文章编号:1009-3087(2016)01-0132-07 DOI:10.15961/j.jsuese.2016.01.020

物联网环境下的敏感信息保护方法

沙乐天[1],何利文[1],傅建明[2],王延松[3],胡学理[3],牛小兵[3],李鹏伟[2],陈 晶[2]
(1.南京邮电大学 计算机学院,江苏 南京 210003;2.武汉大学 空天信息安全与可信计算教育部重点实验室,湖北 武汉 430072;
3.中兴通讯股份有限公司,江苏 南京 210012)

摘 要:针对物联网融合网络环境中多种敏感信息的保护问题,定义敏感信息全局生命期的若干特征属性,设计相关规则标记敏感信息动态安全级别,度量特征属性与实时泄露场景的关联性,进而采用基于身份的加密方法(IBE)对敏感信息部署加密方案,最后在中间层及应用层部署补丁分发机制预防感知层的防护失效,从而实现敏感信息在全局生命期中面向泄露场景的安全防护模型。实验针对3种异构网络环境下敏感信息的泄露场景进行测试,加密算法安全性较高且系统开销较低。

关键词:物联网;敏感信息;特征属性;IBE;补丁分发
中图分类号:TP31 **文献标志码**:A

A Protection Method for SI in IOT Environment

SHA Letian[1], *HE Liwen*[1], *FU Jianming*[2], *WANG Yansong*[3], *HU Xueli*[3], *NIU Xiaobing*[3], *LI Pengwei*[2], *CHEN Jing*[2],
(1. College of Sci. & Technol., Nanjing Univ. of Posts and Telecommunications, Nanjing 210003, China;
2. State Key Lab. of Aerospace Info. Security and Trusted Computing, Ministry of Education, Wuhan Univ., Wuhan 430072, China;
3. ZTE Co., Nanjin 210012, China)

Abstract: In order to protect multi-type sensitive information (SI) in internet of thing, some characteristic attributes were defined in global data life time, relative rules were designed to mark dynamic security level, and the relationship between attributes and leakage-points was measured. Moreover identity based encryption (IBE) was applied in middle layer, finally patch distribution was performed to prevent expiration in above layers. Experiments were accomplished for SI in three heterogeneous networks and the result showed that the security of encryption algorithm can be ensured with low overhead.

Key words: IOT; sensitive information; characteristic attribute; IBE; patch distribution

随着物联网应用范围的扩展及相关技术的提高,其带来的安全威胁也愈演愈烈,其中最大的威胁来自于信息泄露及数据篡改。具体来看:1)WSN环境下攻击者可伪造信息采集节点来窃取或篡改敏感信息。2)RFID环境下数据加密及防护的算法较脆弱,攻击者可通过离线方式读取标签中的敏感信息。3)环境资源受限。无论是传感器网络还是RFID网络环境,隐私保护或数据防护不能直接应用在此类环境中。4)用户隐私或敏感信息在物联网体系结构上层的数据传递过程中容易受到流量监听、嗅探等网络流攻击,导致敏感信息在传递过程中被窃取或篡改。

从物联网技术发展的全局角度及物联网系统结构的框架设计出发,当前的研究工作具体从以下角度展开:文献[1]中综述了全球物联网发展的现状,强调物联网安全机制的加强需要着重考虑认证与访问控制机制及数据加密方法。文献[2]针对传感网的故障检测及定位总结并比较了现有的系统状态获取技术,探讨故障修复及网络调试的关键技术。文献[3-4]分别针对3G接入及RFID接入网络提出

收稿日期:2014-12-25
基金项目:南京邮电大学引进人才科研启动基金资助项目(NY212012);国家自然科学基金资助项目(61202387;90718005;61272451;61373168);高等学校博士学科点专项科研基金资助项目(20120141110002);国家重大科技专项项目资助(2010ZX03006-001-01)
作者简介:沙乐天(1985—),男,讲师. 研究方向:物联网. E-mail:ltsha@whu.edu.cn

