Table 3 Statistic analysis for basic definition values

表 3 基本定义取值统计分析

基本定义	取值	数量(比例)	说明
BP.nl	dl ml	85(62.0%) 52(38.0%)	设备层中目标后门较多,主要由于设备层后门利用较中间层后门利用简单,且不易被检测
BP.aa	nr-nw r-nw r-w	21(15.3%) 103(75.2%) 13(9.5%)	地址属性大都为可读不可写状态,即可利用后门,但不可植入后门.最少情况为可读可写状态,即软件或固件为植入后门开放接口,为最差安全性
BP.ds	pt ct ot	64(46.7%) 27(19.7%) 46(33.6%)	数据格式半数为明文,即字符未加密,无需解密直接可利用.其次为混淆字符,部分内容置乱,需去混淆再利用.最少为加密字符,解密后可利用
BP.dc	iv niv	94(68.6%) 43(31.4%)	可见内容作为真实后门输入设备或软件中;不可见内容表示后门不能直接开启特殊权限,涉及多次、多点关联输入
BP.do	ad su at	61(44.5%) 54(39.4%) 22(16.1%)	数据主体主要为管理员,其通过检查输入源白名单可确定目标管理员通过后门实现远程控制;同理可检测目标远程用户利用后门实现控制.其他为后门泄露情况下的恶意攻击者,具体场景来自实验模拟过程
BP.df	rc prc	94(68.6%) 43(31.4%)	数据功能中 68%为开启远程控制权限,其他为开启部分远程控制权限,包括特殊端口开放、特殊函数开放等
BP.tm	at pt	79(57.7%) 58(42.3%)	触发方式中主动连接方式居多,易用性强.其他为被动连接方式,目标固件或软件接受特征数据包后可触发

4.3.3 上层语义取值分析

对上层语义包括逆向痕迹及流量检测两部分,首先收集在线及离线的场景信息,基于算法 1 与算法 2 生成两种语义的取值,并对比同一后门在不同出现点处、同一固件中不同后门、同一软件中不同后门的上层语义取值特征.具体如图 3 所示.

