信息物理系统安全及相关措施①

邢静宇[1], 张立臣[2]

[1](南阳理工学院 软件学院, 南阳 473004)
[2](广东工业大学 计算机学院, 广州 510090)

摘 要: 开放互联的网络和信息与物理组件的交互使得信息物理系统面临着巨大的安全挑战, 通过研究信息物理系统的安全目标和攻击模型, 给出了分层的信息物理系统安全体系. 信息物理系统安全主要是解决在恶意攻击下的加密技术, 访问控制策略, 弹性机制等问题, 在介绍了信息物理系统安全方面的相关研究后, 对信息物理系统安全体系中的关键技术——访问控制策略和隐私数据保护进行了深入的研究.

关键词: 信息物理系统; 安全; 加密技术; 访问控制; 隐私保护

Cyber Physical System Security and Related Measures

XING Jing-Yu[1], ZHANG Li-Chen[2]

[1](School of Software, Nanyang Institute of Technology, Nanyang 473004, China)
[2](Faculty of Computer, uangdong University of Technology, Guangzhou 510090, China)

Abstract: Cyber physical system is facing enormous security challenges because of open and interconnected network and the interaction between cyber components and physical components. There is a description of layered cyber physical system security hierarchy by studying the security objectives and attack model of cyber physical system. Cyber physical system security is mainly to solve the encryption technology, access control strategy and resilience schema, etc. After the introduction of the related research of cyber physical system, gives a depth research about the key technologies of cyber physical system which including access control strategy and privacy data protection.

Keywords: cyber physical system; security; encryption technology; access control; privacy protection

信息物理系统(Cyber Physical System, CPS)是一个综合计算、通信和物理环境的多维复杂系统, 也是实现了计算资源和物理资源紧密结合与协调的下一代智能系统. 安全可靠是大型复杂系统的首要指标, CPS 强调信息与物理的交互, 因此, 物理组件与信息系统之间的安全信息传递变得更加重要, CPS 系统规模与复杂性对信息系统安全也提出了更高的要求[1]. 针对信息物理系统, 一种比较完善的安全服务包括: 数据机密性、信息完整性、身份认证、访问控制、可用性、鲁棒性、可扩展性、时效性、自适应和隐私保护.

1 信息物理系统安全目标

网络安全和 CPS 安全有很大的不同, 在网络安全中, 经常使用更新机制来对以前的安全软件进行修补, 但是, 这种方式对 CPS 系统中的安全却不适用. 因为, 在升级一个系统之前, 需要大量的时间安排规划现运行系统进行下线, 并且, 如果定期的停止工业级的服务器或计算机的运行去安装新的安全补丁, 这很大程度上损失了经济利益.

在信息物理系统中的安全问题, 有些只需提升现有技术安全等级, 有些需要全新的安全技术. CPS 的安全目标以传统的安全目标为基础可分为: 完整性, 有效性和机密性. 完整性是指数据或资源的可信任, 有效性是指系统的可访问和可使用能力, 机密性是指对非授权用户保持信息的不可访问. CPS 系统安全需求可分为以下几类: 感知安全, 通信安全, 信息存储安全,

① 基金项目:国家自然科学基金(61173046);广东省自然科学基金(S2011010004905)
收稿时间:2013-10-16 改稿时间:2013-11-18

行为控制安全及信息反馈安全. 信息物理系统的体系架构可分为三层, 分别为: 感知层, 数据传输层和应用控制层. 如图 1 所示:

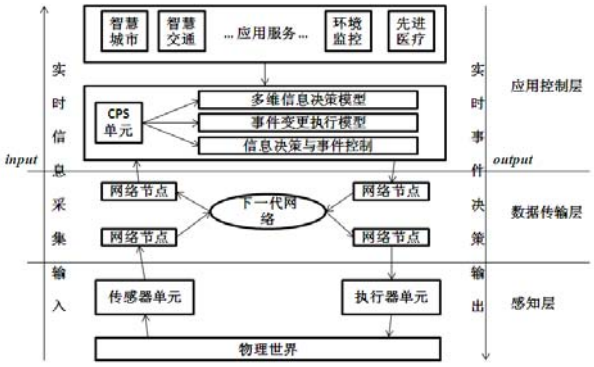

图 1 信息物理系统体系架构

2 信息物理系统攻击模型

将图 1 中的 CPS 体系架构中的实时信息采集输入定义为 input, 实时事件决策输出定义为 output, 那么, input 表示传感器数据到应用控制层 CPS 单元的输入, output 表示 CPS 单元命令发送至执行器的输出. 在应用控制层, CPS 单位的算法通常分为两类, 一类是估测算法, 用于跟踪物理世界的实时状态; 另一类是控制算法, 根据估测算法选择合适的控制命令返回.