安全架构模型及信任传递机制,旨在建立多网融合环境下主体网络结构的安全防护。

而针对物联网中间层,文献[5]论述了传感网中间件的研究现状,提出在 WSN 网络环境特征下的中间件设计要求及规范;文献[6]对传感模块的接口进行标准化描述,设计可重用的数据采集中间件;同样针对中间件的数据传输过程,文献[7-8]分别提出了一种可订制的信任管理框架及安全传输模型,并给出实验结果。

最后,落实到物联网环境的感知层,主要分为 WSN 环境及 RFID 环境下的数据保护方法及安全协议分析。WSN 环境下,文献[9-10]均针对面向用户的位置服务展开研究,前者提出一种抗连续查询的隐私保护方法,后者针对一种流向的保护方法(silent cascade)提出新的轨迹隐私度量策略。文献[11]则针对隐私信息在云环境下的保护及销毁实现相关系统并进行性能测试。另一方面,RFID 环境下,文献[12]借助于差分故障攻击方法评估 LED 轻量级加密算法的安全性,但未能对其进行相关改进。

针对这一情况,提出一种物联网环境下的敏感信息识别与防护方法。基于异构网络中间件这一核心处理模块,通过动态组件加载的方式在 WSN 网络、RFID 网络、GSM 网络融合环境中在物联网感知层对敏感信息进行识别,给出其特征属性定义,并依据外部攻击关联度量将特征属性聚合生成动态敏感级别,进而以此为敏感信息身份特征采用基于身份的加密算法(IBE)部署访问权限管控。最终设计并实现了相关系统结构,并通过实验验证该方法的有效性并测试了系统运行效率。

1　基于中间件技术的敏感信息识别及防护方法

本研究首先给出研究对象的相关定义以及敏感信息的若干种特征属性,而后给出设计方案在物联网环境下的应用场景,最后针对该系统结构的实现特征及实现原理进行详细描述。

1.1　敏感信息定义

本研究所保护的敏感信息主要是指个人或组织等实体机构在该环境中不愿公开的信息,定义为 sensitive information,简记为 SI。而后根据实际系统环境及人工分析确定该定义下若干种重要的特征属性:

1)网络环境(network environment),简记为 SI. ne。本研究的物联网环境主要由以下 3 种异构网络组成:传感器网络、RFID 网络、GSM 网络,分别简记为 WSN、RFID、GSM。

2)数据生命期(data lifetime),简记为 SI. dl。结合敏感信息在物联网环境下的独有特征,按照物联网的体系结构定义敏感信息的数据生命期,包括:感知层生命期(sensor-layer lifetime),简记为 sll;中间层生命期(middleware-layer lifetime),简记为 mll;应用层生命期(application-layer lifetime),简记为 all;用户层生命期(user-layer lifetime),简记为 ull。

3)数据操作语义(data operation semantics),简记为 SI. dos。主要描述当前针对敏感信息的操作属性,具体包括几种:读操作,记为 read;写操作,记为 write;拷贝操作,是指将当前保存地址上的信息拷贝到其他地址上,记为 copy;加密操作,记为 encrypt;擦除操作,是指将当前敏感信息地址上的信息进行销毁或归零处理,记为 clear。

4)数据操作主体(data operation host),简记为 SI. doh。主要描述完成数据操作语义时执行主体的属性,描述的方式主要通过度量执行代码主体所处的内存空间布局,主要分成:内部主体(internal host),简记为 ih;外部主体(external host),简记为 eh。

5)数据格式(data format),简记为 SI. df。主要描述敏感信息的实时数据格式,具体可分为 2 种:明文格式(plain-text),简记为 pt;密文格式(cipher-text),简记为 ct。

