计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2018,27(7):50−56 [doi: 10.15888/j.cnki.csa.006453]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向智慧城市的数据驱动信息物理系统安全威胁分析模型与方法①

蒋建春[1], 肖佳平[1], 唐　琨[2]

[1](中国科学院 软件研究所, 北京 100190)
[2](南宁市发展和改革委员会, 南宁 530028)
通讯作者: 肖佳平, E-mail: jiaping@iscas.ac.cn

摘　要: 信息物理系统 (CPS) 是一个集成计算、通信和物理过程的混成系统, 在智慧城市中占据至关重要的地位,其安全问题面临许多挑战. 本文首先建立信息物理系统安全威胁分析模型, 给出 CPS 各个组成部件的安全威胁, 然后提出了信息物理系统的威胁关联分析方法, 并以智能电网为例给出实验测试结果. 结果表明, 该方法能实现快速大规模安全威胁建模和自动化分析, 为智慧城市中的关键信息基础设施提供技术支撑. 最后, 本文总结了智慧城市中信息物理系统的安全威胁研究进展和未来研究方向.

关键词: 智慧城市; 信息物理系统; 入侵检测; 高级持续威胁; 硬件威胁

引用格式: 蒋建春,肖佳平,唐琨.面向智慧城市的数据驱动信息物理系统安全威胁分析模型与方法.计算机系统应用,2018,27(7):50–56. http://www.c-s-a.org.cn/1003-3254/6453.html

Data-Driven Cyber-Physical System Security Threat Analysis Model and Method for Smart Cities

JIANG Jian-Chun[1], XIAO Jia-Ping[1], TANG Kun[2]

[1](Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[2](Nanning Municipal Development &Reform Commission, Nanning 530028, China)

Abstract: A Cyber-Physical System (CPS) is a mixed system integrated with computation, communication, and physical processes, which takes an important position in the smart city, and there are many challenges in its security issues. Firstly, we establish a cyber security model for CPS, providing with the security threats of various components of CPS. Then, we propose a CPS threats analysis method and provide experimental test results. The results show that this method can achieve rapid large-scale security threat modeling and automatic analysis. Consequently, it can provide technical supports for the security assurance of the key information infrastructures in smart cities. Finally, we summarized the research advance and future research direction of security threats on CPS in the smart city.

Key words: smart city; Cyber-Physical Systems (CPS); intrusion detection; advanced persistent threat; hardware threat

信息物理系统 (Cyber-Physical Systems, CPS) 是指一个集成了计算、通信和物理过程的混成系统, 具有自主行为的智能化、网络化、开放控制系统[1]. 在智慧城市建设进程中, CPS 将占据核心地位, 例如依靠大数据出行的智能交通系统、物联网、融合生物信息采集验证的电子政务系统和智能电网等. 美国国家科学基金会 (NSF) 认为, CPS 将让整个世界互联起来, 如同互联网改变了人与人的互动一样, CPS 将会改变我们与物理世界的互动[2]. 2007 年 7 月, 美国总统科学技术顾问委员会在题为《挑战下的领先——竞争世界中的信

① 基金项目: 南宁市大数据关键信息基础设施安全体系研究 (2017 NCCJA043)
Foundation item: Study on the Security System of Big Data Key Information Infrastructure in Nanning (2017 NCCJA043)
收稿时间: 2017-11-29; 修改时间: 2017-12-12; 采用时间: 2017-12-27; csa 在线出版时间: 2018-04-18