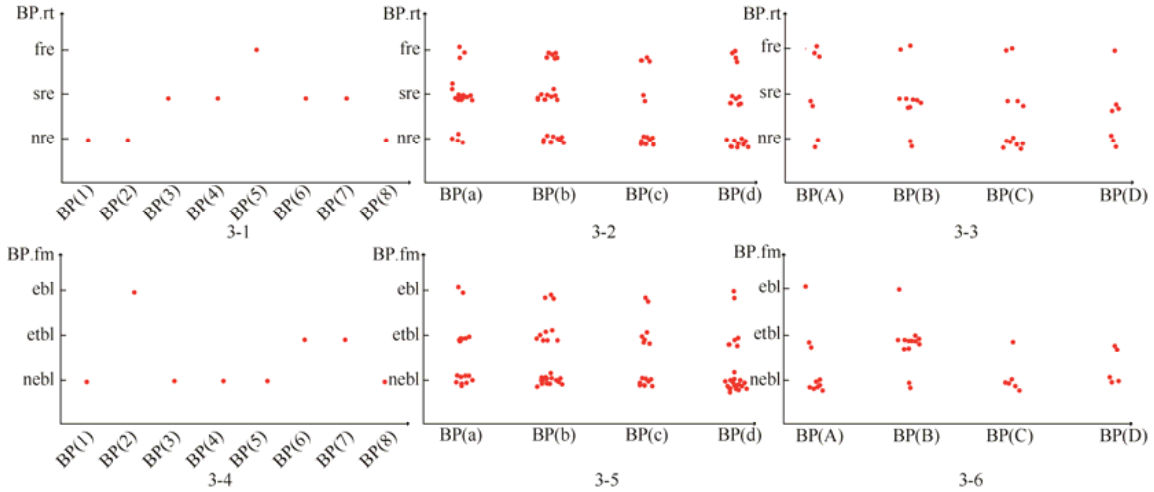

Fig.3 Statistic analysis for upper semantic values

图 3 上层语义取值统计分析

图 3 中选择同一后门隐私(IPC 系列摄像头中:IPC7185/IPC)进行逆向痕迹与流量检测的统计分析,如图 3-1 和图 3-4 所示;选择同一固件 NOE771PLC 中的 4 种不同后门:sysdxxg、kvxxxic、bbddRdkm9、bbddrdkm9(依次为 BP(a)、BP(b)、BP(c)、BP(d))作为分析对象对比分析逆向痕迹与流量检测取值分布,如图 3-2 与图 3-5 所示;选择同一软件 TP-Link TL 路由器中 4 种不同后门:axxxxxp、axxxxe、tl49xxxxk、root(依次为 BP(A)、BP(B)、BP(C)、BP(D))对比分析逆向痕迹与流量检测分布,如图 3-3 与图 3-6 所示.由图 3-1 可知,IPC 后门共 8 个出现点,只有第 5 个出现点处逆向痕迹为完全逆向破解,其他共 4 个点处为半逆向破解,其余为未逆向破解.可知在检测过程中半数以上加入的原始污点被破坏,而全部原始污点被破坏的情况下可认定目标固件已被攻击者逆向分析并去除安全保护的混淆过程.对比分析图 3-2 可知,在线流量检测结果中后门利用情况较少,只在第 2 个出现点处检测结果显示存在后门利用,在点 6、点 7 中显示存在后门探测利用,即不完全正确的后门利用过程,其

余为非后门利用过程.对比分析可知,对同一后门而言,离线逆向分析是在线利用攻击的基础,攻击者通常会在确保离线逆向破解成功的基础上谨慎部署在线后门利用,保证后门利用一次成功.对比同一固件中的不同后门,图 3-2 统计分析了 4 种后门在全局生命期中各个出现点处 *BP.rt* 的取值特征,由分布可知,取值显示完全逆向破解的情况总体偏少,而部分逆向破解的情况居多,未逆向破解的情况最多.统计中主要针对目标设备的常规运行状态完成数据采集,因此,表示常规运行状态下插入的原始污点未被修改或部分被修改,而完全被修改的情况较少,可认定被彻底破解.对比分析图 3-5 中数据可知,在线流量检测中可获得的后门攻击场景更少,绝对情况下可认定为后门利用的在线攻击在常规运行状态中基本没有,均来自实验构造的模拟过程.而中间层软件中的后门与设备层固件相比呈现更少的数据采集特征,由图 3-3 及图 3-6 的对比可知,在离线逆向痕迹及在线流量检测中的完全破解或在线攻击数明显减少,部分数据采集为 0.因此可证明软件内部的后门利用较固件来说频率较低,数据量不大,主要原因在于软件可实现较好的安全防护与较快的安全补丁,而固件层相关技术较匮乏.

4.3.4 判决语义取值分析

判决语义共包括 4 种:静态泄露度、动态泄露度、安全级与安全阈值.根据第 3.3 节中的判决语义生成规则可知,静态泄露度由网络层级、地址属性、数据格式、数据内容、数据功能以及逆向痕迹聚合生成,而动态泄露度由网络层级、数据内容、操作主体、数据功能、触发方式以及流量检测聚合而成,而安全级与安全阈值则基于静态与动态泄露度的反理想优基点聚合而成.如图 4 所示,统计分析目标后门集合中的各种后门隐私在各个出现点处静态泄露度与动态泄露度的取值,并通过安全级与安全阈值的比较实现后门泄露场景的感知.