在图 2 的攻击模型中, A 和 B 代表欺骗攻击, 在 A 中, 在从物理世界到 CPS 控制单元发送信息输入的过程中, 攻击者将 input 改变为 input', 反之, 在 B 中, 更改为 output', 错误信息中可能包含数据错误, 采集错误, 时间错误, ID 错误等. C 和 D 代表拒绝服务攻击, 在 C 中攻击者阻止或中断信息输入过程, 在 D 中攻击者阻止或中断命令传输过程. 在 C 和 D 中攻击者一种是攻击网络节点至其停止工作, 阻塞网络. 另一种是对感知层进行睡眠攻击, 迫使感知节点提前损坏失效.

3 信息物理系统安全体系

应用控制层是 CPS 的决策层, 需要决策 CPS 系统中的资源分配, 任务调度, 并且需要考虑经济因素的制约. 应用控制层提供了多样化的 CPS 平台, 整合了数据管理, 业务管理, 中间件等多种技术. 另外, 应用平台软件会涉及到大量的用户数据, 可能会有诸如非授权访问, 数据挖掘中的隐私泄露, 控制命令伪造攻击, 数据库攻击等各种安全威胁. 因此, 必须对应用控制层的隐私信息进行保护. 针对这些安全威胁的技

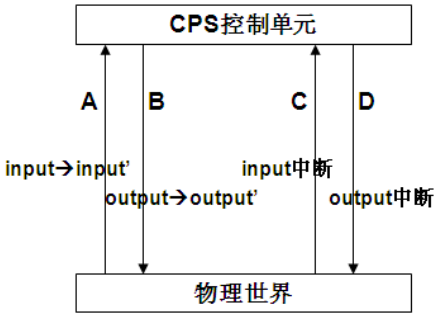

图 2 CPS 攻击模型

术性的安全对策包括计算机取证, 隐私保护, 身份认证与数据加密, 访问控制等.

信息物理系统具有独特的物理特性, 系统的计算和通信行为都需要满足实时性的约束, 在资源配置有限的动态场景中, 信息物理系统还需要满足自适应特性, 避免资源的过度调用和利用率不足. 网络系统对于信息物理系统的影响是巨大的, 因为它决定着 CPS 系统对物理世界的了解认知精度, 同时也决定了 CPS 系统对物理世界的控制执行粒度. 数据传输层的安全威胁有多种, 包括认证攻击, 拒绝服务攻击, 路由攻击, 跨网攻击, 汇聚节点攻击, 篡改路由加入网络等. 在技术上的安全对策包括入侵检测, 流量检测, 身份认证, 路由安全, 冗余路由, 加密和逐跳认证机制, 随即密钥分配机制等.

感知层和物理世界紧密联系, 感知层包含感知和控制两部分, 典型的物理设备包括 RFID 装置, 执行器单元, 图像捕捉装置, GPS 装置, 红外, 温度等各类传感器. 感知层的安全威胁包括设备破坏, 设备故障, 电磁干扰, 时钟同步攻击, 谐振攻击等. 在技术上的安全对策包括物理设备保护, 物理设备冗余和备份, 电磁屏蔽, 全局时钟控制, 无线资源监测等.

4 信息物理系统安全技术

信息物理系统的研究在国内刚刚起步, 相关的研究还非常有限. 在安全方面, 主要都是解决在恶意攻击下的加密技术, 访问控制策略, 弹性机制等问题. 文献[2]给出一种在无线移动 CPS 网络中的无证书签名机制, 解决了加密成本和密钥管理间的复杂性问题. 在文献[3]中, 作者提出, 在信息物理系统中, 由于信息

组件和物理组件之间的信息交互, 可能导致意想不到的信息流, 因此, 作者将时间特性加入机密决策, 使用形式化信息流模型描述在 CPS 模型中的信息泄露并给出了模拟结果. 信息物理系统中包含大量的反馈控制回路, 如果这些控制回路受到攻击, 那么会产生巨大的灾难性后果. 控制系统规模越来越庞大, 地理位置越来越分散, 那么就越容易受到攻击. Hamza Fawzi 等人在文献[4]中首先估测系统在受到攻击时的弹性应变能力, 然后给出一个算法估测在攻击状态下的系统状态并进行了性能描述.