息技术研发》的报告中列出了 8 大关键的信息技术, 其中 CPS 位列首位[3]. CPS 的应用也极为广泛, 应用包括高可信的医疗设备和服务系统、智能高速公路、智能交通系统、智能电网、分布式机器人等[4]. 但与此同时, 信息物理系统的安全问题相继出现, 与信息物理系统相关的安全威胁事件逐年递增. 根据美国工业控制系统网络应急响应组统计, 2011 年上报工业控制系统相关的安全事件 198 件. 2010 年, 震网 (Stuxnet) 蠕虫事件利用西门子公司控制系统存在的漏洞, 感染数据采集与监测系统 (SCADA), 隐蔽实施攻击活动, 导致伊朗布什尔核电站项目推迟[5]. 2011 年, 美国华盛顿大学与加州大学圣地亚哥分校的研究团队, 发表了一篇题为《汽车攻击面的综合实验性分析》的论文, 该论文提到直接拨打车载电话号码或是播放特制的声音信号就能取得汽车的控制[6]. 2013 年, 德国安全研究人员 Hugo Teso 在 Hack In The Box 黑客大会上表示, 利用航空系统 ACARS 的相关漏洞, 可以控制飞机[7]. 同互联网的安全事件相比较, 针对工业控制系统的事件数量小, 但因工业控制系统涉及到国计民生和国家关键基础设施的安全控制, 其安全事件带来的影响和危害巨大. 因此, 系统化分析信息物理系统的安全威胁显得十分必要.

本文内容组成如下: 第 1 节是已有的相关研究工作; 第 2 节是信息物理系统安全威胁分析模型与威胁分析方法; 第 3 节信息物理系统安全威胁分析系统工具实现; 第 4 节信息物理系统安全威胁分析案例; 第 5 节, 总结智慧城市中信息物理系统安全威胁模型分析方法和未来的研究方向.

1 相关工作

安全威胁分析是信息物理系统的核心问题之一, 针对该问题, 国内外研究人员已开展了相关研究工作. Clifford Neuman 等研究人员分析了信息物理系统的网络域、物理域相互影响的 7 种安全威胁模式, 即 CC (Cyber-Cyber threats)、CP (Cyber-Physical threats)、PC (Physical-Cyber threats)、PP (Physical-Physical threats)、CPP (Cyber-Physical-Physical threats)、CPC (Cyber-Physical-Cyber threats)、PCP (Physical-Cyber-Physical threats)[8]. M.Yampolskiy 等提出基于数据流图分析 CPS 的安全威胁[9]. Katherine R. Davis 等提出利用信息系统和物理系统依赖关系在线辨识 CPS 脆弱点[10]. 关于安全威胁建模方法, 常见的方法有攻击树、攻击图、威胁列表、本体等方法. 在威胁建模工具方面, 开源代码工具有 TRIKE、SeaMonster 等, 而商业方面的安全建模工具有 Threat Modeler、Corporate Threat Modeller、SecurlTree、Little-JIL 以及微软 SDL 威胁建模工具等[11]. Oleg Mikhail Sheyner、Xinming Ou 提出利用攻击图构建安全威胁场景[12]. 上述已有的安全威胁建模的研究方法局限于网络域, 不能对信息物理系统的跨域安全威胁进行建模分析. 同时对于智慧城市的信息物理系统来说, 其涉及组件之众多, 组件之间存在多种依赖关系, 各组件的安全漏洞数量动态变化, 而且组件时有更新, 传统的安全威胁建模方法依赖专家经验, 难以适应大规模、快速、智能化的安全威胁建模. 本文拟主要针对智慧城市的 CPS, 提出一种基于大数据、通用的信息物理系统安全威胁分析模型和威胁视图分析方法, 实现大规模安全威胁自动化建模, 为智慧城市的网络安全建设提供技术支撑.

2 信息物理系统威胁分析研究框架

2.1 信息物理系统模型

信息物理系统实现信息空间、物理空间的融合, 计算深度嵌入到物理设备中, 首先利用传感器获取物理世界的数据信息, 然后把这些数据通过异构网络传输到数据分析中心进行深度计算, 执行器依据计算结果控制物理设备及环境的状态变化, 从而形成感知、联网、计算、控制复杂的系统. 为更好分析信息物理系统的安全威胁, 本文将信息物理系统抽象为感知组件、网络传输组件、计算分析决策组件、控制执行组件、人机交互组件、物理实体组件.

(1) 感知组件

感知组件是 CPS 的数据来源和控制命令执行器, 是信息空间和物理世界连接点, 因感知部件所处环境为开放性、不确定性环境, 而感知节点数据处理能力、通信能力和存储能力有限, 极易形成对 CPS 的攻击威胁. 感知部件面临的安全威胁有物理攻击威胁、女巫攻击威胁、节点捕获攻击威胁、传感器数据攻击威胁、传感器侧信道攻击威胁、传感器操作系统攻击威胁、传感器节点假冒攻击、能耗攻击等.