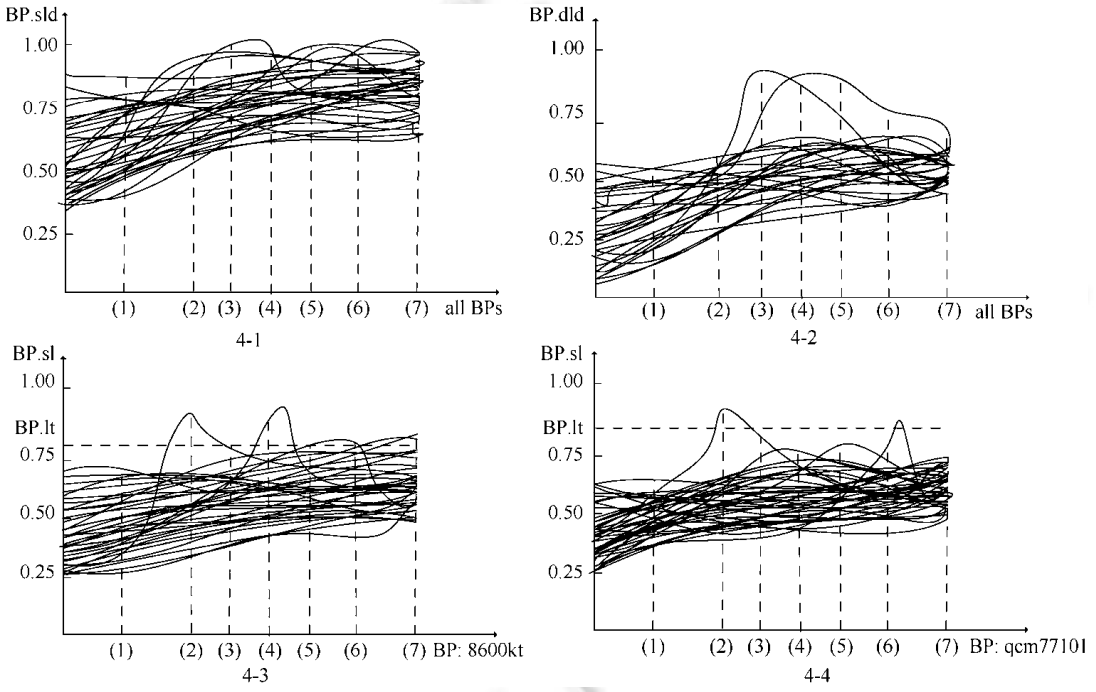

Fig.4 Analysis for judgement semantic

图 4 判决语义取值分析

图 4-1 及图 4-2 中选择目标后门隐私集合中全部 27 个元素进行静态泄露度及动态泄露度的取值统计分析,并对每种后门隐私选择 7 个出现点进行取值采样.静态泄露度的取值分布为[0.2743,0.9635],整体分布取值较大,主要集中在[0.5,0.85]的取值区间,尤其是在数据生命期末期,由于后门在静态文件结构回收或销毁操作的缺失导致静态泄露度增大,取值集中在[0.8,1]的区间.从取值变化上分析,取值曲线的斜率较大,会在某些出现点处呈现突然增大的情况,如 IPC7185 摄像头后门从第 2 出现点到第 3 出现点的过程中呈现静态泄露度取值从 0.7793~0.9446 的突变,而后又在第 4 出现点下降至 0.796 1,证明在出现点 3 处静态泄露情况严重,结合该位置处

的逆向痕迹检查结果可知,该后门在第 3 出现点处呈现被攻击者逆向破解的泄露场景.同理,分析 TP-Link 路由器后门 tl49xxxxk 可知,在出现点 5、点 6 的取值为 0.884 3 与 0.860 6,较之前与之后的各个出现点呈现出静态泄露度的陡增,结合逆向痕迹检测结果可以确定在出现点 5 与点 6 中被攻击者逆向破解.对比分析图 4-2 中的动态泄露度,取值分布为[0.1226,0.8420],整体分布取值较小,主要集中在[0.1,0.70]的取值区间,在全局生命期中的取值过程较平缓,斜率较小.从取值变化的角度来看,个别后门隐私的出现点会出现动态泄露度陡增,如 NOE771 PLC 固件后门 sysdxxg 与 siemens 电表组态软件 Powerconfig V2.x 后门 kvgxxxxxx27,分别在第 3、第 4 出现点呈现取值陡增,分别由 0.611 6 增大到 0.842 0,以及从 0.772 5 增大到 0.824 8.结合流量检测结果分析可知,这两种后门分别在这两个出现点被检测到有后门利用的恶意流量.

