基于攻击图的工控系统脆弱性量化方法

黄家辉 [1]　冯冬芹 [1]　王虹鉴 [1]

摘　要　提出了一种基于攻击图的工控系统脆弱性量化研究方法. 从工控系统中存在的漏洞利用难度和漏洞危害性两个维度出发, 同时结合具体的工业系统中有关防御强度、攻击强度、物理损失、信息损失等方面, 提出了一系列的脆弱性量化指标, 制定了比较全面的等级划分标准. 之后将量化指标与攻击图相结合, 利用攻击过程中每一步的原子攻击期望来对可能存在的所有攻击路径进行脆弱性分析. 最后以典型的锅炉控制系统作为实验背景进行了案例分析. 实验结果表明, 该方法能够较全面地分析工控系统中潜在的隐患威胁, 科学合理地评估各条攻击路径的脆弱性, 由此得到总攻击期望最大的攻击路径.

关键词　工控系统, 脆弱性, 漏洞利用难度, 漏洞危害性, 等级划分标准

引用格式　黄家辉, 冯冬芹, 王虹鉴. 基于攻击图的工控系统脆弱性量化方法. 自动化学报, 2016, **42**(5): 792−798

DOI　10.16383/j.aas.2016.c150517

A Method for Quantifying Vulnerability of Industrial Control System Based on Attack Graph

HUANG Jia-Hui[1]　FENG Dong-Qin[1]　WANG Hong-Jian[1]

Abstract　A method for quantifying the vulnerability of industrial control system based on attack graph is proposed. First, the two dimensions of vulnerability existing in industrial control systems are analyzed, which are exploitation difficulty of vulnerability and vulnerability hazard. Some quantitative indexes of vulnerability are proposed by combining these dimensions with some concrete industrial aspects, such as defense strength, attack strength, physical loss, and information loss. Then, a specific grade division standard is formulated. By means of attack graph, the vulnerability of each attack path in industrial control system can be obtained by calculating each atomic attack expectation. Finally, a case of boiler control system is analyzed and simulated to verify the rationality of this method. Experimental results show that this method can analyze the potential threats in industrial control systems more comprehensively and evaluate the vulnerability of each attack path more reasonably. The attack path that has the largest attack expectation can be obtained through simulation.

Key words　Industrial control system, vulnerability, exploitation difficulty of vulnerability, vulnerability hazard, grade division standard

Citation　Huang Jia-Hui, Feng Dong-Qin, Wang Hong-Jian. A method for quantifying vulnerability of industrial control system based on attack graph. *Acta Automatica Sinica*, 2016, **42**(5): 792−798

收稿日期 2015-08-13　录用日期 2015-11-26
Manuscript received August 13, 2015; accepted November 26, 2015
国家自然科学基金 (61223004), 工控网络安全研究 (2015XZZX005-03) 资助
Supported by National Natural Science Foundation of China (61223004) and Research on the Security of Industrial Control Network (2015XZZX005-03)
本文责任编委 胡昌华
Recommended by Associate Editor HU Chang-Hua
1. 浙江大学智能系统与控制研究所工业控制技术国家重点实验室 杭州 310027
1. State Key Laboratory of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou 310027

随着工业技术的发展和工控系统应用的普及, 工业生产控制正逐步改变着社会生产方式. 工控系统的普及必然带来更高标准的工业安全需求[1], 而对工控系统进行科学合理的脆弱性评估是工控系统安全运行的重要前提保障. 近年来相继出现的毒区病毒、火焰病毒[2] 和震网事件[3] 等, 充分暴露了工控系统安全性差的缺点, 对其进行安全评估已经成为国际性难题. 工控系统一般划分为三层架构: 计划管理层、制造执行层和工业控制层, 图 1 显示了一个简单的工控系统图.

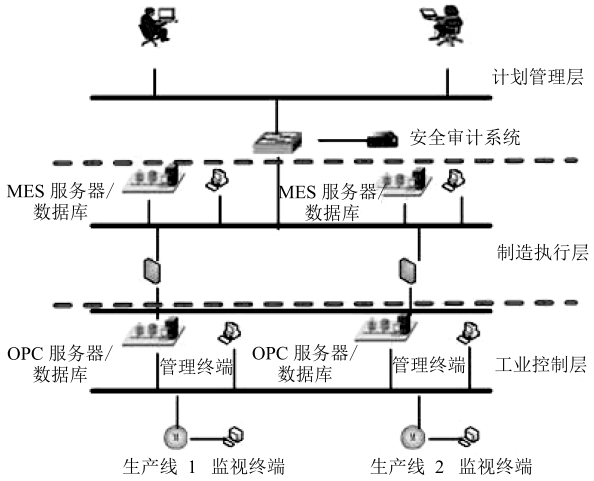

图 1　工控系统图

Fig. 1　Industrial control system

计划管理层主要用于底层信息的汇总和分析, 其与制造执行层之间主要进行的安全防护包括身份鉴别、访问控制、检测审计、链路冗余和内容检测等; 制造执行层主要包括 MES (Manufacturing execution system) 服务器或 MES 数据库等, 其与工业控制层之间的防护主要是避免管理层直接对工控层的访问, 保证制造执行层对工业控制层的操作唯一性; 工业控制层主要由 OPC (OLE for process control) 服务器、管理终端、PLC (Programmable logic controller)、监控终端等组成.