(2) 网络组件

网络组件是 CPS 的神经网络, 是信息空间和物理世界联接器. CPS 的网络传输结构、接入方式、通信

协议存在各种安全脆弱性, 从而导致攻击威胁发生. 网络部件面临的安全威胁有路由攻击、黑洞攻击、蠕虫漏洞攻击、HELLO 泛洪攻击、SCADA 攻击、控制网络拒绝服务攻击等.

(3) 计算分析决策组件

计算分析决策组件是信息物理系统的“大脑”, 该组件依据搜集到的数据信息, 通过计算分析, 给信息物理系统发出控制操作指令. 决策层的安全威胁除研究传统信息空间攻击外, 还有新的攻击方法, 例如数据注入攻击、机器学习算法攻击、恶意代码攻击等. 北卡州立大学的研究人员分析电力网络的状态估计算法安全缺陷, 提出了虚假数据的注入攻击方法, 该方法通过访问电力系统的配置信息, 操纵测量器的测量, 可以绕过目前电力系统的异常数据度量方法检测, 从而改变状态估计结果[13,14].

(4) 控制执行组件

控制执行组件是信息空间和物理世界的交互点, 通过控制执行部件的操作可将信息空间数据处理结果转换成物理世界过程, 从而导致信息空间能够影响到物理世界. 控制执行层的安全威胁主要有控制命令伪装攻击、控制协议攻击、控制网络攻击等.

(5) 人机交互组件

人机交互组件是人同信息物理系统进行交互操作的窗口, 通过人的外部干预, 确保信息物理系统按照人类预期行为进行活动. 人机交互组件的安全威胁主要有认证攻击、身份假冒攻击、权限滥用攻击、数据驱动攻击等.

(6) 物理硬件组件

信息物理系统通过物理实体组件来影响和操作外部物理环境及对象. 物理实体组件将信息物理系统的信息转化成物理行为或改变物理环境.

2.2 安全威胁分析系统模型框架

本文的信息物理系统安全威胁分析系统框架由信息物理系统版本数据库、工控组件漏洞数据库、组件安全威胁知识库、威胁搜索与关联引擎、安全威胁分析模块和系统安全威胁分析结果展示模块组成, 系统结构框架如图 1 所示.