图 4-3 与图 4-4 选择 ION8600 智能电表固件中的后门 8600kt 及 Schneider IONsetup 电表软件中的后门 qcm77101 进行安全级与安全阈值的取值统计分析,随机选择 30 种系统运行状态,针对 7 个后门出现点进行取值采样.由图 4-3 可知,30 种系统运行状态中后门 8600kt 的安全级分布为[0.2606,0.8933],主要集中于[0.3,0.6]的取值区间,安全级在全局生命期中变化不大,且取值稳定,结合静态泄露度、动态泄露度及两种定义的反理想优基点取值分析可知,该后门相关的静态、动态泄露度的反理想优基点较大,导致关联系数取值较大,因此导致安全级取值较小,稳定在 0.5±0.2 左右.在第 7 运行状态与第 15 运行状态中,分别在第 2 与第 4 出现点呈现安全级突然增大,结合相关定义取值分析,第 7 运行态下的第 2 出现点处存在逆向痕迹,则静态泄露度出现突然增大的情况,在其他值取值基本保持不变的情况下导致安全级突然增大.而第 15 运行态下的第 4 出现点则存在动态泄露度增大的情况,该点处可判决为存在目标后门正相关的在线恶意流量,与之前的第 3 出现点的采样结果呈现出明显区别,因而在该点处表现为安全级突然增大.且两处的安全级取值均已超出安全阈值 0.815 1,可实现基于安全级比较的泄露感知.对比分析图 4-4 中的 Schneider IONsetup 电表软件中的后门,在第 12 运行状态的第 2 出现点及第 26 运行状态的第 6 出现点呈现安全级陡增,分别取值为 0.910 4 和 0.873 6,均超出安全阈值 0.869 6.进一步分析关联定义取值可知,第 12 运行状态的第 2 出现点处静态泄露度与动态泄露度取值均偏大,深入分析逆向痕迹与流量检测结果,逆向痕迹为半逆向破解,且存在后门探测利用.总结以上取值可以判定该场景中存在攻击者离线逆向破解与在线后门利用,但利用的准确度不高,证明目标后门并未被完全破解.而第 26 运行态的第 6 出现点处安全泄露度取值较大,具体分析流量检测结果发现,流量检测中存在外部主体的后门利用远程连接流量,可知在半逆向破解的情况下,后门已被攻击者成功利用实现远程控制.

4.4 对比分析

第一,安全性对比.为评估本方法的安全性,本文选择几种经典的访问控制模型进行对比分析[28],结合本文方法在基本定义、建模分析、威胁感知等方面的特点,共选择 3 种访问控制模型进行比较:强制访问控制模型 MAC、基于角色的访问控制模型 RBAC、基于属性的访问控制模型 ABAC.选择依据是:本文方法在本质上可理解为围绕后门隐私信息的数据泄漏感知方法,而经典的访问控制模型则是围绕目标信息构建以主体、客体的对象的访问策略集合与访问控制模型,因此有较大的可比性.同时,依据对目标信息进行属性定义的方法各有不同,选择以上 3 种典型的访问控制模型进行比对.

如表 4 所示,从模型本质上看,MAC 的特点在于主体到客体访问规则的强制性,BRAC 则定义了与角色关联的访问策略,ABAC 拓展到主体、客体、环境的属性范畴,而本文方法围绕工业物联网中的隐私信息建立了主体、客体、环境的多级属性定义,进而提出泄露感知方法.从属性定义上看,从 MAC 到 ABAC 的属性定义呈现出完整性优化的趋势,本文中的属性对象在 ABAC 进一步拓展,加入了面向场景的属性定义.从属性聚合的角度分析,前 3 种访问控制模型中只有 ABAC 涉及到部分的属性聚合过程,但并不包括全部的属性定义.本文则通过多属性决策方法将所有安全相关属性聚合为统一值,并利用灰色关联分析去除了属性间的不确定关系.从威胁关联和场景判决上看,由于访问控制策略重在事前防范,策略部署及实施的目标在于防范目标数据的恶意访问,因此均不涉及这两方面的功能.而本文方法针对泄露场景的实时特征抽取威胁关联关系,准确判决是否为泄露场景及泄露场景中泄露程度、泄露途径等具体泄露特征.

第二,可用性对比.鉴于目前面向工业物联网环境的数据泄露模型较少,而本文的原型系统从本质上看也可

等价于一个动态污点插桩系统,因此,本文选择 3 种典型的污点插桩系统进行性能比对,经预备实验结果分析可知,这 3 种典型插桩工具可在目标仿真环境中兼容运行,包括设备层、中间层及私有云层,因此具体同构对比的前提条件;且插桩平台主要用于污点跟踪系统部署前的目标程序修改,因此插桩过程的兼容则代表污点跟踪的可行性.实验主要从插桩方式、指令集支持种类、性能损耗几个方面对比系统的优劣性.