6)数据传播方式(data spreading),简记为 SI. ds。主要描述敏感信息在当前操作语义下的数据传播方式,具体分为:不传播(non spreading),表示当前操作语义下敏感信息并未导出到其他数据地址上,记为 ns;常规传播(regular spreading),表示当前操作语义下敏感信息按照规定的数据传播方式导出到合法的地址,记为 rs;越界传播(cross spreading),表示当前操作语义下敏感信息被导出到外部未知的地址范围中,记为 cs。

7)敏感级别(sensitive level),简记为 SI. SL。该定义是根据以上若干种属性采用度量规则判决生成,具体度量规则过程见 1.3 节。

8)敏感级别阈值(sensitive threshold),简记为 SI. ST。该定义表示敏感信息泄露场景发生时的动态敏感级别,可用于度量敏感级别动态变化与敏感信息泄露之间的关联性,具体生成规则方法见 1.3 节。

1.2 系统结构(internet of things-sensitive information recognition and protection, IoT-SIRP)

首先给出传统物联网环境下的层次结构,如图1左半边结构所示,包括感知层、中间层及应用层。IoT-SIRP是在常规体系结构中引入的一种敏感信息识别与保护机制,如图1右半部分所示,从感知层开始对各种网络接入端的敏感信息进行获取并标记,监控敏感信息在物联网层次结构中的全局生命期。该系统主要包括3个核心组件:泄露感知组件、攻击防御组件、补丁分发组件。具体运行机制及原理见1.3~1.5节。