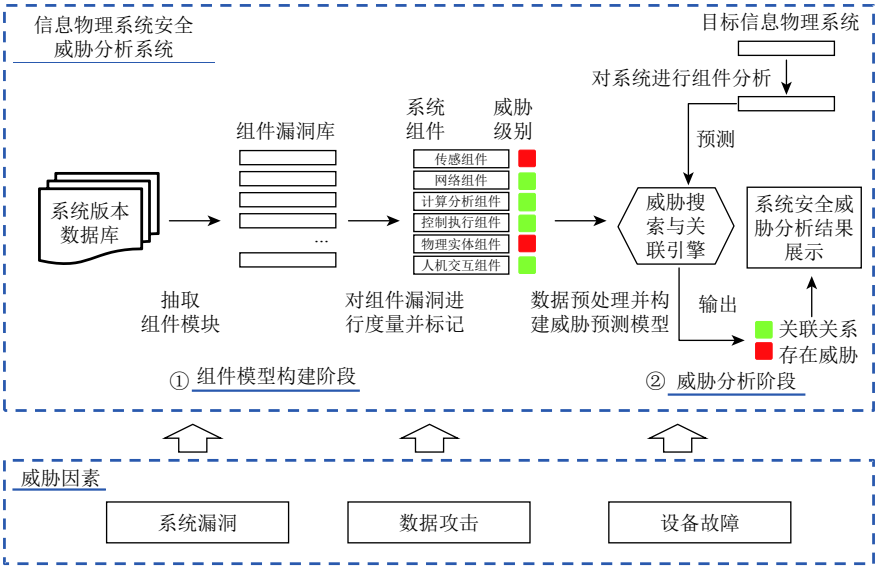


图 1 基于威胁库和漏洞库搜索关联的信息物理系统安全威胁分析框架

信息物理系统版本数据库用于存放各个阶段的系统版本信息 (包括传感器设备信息、支撑操作系统和路由协议等). 工控组件漏洞数据库用于实时更新存储已发现的信息物理系统组件相关漏洞数据. 组件安全威胁知识库用于存放信息物理系统组件相关的安全威胁数据 (例如验证绕过、欺骗、失控和自毁等). 威胁搜索与关联引擎则根据提供的信息物理系统组件名称及安全漏洞, 生成相关的安全威胁列表, 并根据提供的信息物理系统组件关联关系及安全威胁列表生成组合的安全威胁关联图. 安全威胁分析模块输出系统存在

的威胁以及相互关联关系, 安全威胁分析结果展示则根据各个模块提供的数据, 生成相应可视化结果供决策者制定相应方案.

通过研究信息物理系统安全威胁分析系统框架, 我们可以清晰提取出信息物理系统安全威胁分析的三个重要因素.

(1) 威胁因素

信息物理系统安全不同于传统意义上的网络安全, 它的威胁因素包括系统漏洞、数据攻击和设备故障, 识别难度远高于传统的网络安全, 因此在对信息物理系统进行安全威胁分析的过程中首先需要明确知悉分析对象的威胁因素, 从而选择合理的分析方法. 本文使用各司其职的方式对威胁因素进行识别, 即每个组件单独设置威胁警报, 例如传感器组件故障则利用故障检测方法监测, 数据攻击则利用数据攻击识别监测.

(2) 组件特征元

信息物理系统所涉及的组件之多由图 1 可以看出, 包括感知组件、网络传输组件、计算分析决策组件、控制执行组件、人机交互组件和物理实体组件. 每个组件的特性如何用不同的特征元来描述成为安全威胁分析的前提条件. 本文利用系统版本、组件标签和编号来对系统的组件进行标记.

(3) 威胁搜索与关联引擎

威胁搜索与关联引擎是安全威胁分析的核心部分, 通过系统组件分析得到的组件特征元在漏洞数据库中快速搜索, 在安全威胁知识库获取安全威胁情况, 同时建立全系统的安全威胁关联视图, 构造完整的威胁途径. 本文的威胁搜索与关联算法在 2.3 节具体描述.

2.3 安全威胁搜索与关联分析方法

安全威胁搜索与关联分析是实现大规模信息物理系统自动化安全威胁分析的核心部分, 主要包括单节点安全威胁分析和复合安全威胁分析.

(1) 信息物理系统单节点安全威胁分析方法

在信息物理系统建模基础上, 本文提出基于知识驱动安全威胁分析及基于实体关联的威胁分析方法, 以系统化分析信息物理系统的安全威胁. 其中, 信息物理系统组件安全威胁的分析方法可采用基于安全威胁知识库来驱动, 其分析方法步骤描述如下:

第 1 步, 获取信息物理系统组件的脆弱性, 即判断系统特征组件存在的攻击危险;

第 2 步, 通过特定数据库, 例如 CVE 库, 获取信息物理系统组件的相关威胁库;

第 3 步, 检查指定的信息物理系统组件威胁的脆弱性是否存在, 如果存在则标示组件存在安全威胁; 否则, 重复第二步, 直到组件威胁库分析完毕;

第 4 步, 生成信息物理系统的组件安全威胁全局清单.

(2) 信息物理系统复合安全威胁分析方法

复杂的信息物理系统安全威胁不是针对单个组件, 而是利用多个组件的安全脆弱性构成安全威胁图, 从而实现攻击目标, 例如 APT 高级持续威胁. 本文提出采用组件关联安全威胁的分析方法, 基于组件之间的关联关系, 建立组件安全威胁关联视图. 具体步骤描述如下:

第 1 步, 任选信息物理系统的一个组件, 标示为 C, 确定 C 与其它组件的关联关系, 以关联矩阵表示.