4.1 访问控制策略

在信息物理系统中, 应用控制层上的应用十分复杂, 访问实体可能发生变化, 实体访问的资源可能发生变化, 对一个资源的访问可能包括环境上下文, 因此, 访问控制策略也应包含环境上下文安全. 另外, 外界环境因素可能引起访问控制配置的改变, 所以, 访问控制策略物理环境的安全也需考虑. 早期的访问控制模型主要有 DAC(Discretionary Access control, 自主访问控制), MAC(Mandatory Access Control, 强制访问控制)和 RBAC(Role-Based Access Control, 基于角色的访问控制)[5], ABAC(Attribute-Based Access Control, 基于属性访问控制)[6, 7]和 UCON(Usage Control, 使用控制)[8]等.

在 1992 年, David Ferraiolo 和 Rick Kuhn 提出了 RBAC(Role-Based Access Control)模型. 在该模型中, 首次引入了角色(Role)的概念, 将用户和权限通过角色进行了逻辑上的分离, 目前提出的大多数访问控制模型都是在 RBAC 模型基础上进行扩展, 增加时空约束, 增强 RBAC 模型的表达能力等. 但是 RBAC 模型系列没有考虑上下文信息, 限制了 RBAC 模型在信息物理系统中的应用. 在文献[9]中, Garcia-Morchon 等人扩展了 RBAC 模型, 将上下文感知列入访问控制系统, 系统设置了三种状态包括正常状态, 紧急状态和严重状态, 分别给出了在三种不同情形下的访问控制策略.

Busch 等人在文献[10]中使用统一的规则形式描述不同模型的安全策略, 提出一种可结合多种访问控制模型的安全策略. UCON 模型是继 RBAC 模型之后的下一代访问控制模型, Wu 等人在[11]中实现了在无线传感器网络中对移动用户通过多跳方式访问传感节点数据的访问控制. 王小明等人在文献[12]中建立了模糊访问控制的区间值模糊集合理论, 并提出了一种区间值模糊推理授权算法. 窦文阳等人在文献[13]提出了面向普适计算的模糊访问控制模型 (Fuzzy Role-Based Access Control, FRBAC). 该模型通过对模糊上下文进行推理, 得出用户在当前状态下可以激活的角色, 用户进而通过激活的角色得到访问资源的权限. 在文献[14]中作者提出一种面向普适计算的模糊主动访问控制模型(Fuzzy Active Access Control, FAAC), 并基于 ECA(Event Condition Action)规则形式, 描述了面向普适计算的访问控制的主动性和模糊性.

在文献[15]中, 作者给出一种信息物理系统的访问控制模型 FEAACS, 该模型可以在危机状态下自适应的分配危机角色, 主动分配访问控制权限给特定的实体, 使用基于优先级和危机态依赖性的行动生成模型选择最优响应路径, 在危机管理失败后可按容错的访问控制策略来消除危机态.

综合比较以上访问控制策略, 可以看出, 近年来访问控制取得的研究性进展主要在以下几个方面:

①对传统访问控制机制的扩展研究.

②针对环境与资源上下文动态改变的访问控制研究.

③模糊访问控制.

④基于信任的访问控制[16-19].

CPS 系统不仅包括信息系统, 也包括物理系统, 对环境和内部实体的安全性和稳定性有较高的要求, 找到一种完全适应于 CPS 系统应用的访问控制模型需要更多深入的研究, CPS 系统访问控制策略还存在以下几种问题:

①在需要快速验证授权的危机状态下, 访问控制策略的可靠授权效率较低, 直接影响着危机事件处理.

②主动访问控制机制不够灵活, 自主性和自适应性不强, 无法满足 CPS 系统的自适应的特点.

③对环境上下文利用率不足, 不能很好的适应无线传感网络的网络环境.

4.2 隐私数据保护

在具体的应用中, 隐私是某个个人或者某个机构等数据所有者不愿意或者不能被披露的敏感或私有信息. 隐私保护是信息安全问题的一种, 信息安全关注数据的机密性, 完整性和可用性. 隐私保护关注的主要问题是系统是否提供了隐私信息的匿名性. 随着 Web2. 0 技术的飞速发展, 各种网络应用应时而生, 随着大量的个人数据和信息在网络中的传递, 保证这些

信息在网络中的安全也变得非常重要.

在互联网中的用户隐私可大致分为三类: 身份信息, 隐秘信息, 用户地址. 身份信息包括姓名, 性别, 手机号, 身份证号等等. 隐秘信息包括个人日志, 机构内部信息等. 用户地址保护在网络环境下的用户 IP 信息, 实际 MAC 地址信息等.