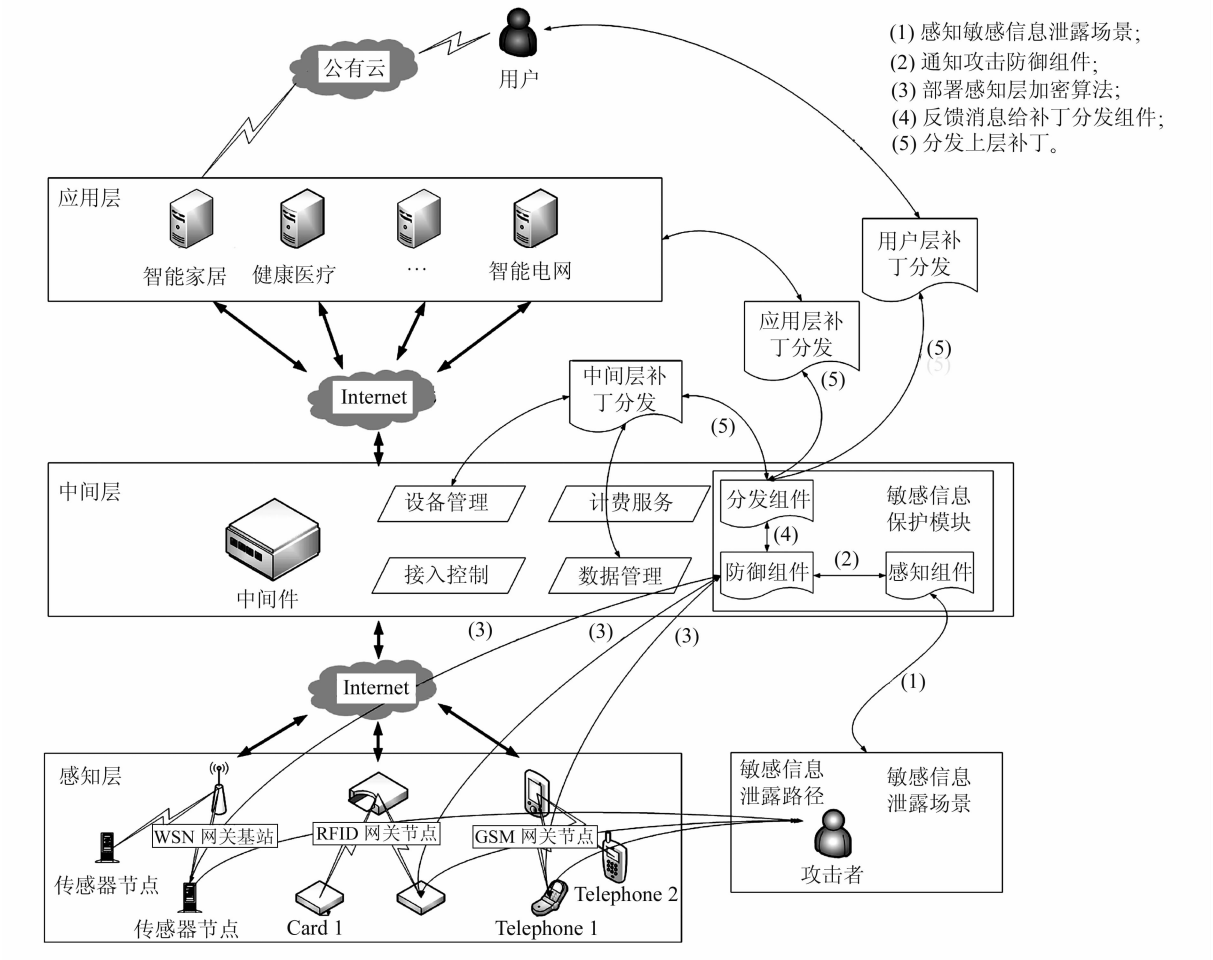

图1 IoT-SIRP:物联网环境下的敏感信息识别与防护

Fig. 1 Recognition and protection of sensitive information in IoT

1.3 泄露感知组件(leak-sensor component, LSCom)

在感知层需要针对不同的网络环境终端对敏感信息的获取进行动态识别,该组件的原理从3方面阐述:敏感信息定位、敏感属性填充、敏感级别标记。

1)敏感信息定位

第一,GSM网络环境。对于GSM终端,具体通过解析Android操作系统下的Contentprovider组件来实现,获取函数定义为MyGSMSILocation()。第二,WSN网络环境。对于WSN网络环境终端,敏感对象主要包括传感器节点(sensor)中的位置信息。具体解析过程是基于TinyOS环境的Xmash传感网数据协议中的数据格式,获取函数为MyWSNSILocation()。第三,RFID网络环境。对于RFID网络环境终端,敏感对象主要包括RFID标签中的个人敏感信息,具体针对RFID卡中的一种高频标签卡Mifare Classic进行数据格式解析。目前已出现针对此类标签的恶意攻击方法,因而设定该标签作为RFID网络环境的主要研究对象,具体解析函数为MyRFIDSILocation()。

2)敏感级别标记

针对已定位的敏感信息,需要建立敏感级别与泄露路径的关联度量。根据1.1节中的敏感信息相关定义,结合实际运行环境下攻击场景的系统特征,

建立关联度量规则如下:

规则 1 (Rule 1):

when SI. ne = WSN/RFID/GSM, SI. dl = sll;

if SI. dos = read&&SI. doh = eh&&SI. df = pt&&SI. ds = ns,
SI. SL = SI. st1 (1)

if SI. dos = write&&SI. doh = eh&&SI. df = pt&&SI. ds = ns,
SI. SL = SI. st2 (2)

if SI. dos = copy&&SI. doh = eh&&SI. df = pt&&SI. ds = cs,
SI. SL = st3 (3)

式(1)~(3)给出了 3 种敏感信息泄露场景的度量规则。在 3 种网络环境下,针对感知层运行环境,有:1)若存在外部数据操作主体读当前敏感信息的明文数据,则定义为敏感级别阈值为 SI. st1;2)若存在外部数据操作主体写当前敏感信息的明文数据,则定义为敏感级别阈值为 SI. st2;3)若存在外部数据操作主体复制当前敏感信息的明文数据到外部未知的地址范围,则定义为敏感级别阈值为 SI. st3。

1.4 攻击防御组件(attack-defense component, ADCom)