第 2 步, 根据单节点安全分析 (1) 中的安全威胁全局清单, 依次选择信息物理系统组件 C 的安全威胁列表 T={T1,T2,⋯,Tn}.

第 3 步, 分析信息物理系统组件 C 与其它组件的关联安全影响, 如果组件 C 与组件 B 有安全关联, 即组件 C 的安全威胁脆弱性造成 B 受到威胁, 则标示组件 C 与 B 的安全关联威胁连接; 否则, 重复第二步, 直到组件 C 威胁分析完毕.

第 4 步, 生成信息物理系统组件 C 的关联威胁图.

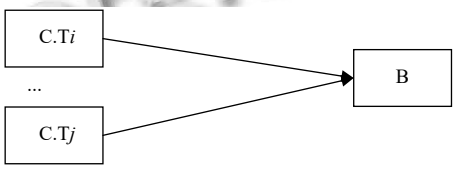


图 2 组件关联威胁图示例

第 5 步, 重复第 1 步, 直到信息物理系统所有组件分析完毕.

第 6 步, 生成信息物理系统的所有分析组件的安全威胁关联视图.

3 系统实现与评价

3.1 系统实现

本文将从信息物理系统组件漏洞分析、安全威胁分析、威胁关联分析和安全威胁路径分析 4 个方面建立信息物理系统安全威胁分析系统原型. 为了实现数

据驱动的信息物理系统安全威胁分析, 设计如下算法.

算法 1. 信息物理系统组件漏洞分析

输入: 组件名、漏洞列表
输出: 组件名漏洞列表, 形如<组件名, 漏洞名>

过程步骤:
1) 初始化获取 CVEDB 数据集, 提取 CVE 漏洞条目为 Y
2) 初始化组件 A 的特征数据 X
3) 检查 Y 是否含有 X, 如果有, 则产生<A, Y>
4) 检查 CVEDB 数据集是否检查完毕, 否则, 重复 1)

算法 2. 信息物理系统组件安全威胁分析

输入: <组件名, 漏洞名>, <漏洞名, 威胁名>
输出: 组件名威胁列表 , 形如<组件名, 威胁名>

过程步骤:
1) 初始化组件 A 的漏洞数据 CVE
2) 初始化威胁库 VBThreatDB
4) 从 CVE 提取组件 A 的漏洞数据条目 X*i*
5) 将 X*i* 与 VBThreatDB 的漏洞进行匹配
6) 如果匹配成功,则产生此漏洞对应的威胁关系, <A→Xi→T>
7) 检查组件的漏洞数据是否分析完毕, 否则重复 4
8) 输出组件威胁库<A→CVE→T>

算法 3. 信息物理系统组件威胁关联分析

输入: 组件威胁库 CTheatDB = <A→CVE→T>, 威胁触发 StartT = <触发条件 1, 触发条件 2, …, 触发条件 *n*>
输出: 威胁关联 <T1→T2>

过程步骤:
1) 初始化组件 A 的 CThreatDB
2) 初始化威胁触发 StartT
3) 从 CTheatDB 提取漏洞数据条目 X 和 Y
4) 将 X.T(StartT) 与 Y.T(StartT) 进行交集运算
5) 如果不为空,则产生 A →X.T→Y.T
6) 检查组件的 CTheatDB 是否两两匹配分析完毕,否则重复 2)
7) 输出威胁关联结果

算法 4. 信息物理系统组件安全威胁路径分析

输入: 组件关联数据, 形如<组件名 A1, 组件名 A2>, 组件名 A1 威胁列表, 形如<组件名 A1, 威胁名 T1>
输出: 关联威胁途径列表, 形如<组件名 A1, 威胁名 T1, 组件名 A2 >

过程步骤:
1) 组件 A1 关联数据初始化 X
2) 组件 A1 威胁数据初始化 Y
3) 从 Y 提取威胁数据 T1
4) 从 X 提取关系 RELATIONSHIP(A1, A2)
5) IF RELATIONSHIP(A1, A2) = TRUE
THEN <A1. T1→ A2>
6) ELSE
检查 A1 的关联数据库 X 是否为空, 否则重复 (4)
检查 A1 的威胁数据库 Y 是否为空, 否则重复 (3)
输出可视化结果

3.2 案例验证

本文以智慧城市的智能电网为例, 验证所提出的信息物理系统的安全威胁分析方法. 智能电网的信息物理系统的架构模型如图 3 所示. 智能电网的信息物理系统由 AMI 头端/系统操作员/数据中心的源端、配电分布的网络端和用户端三个层次构成. 威胁因素为系统漏洞导致电压负载不均衡威胁, 工控系统的程序漏洞数据库来自国家安全信息漏洞共享平台.