射频识别是利用射频信号的空间耦合来实现无接触式的信息传递, 同时利用所传递的信息来达到识别的目的, 射频识别系统由三部分组成: RFID 标签, RFID 阅读器和后端数据库. RFID 系统中的安全威胁主要包括: 信号干扰, 恶意入侵和通信安全. RFID 系统中的隐私包括位置隐私和信息隐私. 针对 RFID 系统的隐私保护有两种解决方法, 一种是采用对 RFID 标签本身的物理保护方法, 一种是采用密码技术.

面向数据挖掘中的隐私保护即为在保护用户隐私的基础上进行准确, 高效的数据挖掘. 采用加密技术在数据挖掘过程中隐藏敏感数据的方法, 多用于分布式应用环境中, 例如安全多方计算(Secure Multiparty Computation, SMC). 在文献[20]中, 作者给出两种计算方法: 用户匿名和安全多方计算. 数据匿名化是指通过对数据进行随机等手段的变化来实现用户数据的隐藏, 数据匿名化研究主要包括两方面: 一是研究设计更好的匿名化原则, 怎样更好的发布数据又能保护隐私; 另一方面是针对特定的匿名化原则, 在特定的应用背景下, 设计更加“高效”的匿名化算法, 使得该算法在发布数据精度和计算开销间达到较好的平衡. 在文献[21]中, 作者提出一种经典的 k-匿名算法, 该算法能在数据包含有 k 个以上用户隐私信息时, 保证任意一个用户的隐私信息都是不可区分的. 在文献[22]中, 作者给出一种多维 k-匿名算法, 算法能够发布精度较高的数据并将原始数据映射到一个多维空间, 然后在该空间中对多维数据进行最优划分. 前面提到的都是针对静态数据而言的数据匿名算法, 文献[23]提出一种在动态环境下保护隐私的匿名化原则 m-Invariance.

表 1 隐私保护方法分类分析

现有技术	主要优点	主要缺点
射频识别隐私保护[24]	自动识别, 应用广泛	攻击者可通过射频标签窃取实体信息, 追踪实体身份获取实体隐私
用户匿名隐私保护	隐私保护程度好	匿名化原则的设计, 匿名化算法的计算开销较大, 数据精度不高
数据挖掘隐私保护	数据分析清晰	数据之间的潜在关联容易暴露个人隐私, 一定程度的数据损失影响数据的准确度
无线传感网位置隐私保护[25]	适用于无线传感网络	通信模块能量消耗大, 通信开销大, 通信延时长, 隐私保护度低
LBS(Location-Based Service)位置隐私保护[26]	快速精确的获知自己的位置可以使人们很方便的使用各种高级应用	攻击者可以利用位置信息推断出其它隐私信息

现有的隐私保护技术存在的不足包括:

①隐私保护技术的简单叠加无法满足新的隐私保护需求.

②现有的隐私保护技术在不同领域、不同网络形态中侧重点不同, 技术之间缺乏衔接, 无法屏蔽技术之间的异构性.

5 结 语

根据现有的安全问题及安全技术, 未来的 CPS 安全领域的研究将会在以下几个方面:

①未来对访问控制研究的方向包括: 无线传感网络环境下, 对只有有限计算、通信和存储能力且具有移动性的节点的安全与访问控制研究. 在需要快速验证授权的场合, 研究安全可靠快速可验证的授权和主动访问控制机制也是一个有意义的研究方向.

②在信息物理系统环境中, 可计算资源的上下文信息通常是模糊的, 不确定的和不完备的, 而且是动态更新的, 因此, 模糊访问控制理论和方法也会成为一个重要的研究方向.

③对于隐私数据保护, 需进一步研究在无线传感网和数据挖掘中的隐私保护. 隐私保护中的匿名化技术, 需要处理好隐私保护和结果准确性之间的平衡. 研究 CPS 多网融合的异构数据的数据隐藏方法是 CPS 安全领域的一个研究方向.

④传统的安全多方计算要求参与的计算资源可计算和可通信, 运算效率低, 寻找理想的安全多方计算的算法也是 CPS 安全研究的一个重要问题.

⑤信息安全的非技术因素, 包括公众对数据安全意识不强, 企业重数据采集, 轻数据挖掘和智能处理, 社会缺乏信息安全相关法律, 这也是未来的安全研究必须考虑的因素之一.

信息物理系统的体系结构从感应, 传输和服务的角度, 可分为感知层, 数据传输层和应用控制层, 由于在物理实体, 网络空间和应用服务的不同层面上, 信息物理系统面临的安全威胁有很大的不同, 因此, 需要针对不同的安全威胁提供不同的应对策略.

有些安全问题在新的信息物理系统中并未发生改变, 只需提升现有的安全等级即可. 有些安全问题则需要研究全新的安全技术. 提升现有的安全服务, 构建一个安全的信息物理系统的安全服务模型, 是下一步需要研究的目标.