如表 5 所示,从插桩方式上看,Pin 针对镜像进行插桩时采用整体镜像缓存插桩,属于粗粒度插桩方法;而 DynamoRIO 在指令级控制插桩精度,更利用插桩分析实现准确、高效的插桩方法;DynInst 则是基于探针技术实现插桩,控制粒度较细,但开销较大.综合分析以上经典方法,BPLeakDetection 选择指令级缓存插桩,平衡插桩精度与系统开销.从指令集支持范围来看,Pin 和 DynamoRIO 主要支持 Windows 环境下的 x86 指令集,而 DynInst 则扩展至 PowerPC 指令集,本文的 BPLeakDetection 系统需兼容固件及 Windows 软件环境,因此支持 x86、arm、PowerPC 这 3 种指令集.最后对比性能损耗,由于本文基于指令集插桩实现,且扩展至多种指令集,因此损耗大于 Pin 和 DynamoRIO 平台,但优于 DynInst 平台,损耗在 210%左右.由于工业物联网环境对实时性要求较高,因而在部署插桩的过程中会对系统运行造成一定影响,但在部署完成后的污点检查及完整审计中对系统的性能影响基本可以忽略不计,对实时性影响较小.

Table 4 Comparison analysis for security

表 4 安全性对比分析

	MAC	RBAC	ABAC	本文方法
模型本质	强制主体服从客体访问策略的访问控制模型	角色与访问策略关联的访问控制模型	基于主体、客体与环境的属性设计的访问控制模型	包含主体、客体、环境等多级属性定义的数据泄露感知方法
属性定义	定义主体与客体的普通属性	围绕角色的不同定义主体与客体的属性	围绕主体、客体、环境 3 方面定义属性	围绕主体、客体、环境、场景 4 方面特征定义多级属性
属性聚合	不涉及	不涉及	部分涉及	利用多属性决策聚合多种属性,利用灰色关联分析去除属性之间的不确定性
威胁关联	不涉及	不涉及	不涉及	基于真实泄露场景的特征抽取实现感知方法与泄露威胁的实时关联
场景判决	不涉及	不涉及	不涉及	针对实时发生的泄露场景完成特征聚类与泄露判决

Table 5 Comparison analysis for availability

表 5 可用性对比分析

对比系统	插桩方式	指令集支持	性能损耗(%)
Pin	镜像级缓存插桩	x86	135.4
DynamoRIO	指令级缓存插桩	x86	168.1
DynInst[29]	探针插桩	x86/PowerPC	246.3
BPLeakDetection	指令级缓存插桩	x86/arm/PowerPC	211.8

当前隐私数据保护或隐私泄露防御的实现方法较多,对比同类研究成果,之前的研究工作针对某种典型环境中的典型隐私或敏感数据进行隐私保护方法或泄露防御方法研究,主要从泄露事前角度出发,大都基于加密算法或访问控制模型设计并实现数据保护或泄露防御.本文则主要从实时后门隐私泄露场景出发,从泄露场景中提取目标数据及数据环境的相关特征,并依据多属性决策方法生成判决语义,以此判定目标后门信息在静态结构或动态流向上的泄露程度,因此与同类方法相比,本文方法与泄露场景关联度较强,可用于泄露事前防御或泄露事中拒绝,并为泄露事后取证提供数据支持.

5 结 论

本文面向工业物联网环境中的后门隐私实现了一种信息泄露的感知方法,通过定义后门的基本属性、上层语义及判决语义从后门的静态二进制结构及动态数据流向中检测泄露场景的特征,最终结合灰色关联分析与多属性决策生成动态安全级,通过与安全阈值的比对判决泄露场景的细粒度特征.最后,本文通过目标环境中的

多种后门信息验证该方法及原型系统的有效性,并测试系统性能开销.后继工作中希望能基于泄露感知进一步实现后门隐私的实时防护,或基于已知后门的泄露感知推演生成同类信息的泄露感知方法.

References:

[1] Ning HS, Xu QY. Research on global Internet of Things' developments and it's lonstruction in China. ACTA ELECTRONICA SINICA, 2010,38(11):2590–2599 (in Chinese with English abstract).