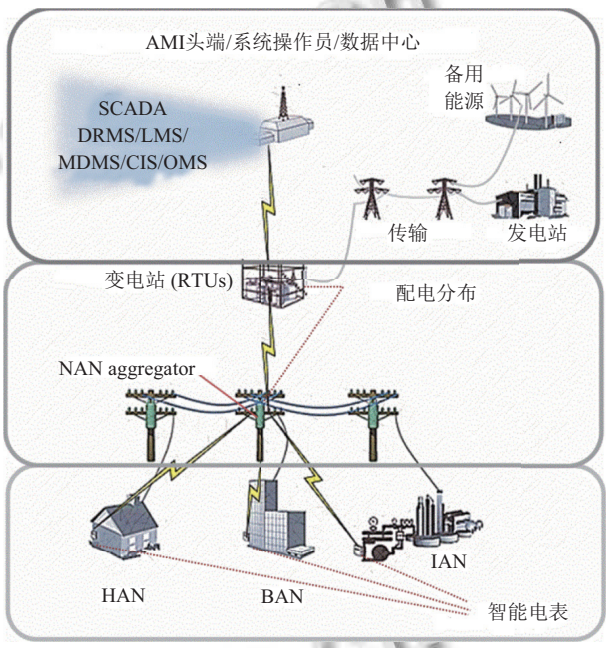


图 3 智能电网多层概念架构模型[15]

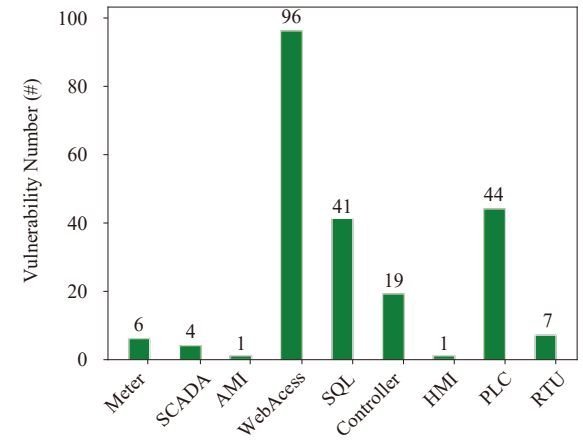
本文首先通过爬虫抓取与工控系统相关的漏洞存储到本地工控系统的程序漏洞数据库, 同时在多个文献资源库搜集漏洞对应的威胁结果建立安全威胁知识库. 本文分析系统漏洞导致电压负载不均衡威胁, 利用检索 IEEE 电子文献库构建电压负载不均衡威胁知识库, 共检索 25 篇有关智能电网电压负载不均衡安全威胁的文章. 威胁知识库以自动和人工的方式实现定期更新. 其次, 对智能电网的系统组件进行词频分析和扫描分析, 按 2.1 归类, 构建智能电网的组件字典和特征量, 如表 1 所示. 然后, 通过在程序漏洞数据库中进行漏洞搜索与扫描. 检测到系统的 SQL 数据注入共有 41 例, 其中 33 例危害级别为“高”, 7 例危害级别为“中”, 1 例危害级别为“低”. 控制器漏洞共有 19 例, 其中 12 例危害级别为“高”, 7 例危害级别为“低”; PLC 漏洞共有 44 例, 其中 25 例危害级别为“高”, 16 例危害级

别为“中”, 3 例危害级别为“低”; PowerSCADA 漏洞共 4 条, 其中 1 例危害级别为“高”, 3 例危害级别为“中”, 10 例危害级别为“低”. 漏洞扫描结果如图 4 所示.