本系统结构将此组件的加密算法设计为基于身份属性的加密算法(identity-based encryption)。核心算法设计主要借鉴 Boneh-Boyen scheme[13],实现函数为 SIBEncrypt(),具体规则设计如下,共包括规则 2 中的 6 个主要部分:

规则 2 (Rule 2):

1)假设 G 和 G_T 为 2 个素数序列 p 的乘法循环群,g 为群 G 的生成元,e 为一个双线性映射,有 $e: G \times G \rightarrow G_T$,则双线性映射有如下属性:

① 双线性:对所有 $u,v \in G$ 和所有 $a,b \in \mathbb{Z}_p$(a,b 均为整数,$\mathbb{Z}_p$ 表示模 p 的整数集),有:

$$e(u^a,v^b) = e(u,v)^{ab} \tag{4}$$

②非退化性:$e(g,g) \neq 1$

2)G 为双线性群且 G 中的操作以及双线性映射 e 是有效的,且 e 为对称的,所以:

$$e(g^a,g^b) = e(g,g)^{ab} = e(g^b,g^a) \tag{5}$$

3)给出公钥共包括:群 G 中的 3 个随机元素以及群 G_T 中的一个元素:

$$PK = \{g,u,h \in G, e(g,g)^{\alpha}\} \tag{6}$$

其中,α 为 $\mathbb{Z}_p$ 中的随机元素,主密钥为 g^{α}。

4)假设已将动态敏感级别 SI. SL′ 映射为 $\mathbb{Z}_p$ 中的元素,则目标 SI 相对于身份信息 SI. SL′ 的私钥给出如下:

$$SK_{\mathrm{SI.SL'}} = \{g^{\alpha}(u^{\mathrm{SI.SL'}}h)^{\gamma}, g^{\gamma}\} \tag{7}$$

其中,γ 也是 $\mathbb{Z}_p$ 中的随机元素。

5)假设需加密的目标敏感信息 SI 已映射为 G_T 中的元素,则使用身份信息 SI. SL′ 对 SI 加密后的密文为:

$$CT = \{SI \cdot e(g,g)^{\alpha s}, g^s, (u^{\mathrm{SI.SL'}}h)^s\} \tag{8}$$

其中,s 为 $\mathbb{Z}_p$ 中的随机元素,用于加密。

6)解密过程则是已知从 g^s 和 $(u^{\mathrm{SI.SL'}}h)^s$ 推导出 $e(g,g)^{\alpha s}$:

$$e(g^{\alpha}(u^{\mathrm{SI.SL'}}h)^{\gamma}, g^s)/e(g^{\gamma},(u^{\mathrm{SI.SL'}}h)^s) = e(g,g)^{\alpha s} \tag{9}$$

1.5 补丁分发组件(patch-distribution component, PDCom)

攻击防御组件将部署结果消息和目标敏感信息的动态敏感级别同时传递给补丁分发组件。该组件首先在以下时间点对运行流程进行挂钩:第一,中间层利用原始敏感信息对数据和设备管理鉴权时;第二,应用层利用原始敏感信息对用户进行授权及提供服务时。具体如规则 3 的伪代码所示:

规则 3 (Rule 3):

```
if (LayoutOfADCom()&&eventOfst(SI)==0)
    //攻击防御组件的部署失效或敏感信息动态敏感级别达到阈值
{
when SI. dl = mll, HookAuthForSI(mll), ReInputPS(ull);
    //对中间层的敏感信息鉴权进行拦截,在用户层要求重新输入敏感信息口令
when SI. dl = all, HookSerForSI(all), ReInputPS(ull);
    //对应用层的敏感信息服务进行拦截,在用户层要求重新输入敏感信息口令
  ReGenSI(SI, SI. SL);
    //通过自身的攻击防御组件进行数据加密并分配密钥
  ReplaceSI(mll);
    //在中间层用新生成并加密后的敏感信息对原始敏感信息进行替换
  ReplaceSI(all);
    //在应用层用新生成并加密后的敏感信息对原始敏感信息进行替换
}
```

