]. Computer Engineering and Applications, 2009, 45(35): 94-98.

[12] MIROWSKI L, HARTNETT J. Deckard: a system to detect change of RFID tag ownership[J]. International Journal of Computer Science and Network Security, 2007, 7(7): 89-98.

[13] YANG H, LI C, HU J. RFID Intrusion detection with possibilistic fuzzy c-means clustering[J]. Journal of Computational Information Systems, 2010, 6(8): 2623-2632.

[14] 卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述[J]. 通信学报, 2004, 25(7): 19-29.
QING Si-han, JIANG jian-chun, MA Heng-tai, et al. Research on intrusion detection techniques: a survey[J]. Journal of China institute of communication, 2004, 25(7): 19-29.

编 辑 蒋 晓