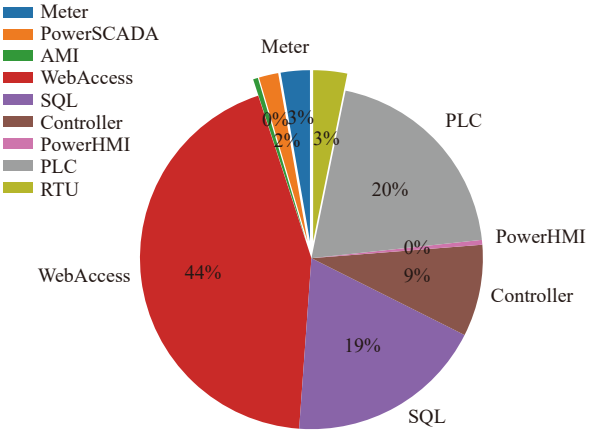
表 1 智能电网系统漏洞扫描结果

组件	漏洞库
感知组件	SCADA、AMI、仪表漏洞
网络组件	Web 漏洞、VPN 漏洞
计算分析决策组件	SQL 漏洞
控制执行组件	Controller 漏洞
人机交互组件	HMI、人因漏洞
物理硬件组件	PLC/RTU 漏洞

最后通过字段匹配建立威胁关联<数据不完整→负载不均衡>, 由漏洞数据库已知组件漏洞<计算分析决策组件→SQL 注入>和威胁<SQL 注入→数据不完整/错误>, 因此根据本文算法 3 建立威胁关联<计算分析决策组件→SQL 注入→数据不完整→负载不均衡>, 同时建立完整威胁路径<恶意数据攻击→计算分析决策组件→SQL 注入→数据不完整→负载不均衡>. 搜索关联得到 SCADA 漏洞同样存在威胁<SCADA 漏洞→数据不完整/错误>, 则据此匹配建立威胁途径有向图. 智能电网中通过引擎计算得到的所有威胁有向图如图 5 所示, 组件与威胁之间边的条数表示组件产生该威胁的漏洞个数. 威胁分析的所有操作均通过 Python 实现自动化检测和分析. 由图 5 可知, 智能电网中的信息物理系统由网络组件带来的漏洞威胁远远大于其他组件, 漏洞个数排列依次为网络组件 > 物理硬件组件 > 计算分析决策组件 > 控制执行组件 > 感知组件 > 人机交互组件, 因此需要加强智能电网中网络组件和物理硬件组件的监控和更新升级, 以提高关键性基础设施的安全性和可靠性.



(a) 智能电网系统漏洞分布柱状图



(b) 智能电网系统漏洞分布扇形图

图 4 漏洞扫描结果

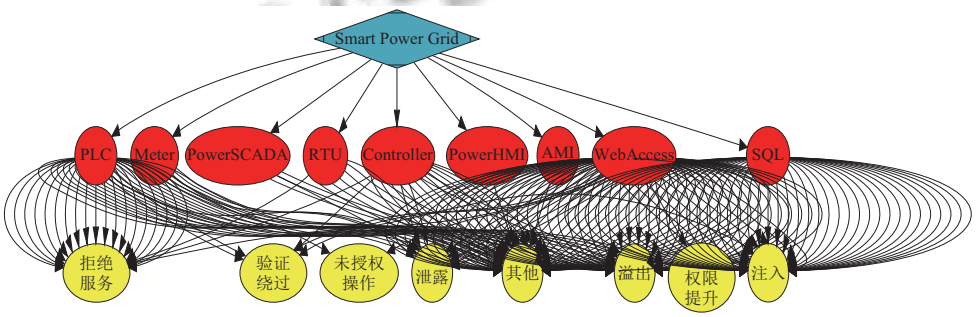


图 5 智能电网系统安全威胁分析智能生成威胁有向图

本文提出的方法适用于存在显性依赖关系的信息物理系统安全威胁建模分析, 信息物理系统的特征组件通过词频分析得到并按属性分类, 漏洞库和威胁库可设置为定时更新, 可实现普遍意义上信息物理系统的大规模自动安全威胁建模分析, 具有一定的通用性.