2 实　验

为证实 IoT-SIRP 的有效性,给出实验结果及相关分析。WSN 环境选用 Crossbow Technology 公司的

设备搭建,包括4个基站节点(MIB520CB),每个基站节点下控制4~5个信息采集节点(MDA300CB);RFID环境选用Mifare Classic 1k标签及AR6181-MX兼容读卡设备,并使用Proxmark3作为仿真攻击设备。GSM网络环境采用Galaxy S3手机作为基站节点和终端节点。具体测试结果如表1所示。

表1 LSCom安全性

Tab.1 Security of LSCom

泄露场景	仿真方法	泄露感知结果
WSN	硬件:mda300cb 软件:TinyOS 2.0	可感知; SI.SL=st1
RFID	硬件:Proxmark3 软件:C language	可感知; SI.SL=st2
GSM	硬件:Galaxy S3 软件:Android 4.1	可感知; SI.SL=st3

实验内容包括:第一,在敏感信息泄露场景下测试LSCom运行功效;第二,对比类似加密算法测试攻击ADCom安全性及复杂度;第三,ADCom部署失败时测试PDCom运行功效;第四,测试IoT-SIRP加载前后系统全局运行功效;最后,对比其他隐私保护方法与IoT-SIRP的差异及各自优缺点。

3种网络环境下敏感信息泄露场景的仿真环境设计如下:WSN网络中通过TinyOS 2.0环境的编程开发模拟传感器板对目标mda300cb传感器板的节点数据操作进行转发节点写入操作。系统对该敏感信息泄露场景检测结果显示SI.SL=st1,即SI.dos=read&&SI.doh=eh&&SI.df=pt&&SI.ds=ns,存在外部对象以读目标敏感信息的明文且数据没有越界传播;RFID网络中通过Proxmark3设备进行C语言开发仿真了windows环境下写UID(卡标示)及关键数据区的操作,系统对该泄露场景检测结果为SI.SL=st2,即SI.dos=write&& SI.doh=eh&&SI.df=pt&&SI.ds=ns,存在外部对象对目标敏感信息进行写操作且数据没有越界传播;GSM网络中在Android 4.1环境下进行程序开发仿真一种复制电话簿信息的操作,检测结果显示SI.SL=st3,即SI.dos=copy&& SI.doh=eh&&SI.df=pt &&SI.ds=cs,存在外部对象拷贝目标敏感信息,且敏感信息越界传播。

另外,给出敏感信息保护模块加载前后系统全局运行功效测试结果,如表2所示。其中,并发用户数采用LoadRunner工具进行模拟,敏感信息保护模块加载前后系统的对事件的响应时间略有上升,平均处理事件能力几乎不受影响,事件处理成功率相同,用户平均流量数稍有下降。总体而言,敏感信息保护模块的加载对系统运行功效几乎没有影响,兼容性好且系统开销低。最后,给出本系统结构和其他类似隐私保护方案的全局对比结果,选取文献[11-12,14]中的4种系统结构与IoT-SIRP进行比较,如表3所示,主要从以下几个方面展开对比工作:

表2 IoT-SIRP运行时间开销

Tab.2 Time-consumption in IoT-SIRP

用户数	响应时间/s		平均每秒处理流量/(Byte·s^{-1})		成功率/%		平均流量/(Byte·s^{-1})	
	加载前	加载后	加载前	加载后	加载前	加载后	加载前	加载后
10	0.064	0.071	112.974	108.753	100	100	38 979.5	39 675.9
25	0.174	0.196	113.531	106.391	100	100	38 989.9	39 282.6
50	0.368	0.404	109.937	104.266	100	100	37 863.6	37 045.2
100	0.694	0.759	104.925	99.683	100	100	36 046.3	35 743.2