参考文献

1 Akella R, McMillin BM. Model-checking BNDC properties in cyber-physical systems. Proc. of International mputer oftware and Application Conference. Seattle, WA. 2009. 660–663.

2 Xu Z, Liu X, Zhang GQ, He WB, Dai GZ, Shu WH. A certificateless signature scheme for mobile wireless cyber-physical systems. Proc. of the 28th International Conference on Distributed Computing Systems Workshops. Beijing. 2008. 489–524.

3 Tang H, McMillin BM. Security property violation in CPS through Timing. Proc. of the 28th International Conference on Distributed Computing Systems Workshops. Beijing. 2008. 519–524.

4 Fawzi H, Tabuada P, Diggavi S. Secure estimation and control for cyber-physical systems under adversarialttacks. http://arxiv. org/abs/1205. 5073. [2013-8-8].

5 Ferraiolo D, Kuhn R. Role-based Access Controls. Proc. of 15th NIST-NCSC National Computer Security Conference. USA Baltimore. 1992. 554–563.

6 Bonatti P, Samarati P. A uniform framework for regulating service access and information release on the web. Journal of Computer Security, 2002, 10(3):241–271.

7 王小明,付红,张立臣.基于属性的访问控制研究进展.电子学报,2010,38(7):1660–1667.

8 Park J, Sandhu R. The usage control model. ACM Transactions on Information and System Security, 2004, 7(1): 128–174.

9 Garcia-Morchon O, Wehrle K. Modular context-aware access control for medical sensor networks. Proc. of the 15th ACM Symposium on Access Control Models and Technologies. New York, NY, USA. 2010. 129–138.

10 Busch S, Muschall B, Pernul G, Priebe T. Authrule: A generic rule-based authorization module. Lecture Notes in ComputerScience, 2006, 4127: 267–281.

11 Wu J, Shimamoto S. Usage control based security access scheme for wireless sensor networks. Proc. Of the IEEE International Conference on the Communications(ICC' 2010). Cape Town, South Africa. 2010. 1–5.

12 王小明.面向普适计算的区间值模糊访问控制.计算机科学与探索,2010,4(10):865–880.

13 窦文阳,王小明,张立臣.普适环境下的动态模糊访问控制模型研究.计算机科学,2010,37(9):63–67.

14 张立臣.面向普适计算的主动访问控制模型研究[学位论文].西安:陕西师范大学,2011.

15 芦东泽.信息物理系统的安全访问控制机制[学位论文].大连:大连理工大学,2010.

16 郭亚军,王亮,洪帆,韩兰胜.基于信任的普适计算的动态授权模型.华中科技大学学报(自然科学版),2007,35(8):70–73.

17 廖俊国,洪帆,朱更明,杨秋伟.基于信任度的授权委托模型.计算机学报,2006,29 (8):1265–1270.

18 Campbell R, AI-Muhtadi J, Naldurg P, Sampemane G, Mickunas MD. Towards security and Privacy for pervasive computing. Lecture Notes in Computer Science. 2003. 2609. 77–82.

19 Hourdin V, Tigli J, Lavirotte S, Rey G, Riveill M. Context-sensitive authorization in interaction patterns. Proc. of the 6th International Conference on Mobile Technology, Application & Systems. Nice, France. 2009. 1–8.

20 Oleshchuk V. Internet of Things and Privacy Preserving Technologies. Proc. of the 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, Wireless VITAE'09. Aalborg, Denmark. 2009. 336–340.

21 Sweeney L. K-anonymity: A model for protecting privacy. International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, 2002, 10(5): 557–570.

22 LeFevre K, DeWitt DJ, Ramakrishnan R. Mondrian multi-dimensional k-anonymity. Proc. of the 22nd International Conference on Data Engineering (ICDE). Atlanta, Georgia, USA. 2006. 25–35.

23 Xiao X, Tao Y. m-Invariance: Towards privacy preserving re-publication of dynamic datasets. Proc. of the ACM SIGMOD Conference on Management of (SIGMOD). Beijing. 2007. 689–700.

24 张涛.射频识别系统中安全与隐私研究[学位论文].西安:西安电子科技大学,2010.

25 Nezhad AA, Miri A, Makrakis D. Location privacy and anonymity preserving routing for wireless sensor networks. Computer Networks, 2008, 52(18): 3433–3452.

26 黄毅,潘晓,孟小峰等.Orient Privacy:移动环境下的隐私保护服务器.计算机研究与发展,2010,47(z1):438–441.