4 相关工作比较分析

传统的安全威胁分析利用人工方法, 构造攻击树来实现安全威胁分析. 同已有的工作相比较, 本文所提出的安全威胁分析方法以安全数据驱动, 通过安全漏洞数据、安全威胁数据所依赖的实体关系, 建立完整的安全威胁链路模型. 文献[12]利用漏洞相互关系形成攻击图, 而本文的安全威胁关联分析方法利用实体物理事实上的业务相互依赖关系, 实现智能化安全威胁分析, 构建安全威胁路径图. 本文有利于发现隐蔽的、间接的安全威胁路径, 同时可根据具体的攻击行为快速找到攻击路径, 为系统防御提供决策性指导.

5 结论与展望

本文首先分析信息物理系统安全问题及抽象的组件模型, 在此基础上提出了基于知识库驱动安全威胁分析及基于实体关联的威胁分析方法, 以系统化分析信息物理系统的安全威胁, 并研发实现信息物理系统安全威胁分析原型系统, 给出了智能电网的安全威胁分析案例, 为智慧城市的关键性基础设施信息化进程提供一种实时可靠的安全威胁分析方法和防御工具. 本文所提出的分析方法和工具原型仍需人工干预, 组件威胁的隐性依赖关系需进一步依据更多的数据进行挖掘, 其分析方法的完备性及适应性需进一步研究.

参考文献

1 Lee EA, Seshia SA. Introduction to embedded systems: A cyber-physical systems approach. 2nd ed. Kamp Bridge, Massachusetts: MIT Press, 2017. http://leeseshia.org.

2 US National Science Foundation. Cyber-physical systems (CPS). https://www.nsf.gov/pubs/2011/nsf11516/nsf11516.htm. [2016-11-07].

3 Marburger JH, Kvamme EF, Scalise G, *et al*. Leadership under challenge: Information technology R&D in a competitive world. An Assessment of the Federal Networking and Information Technology R&D Program. Executive Office of The President's Council of Advisors on Science and Technology. Washington, DC, USA. 2007.

4 Khaitan SK, Mccalley JD. Design techniques and applications of cyberphysical Systems: A survey. IEEE Systems Journal, 2015, 9(2): 350–365.

5 Kushner D. The real story of stuxnet. IEEE Spectrum, 2013, 50(3): 48–53.

6 Checkoway S, Mccoy D, Kantor B, *et al*. Comprehensive experimental analyses of automotive attack surfaces. Proceedings of the 20th USENIX Conference on Security. Berkeley, CA, USA. 2011. 6.

7 Gross D, CNN. Hacker says phone app could hijack plane. CNN. com, 2013, 12.

8 Neuman C. Challenges in security for cyber-physical systems. Workshop on Future Directions in Cyber-physical Systems Security. Newark, NJ, USA. 2009. 1–4.

9 Yampolskiy M, Horvath P, Koutsoukos XD, *et al*. Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. Proceedings of 2012 5th International Symposium on Resilient Control Systems. Salt Lake City, UT, USA. 2012. 55–62.

10 Davis KR, Davis CM, Zonouz SA, *et al*. A cyber-physical modeling and assessment framework for power grid infrastructures. IEEE Transactions on Smart Grid, 2015, 6(5): 2464–2475.

11 Shostack A. Threat Modeling: Designing for Security. New York, USA: John Wiley & Sons, 2014.

12 Ou XM, Boyer WF, Mcqueen MA. A scalable approach to attack graph generation. Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, VA, USA. 2006. 336–345. [doi: 10.1145/1180405.1180446]

13 Manandhar K, Cao XJ, Hu F, *et al*. Combating false data injection attacks in smart grid using Kalman filter. Proceedings of 2014 International Conference on Computing, Networking and Communications. Honolulu, HI, USA. 2014. 16–20.

14 Manandhar K, Cao XJ, Hu F, *et al*. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Transactions on Control of Network Systems, 2014, 1(4): 370–379.

15 Komninos N, Philippou E, Pitsillides A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 2014, 16(4): 1933–1954.