表3 IoT-SIRP与其他隐私保护方法对比

Tab.3 Comparison between IoT-SIRP and other privacy protections

隐私保护方案	隐私对象识别	隐私对象防护	隐私对象灾备
文献[11]	依靠握手协议对隐私对象进行识别	基于AES算法对隐私对象进行对称加密	无
文献[12]	随机选择	基于LED算法对隐私对象进行分组加密	无
文献[14]	随机选择	基于IBE算法对隐私对象进行属性加密	无
IoT-SIRP	基于API封装及泄露路径语义描述对隐私对象定位及标记	基于IBE算法对隐私对象敏感级别属性进行动态感知加密	基于敏感级别判决及可靠重入对隐私对象泄露场景进行灾备处理

1)隐私对象识别方法。在隐私对象识别方面,文献[11]主要通过分析网络流向来获取隐私对象,分别通过WSN网络中的网络拓扑结构及云环境下的网络通信协议判决隐私对象。而文献[12]和

[14]中均忽略了隐私对象识别过程,基本可视为随机选择保护对象。IoT-SIRP 基于标准 API 封装及泄露路径语义描述对隐私对象定位及标记,以确保识别过程的保密性及属性标记的准确性。

2)隐私对象保护方法。作为系统结构中的核心过程,本研究及对比文献中所采用的加解密算法各有不同,主要取决于各原型系统所对抗的攻击方法及设计目的的差异性。文献[11]为基于 AES 算法对隐私对象进行对称加密,在虚拟化的云环境下设计密钥分配及管理模块;文献[12]为基于 LED 算法用于对抗差分故障攻击的分组加密方法;文献[14]与 IoT-SIRP 所使用的都是基于 IBE 算法的加解密方案,但本研究的加密算法将隐私信息的公开身份标志设计为动态敏感级别属性,实现了隐私标志与泄露场景的关联度量,因而该组件只有在感知到泄露场景的情况下才动态加载,在很大程度了节约了系统开销及节点能耗。

3)隐私对象泄露场景下灾备及鉴证方法。对比各文献中的算法,只有本研究提出的加密方案部署失败后的泄露场景灾备方法,基于敏感级别判决及可靠重入机制,PDCom 部署中间层及应用层的补丁分发及协作方案,有效地防止泄露场景的扩散。

3　结　论

基于传统的物联网架构实现了一种针对敏感信息的防护方法,通过部署敏感信息保护模块 IoT-SIRP,识别感知层的敏感信息流向并进行属性标记,建立属性的动态变化与信息泄露的关联规则来感知敏感信息泄露场景,采用基于身份的加密方法(IBE)对敏感信息进行实时数据加密以抵抗外部攻击。并通过消息反馈的方式通知系统中间层及应用层,以便在加密方案失败时部署上层补丁管控敏感信息流向,防止敏感信息泄露场景的扩散。最终通过实验验证该设计方案的有效性并测试系统性能开销。

后继工作中希望能将防护对象进一步扩大化并实现自适应信息防护,即在未知保护对象的前提下自动化的获取对象属性并建立安全规则。

参考文献:

[1]Ning Huansheng, Xu Qunyu. Research on global Internet of things' developments and it's lonstruction in China[J]. Acta Electronica Sinica, 2010, 38(11): 2590 – 2599. [宁焕生,徐群玉. 全球物联网发展及中国物联网建设若干思考[J]. 电子学报,2010,38(11):2590 – 2599.]

[2]Ma Junyan, Zhou Xingshe, Zhang Yu, et al. Debugging sensor networks: A survey[J]. Chinese Journal of Computers, 2012, 35(3): 406 – 422. [马峻岩,周兴社,张羽,等. 传感器网络调试研究综述[J]. 计算机学报,2012,35(3):406 – 422.]

[3]Liu Wenmao, Yin Lihua, Fang Binxing, et al. A hierarchical trust model for the internet of things[J]. Chinese Journal of Computers, 2012, 35(5): 847 – 855. [刘文懋,殷丽华,方滨兴,等. 物联网环境下的信任机制研究[J]. 计算机学报,2012,35(5):847 – 855.