[2] Kang SL, Du ZY, Lei YM, Wang J. Overview of industrial Internet of Things. Internet of Things Technolegies, 2013,(6):80–82 (in Chinese with English abstract).

[3] Yang JC, Fang BX, Zhai LD, Zhang FJ. Reseach towards IoT-oriented universal control system security model. Journal on Communications, 2012,(11):49–56 (in Chinese with English abstract).

[4] Cherdantseva Y, Burnap P, Blyth A, Eden P, Jones K, Soulsby H, Stoddart K. A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 2016,56(C):1–27.

[5] Ponomarev S, Atkison T. Industrial control system network intrusion detection by telemetry analysis. IEEE Trans. on Dependable & Secure Computing, 2016,13(2):1–13.

[6] Mitchell R, Chen IR. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. IEEE Trans. on Dependable & Secure Computing, 2015,12(1):16–30.

[7] Urbina DI, Giraldo JA, Cardenas AA. Limiting the impact of stealthy attacks on industrial control systems. In: Kruegel C, ed. Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. New York: Academic Press, 2016. 1092–1105.

[8] Abera T, Asokan N, Davi L, *et al*. C-FLAT: Control-Flow attestation for embedded systems software. In: Jaeger T, ed. Proc. of the ACM SIGSAC Conf. New York: Academic Press, 2016. 743–754.

[9] Daming C, Manuel E, Maverick W, *et al*. Towards automated dynamic analysis for linux-based embedded firmware. In: Gunter CA, ed. Proc. of the Network and Distributed System Security Symp. University of California Press, 2016. 452–468.

[10] Eschweiler S, Yakdan K, Gerhards-Padilla E. discovRE: Efficient cross-architecture identification of bugs in binary code. In: Gunter CA, ed. Proc. of the Network and Distributed System Security Symp. University of California Press, 2016. 49–64.

[11] Ooi ST, Lorber B. Avatar: A framework to support dynamic security analysis of embedded systems' firmwares. In: Gunter CA, ed. Proc. of the Network and Distributed System Security Symp. University of California Press, 2014. 112–129.

[12] Wang JH, Liu CY, Fang BX. Survey on data preserving for the search of internet of things. Journal on Communications, 2016,37(9):142–153 (in Chinese with English abstract).

[13] Fernandes E, Jung J, Prakash A. Security analysis of emerging smart home applications. In: Peterson Z, ed. Proc. of the 37th IEEE Symp. on Security and Privacy. University of California Press, 2016. 312–328.

[14] Earlence F, Justin P, Amir R, *et al*. FlowFence: Practical data protection for emerging IoT application frameworks. In: Holz T, ed. Proc. of the 2016 USENIX Security Symp. Boca Raton: CRC Press, 2016. 207–225.

[15] Wan S, Li FH, Niu B, Sun Z, Li H. Research progress on location privacy-preserving techniques. Journal on Communications, 2016,37(12):124–141 (in Chinese with English abstract).

[16] Narain S, Vo-Huu TD, Block K, Noubir G. Inferring user routes and locations using zero-permission mobile sensors. In: Peterson Z, ed. Proc. of the 37th IEEE Symp. on Security and Privacy. University of California Press, 2016. 397–413.

[17] Peng H, Chen H, Zhang XY, Zeng JR, Wu YC, Wang S. Privacy-Preserving *k*-NN query protocol for two-tiered wireless sensor networks. Chinese Journal of Computers, 2016,39(5):872–892 (in Chinese with English abstract).

[18] Dai H, Yang G, Qin XL, Liu L. Privacy-Preserving top-*k* query processing in two-tiered wireless sensor networks. Journal of Computer Research and Development, 2013,50(6):1239–1252 (in Chinese with English abstract).

[19] Wang P, Wang D, Huang XY. Advances in password security. Journal of Computer Research and Development, 2016,53(10): 2173–2188 (in Chinese with English abstract).

[20] Zhang YX, He JS, Zhao B, Zhu NF. A privacy protection model base on game theory. Chinese Journal of Computers, 2016,39(3): 615–627 (in Chinese with English abstract).