[4]Sun Yuyan, Liu Zhuohua, Li Qiang. A security framework for internet of things based on 3G access[J]. Journal of Computer Research and Development, 2010, 47(Suppl): 327 – 332. [孙玉砚,刘卓华,李强. 一种面向 3G 接入的物联网安全架构[J]. 计算机研究与发展,2010,47(增刊):327 – 332.]

[5]Li Renfa, Wei Yehua, Fu Bin, et al. A review for middleware in wireless sensor networks[J]. Journal of Computer Research and Development, 2008, 45(3): 383 – 391. [李仁发,魏叶华,付彬,等. 无线传感器网络中间件研究进展[J]. 计算机研究与发展,2008,45(3):383 – 391.]

[6]Chen Pengpeng, Guo Zhongwen. Standardization of sensing module interfaces and design of reuseable data collection middleware[J]. Journal of Computer Research and Development, 2010, 47(Suppl): 288 – 292. [陈朋朋,郭忠文. 传感设备模块接口标准化及可重用数据采集中间件设计[J]. 计算机研究与发展,2010,47(Suppl):288 – 292.]

[7]Zhou Minghui, Mei Hong, Jiao Wenpin. A custermizable trust management framework based on middleware[J]. Acta Eleronica Sinica, 2005, 33(5): 821 – 826. [周明辉,梅宏,焦文品. 基于中间件的可定制信任管理框架[J]. 电子学报,2005,33(5):821 – 826.]

[8]Wu Zhenqiang, Zhou Yanwei, Ma Jianwei, et al. A security tranmission model for internet of things[J]. Chinese Journal of Computers, 2011, 34(8): 1352 – 1364. [吴振强,周彦伟,马建峰. 物联网安全传输模型[J]. 计算机学报,2011,34(8):1352 – 1364.]

[9]Pan Xiao, Hao Xing, Meng Xiaofeng. Privacy preserving towards continuous query in location-based services [J]. Journal of Computer Research and Development, 2010, 47(1): 121 – 129. [潘晓, 郝兴, 孟小峰. 基于位置服务中的连续查询隐私保护研究[J]. 计算机研究与发展, 2010, 47(1): 121 – 129.]

[10]Wang Caimei, Guo Yajun, Guo Yanhua. Privacy metric for user's trajectory in location-based services[J]. Journal of Software, 2012, 23(2): 352 – 360. [王彩梅, 郭亚军, 郭艳华. 位置服务中用户轨迹的隐私度量[J]. 软件学报, 2012, 23(2): 352 – 360.]

[11]Zhang Fengzhe, Chen Jin, Chen Haibo, et al. Lifetime privacy and self destruction of data in the cloud[J]. Journal of Computer Research and Development, 2011, 48(7): 1155 – 1167. [张逢喆, 陈进, 陈海波, 等. 云计算中的数据隐私性保护与自我销毁[J]. 计算机研究与发展, 2011, 48(7): 1155 – 1167.]

[12]Li Wei, Gu Dawu, Zhao Chen. Security analysis of the LED lightweight cipher in the internet of things[J]. Chinese Journal of Computers, 2012, 35(3): 435 – 445. [李玮, 谷大武, 赵辰. 物联网环境下 LED 轻量级密码算法的安全性分析[J]. 计算机学报, 2012, 35(3): 435 – 445.]

[13]Waters B. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions[C]//Proceedings of the CRYPTO 2009. Santa Barbara: Springer, 2009: 619 – 636.

[14]Tang Jiahui, Zhu Yanqin, Luo Xizhao. Identity-based encryption scheme against adaptive leakage[J]. Journal on Communications, 2012, 33(7): 90 – 95. [汤佳慧, 朱艳琴, 罗喜召. 抗自适应泄露的基于身份加密方案[J]. 通信学报, 2012, 33(7): 90 – 95.]

(编辑 杨 蓓)