[21] Zeng JR, Chen H, Peng H, Wu Y, Li CP, Wang S. Privacy preservation in mobile participatory sensing. Chinese Journal of Computers, 2016,39(3):595–614 (in Chinese with English abstract).

[22] Xue R, Ren K, Zhang YQ, Li H, Liu JQ, Zhao B, Zhu LH. Introduction for special issure of security research for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1325–1327 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5010.htm [doi: 10.13328/j.cnki.jos.005010]

[23] Xue R, Feng DG. The approaches and technologies for formal verification of security protocols. Chinese Journal of Computers, 2006,29(1):1–20 (in Chinese with English abstract).

[24] Sajid A, Abbas H, Saleem K. Cloud-Assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 2016,4:1375–1384.

[25] Huberman BA. Ensuring trust and security in the industrial IoT—The Internet of Things (Ubiquity Symp.). Gastroenterology, 2002, 122(5):1235–1241.

[26] Viswanathan S, Tan R, Yau DKY. Exploiting power grid for accurate and secure clock synchronization in industrial IoT. In: Clack R, ed. Proc. of the Real-Time Systems Symp. Chicago: University of Chicago Press, 2017. 146–156.

[27] Hassanzadeh A, Modi S, Mulchandani S. Towards effective security control assignment in the industrial Internet of Things. In: Justin B, ed. Proc. of the Internet of Things. New York: Academic Press, 2015. 795–800.

[28] Li FH, Su M, Shi GZ, Ma JF. Research status and development trends of access control model. ACTA ELECTRONICA SINICA, 2012,40(4):805–813 (in Chinese with English abstract).

[29] Buck B, Hollingsworth JK. API for runtime code patching. Int'l Journal of High Performance Computing Applications, 2000,14(4): 317–329.

附中文参考文献:

[1] 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.电子学报,2010,38(11):2590–2599.

[2] 康世龙,杜中一,雷咏梅,张璟.工业物联网研究概述.物联网技术,2013,(6):80–82.

[3] 杨金翠,方滨兴,翟立东,张方娇.面向物联网的通用控制系统安全模型研究.通信学报,2012,(11):49–56.

[12] 王佳慧,刘川意,方滨兴.面向物联网搜索的数据隐私保护研究综述.通信学报,2016,37(9):142–153.

[15] 万盛,李凤华,牛犇,孙哲,李晖.位置隐私保护技术研究进展.通信学报,2016,37(12):124–141.

[17] 彭辉,陈红,张晓莹,曾菊儒,吴云乘,王珊.面向双层传感网的隐私保护 *k*-NN 查询处理协议.计算机学报,2016,39(5):872–892.

[18] 戴华,杨庚,秦小麟,刘亮.面向隐私保护的两层传感网 Top-*k* 查询处理方法.计算机研究与发展,2013,50(6):1239–1252.

[19] 王平,汪定,黄欣沂.口令安全研究进展.计算机研究与发展,2016,53(10):2173–2188.

[20] 张伊璇,何泾沙,赵斌,朱娜斐.一个基于博弈理论的隐私保护模型.计算机学报,2016,39(3):615–627.

[21] 曾菊儒,陈红,彭辉,吴垚,李翠平,王珊.参与式感知隐私保护技术.计算机学报,2016,39(3):595–614.

[22] 薛锐,任奎,张玉清,李晖,刘吉强,赵波,祝烈煌.云计算安全研究专刊前言.软件学报,2016,27(6):1325–1327. http://www.jos.org.cn/1000-9825/5010.htm [doi: 10.13328/j.cnki.jos.005010]

[23] 薛锐,冯登国.安全协议的形式化分析技术与方法.计算机学报,2006,29(1):1–20.

[28] 李凤华,苏铓,史国振,马建峰.访问控制模型研究进展及发展趋势.电子学报,2012,40(4):805–813.

沙乐天(1985－),男,江苏徐州人,博士,讲师,CCF 专业会员,主要研究领域为网络安全,物联网攻防.

孙晶(1985－),男,工程师,主要研究领域为通信网络技术,通信技术保障.

肖甫(1980－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为传感网,物联网.

王汝传(1943－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为物联网,网络安全.

陈伟(1979－),男,博士,教授,CCF 专业会员,主要研究领域为无线网络安全,移动互联网安全.