目前国内外针对工控系统安全的脆弱性评估研究还处于起步阶段, 由于工业系统具有复杂度高、灵活性差等特点, 使得目前仍然缺少一种成熟的工控系统安全评估方法. 从数学建模的角度, 刘芳[4] 提出了一种 ISSUE (Information system security evaluation) 安全评估方法, 并结合安全风险概率预测技术, 基于模糊多属性群体决策, 将模糊数学、多属性决策和群体决策的理论运用在安全评估中. 但该方法需要大量的历史数据作为理论支撑, 且评估结果存在不合理的情况; 周小锋等[5] 提出针对 ICS (Industrial control system) 安全指标的分层计算模型, 使用灰色数学模糊聚类方法, 增加了评估准确性. 但是模糊聚类方法在样本量比较大时, 得到聚类结果有一定困难; 从网络模型的角度, Vintr 等[6] 基于攻击树模型来评估防护系统的脆弱性, 分析了工控系统的网络攻击空间, 使用 FTA (Fault tree analysis) 和 ATA (Accident tree analysis) 来识别潜在的攻击场景, 但该方法不能独立用于识别全部攻击目标; Jha 等[7] 对工控系统进行攻击图建模, 为每个原子攻击指派成功发生的概率, 利用马尔科夫模型计算攻击者达到攻击目标的可能性. 但这个概率值容易受到人

为因素的干扰, 且该方式实现起来较复杂, 使得评估结果缺乏科学性和合理性. 从脆弱性指标的评价方法的角度, Sener 等[8] 采用层次分析法来进行地下水系统的脆弱性评估, 但该方法的缺点就是评估指标过多时权重无法确定, 并且使用特征值和特征向量的计算相对复杂; Stewart 等[9] 采用主成分分析法对多个脆弱性指标进行综合决策, 但需要大量样本的支持; 从国际标准的角度, 美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST)[10] 发布了一系列指南, 重点研究带有复杂网络类型的大型控制系统的深度防御架构及配置方法, 包括 SP800-82、NIST 7176 等. 美国国家标准学会 (American National Standards Institute, ANSI) 制定了 ISA99 标准[11], 从工业自动化控制系统的安全要求、编程要求、系统级技术要求和组件级技术要求四方面进行安全评估. 但这些标准和指南只是提出了一些理论性的概念和知识, 缺乏实际的现场可操作性.

结合工控系统的特征和上述脆弱性研究方法的不足, 本文提出了一种基于攻击图的工控系统脆弱性量化评估方法. 首先, 提出了两个量化评估指标: 漏洞利用难度和漏洞危害性, 结合实际工控系统的安全属性, 如防御强度、攻击强度、物理损失、信息损失等, 制定出一套比较全面的工控系统脆弱性量化指标等级划分标准. 其次, 利用攻击图来对工控系统的拓扑结构进行建模分析, 以研究每条攻击路径的脆弱性为目标, 计算攻击过程中每一步的原子攻击期望 (该值与漏洞利用难度和漏洞危害性相关) , 从而得到每条路径的总攻击期望. 最后, 以锅炉控制系统作为实验对象进行仿真来验证该方法的可行性. 相比于刘芳[4] 的评估方法, 本方法更贴近实际的工业环境, 将工艺方面考虑进去, 而不是只分析信息安全; 相比于周小锋等[5] 的模糊聚类, 本方法对原始数据的依赖性低, 且无需大量样本数据的支撑; 相比于国内外标准[10−11], 本方法具有一定的可操作性; 相比于 Jha 等[7] 的方法, 本方法与脆弱性标准相结合, 因此得到的结果更加科学合理.

1　脆弱性评估指标

为了对工控系统的脆弱性进行全面的量化评估, 本文提出两个脆弱性量化指标: 漏洞利用难度和漏洞危害性, 并进行以下定义.

定义 1. 攻击期望 ($Att_{\exp}$): 漏洞利用难度 ($Vul_{\exp}$) 和漏洞危害性 (Vul_{haz}) 的乘积, 记为

$$Att_{\exp} = Vul_{\exp} \times Vul_{\mathrm{haz}} \tag{1}$$

基于此, 对不同攻击路径的攻击期望损失进行综合评价, 并用最大的期望损失作为衡量整个工控系统的脆弱性参考指标.

1.1　漏洞利用难度

漏洞利用难度 $Vul_{\exp}$ 指利用某一漏洞来实现一次成功攻击的可能性. 该指标不仅与防御强度有关, 也与攻击强度相关. 防御越弱, 攻击越强, 则漏洞被利用的难度越小. 基于工控系统的层次性特点以及其中组件的特点, 防御强度主要包括加密、认证、信息屏障、物理屏障, 攻击强度主要包括攻击者数量、攻击者的知识水平和威胁频率.

1.1.1　防御强度

1) 加密: 工控系统中传输数据的方式主要有明文传输和密文传输, 其中密文传输又包括 AES (Advanced encryption standard) 加密[12] 和 DES (Data encryption standard) 加密. 加密的强度主要可以由密钥长度、破解难度和加减密时间来确定.

2) 认证: 工控系统中的组件需要经过认证来鉴别数据的安全性, 主要包括数字摘要、数字签名、数字信封和数字证书四种认证方式, 若在某个组件中部署的认证方式越多, 则其越安全. 其中数字信封由于采用双重加密技术来保证只有规定的接受者才能阅读数据, 其安全性最高.

3) 信息屏障: 主要的防护技术包括防火墙、入侵检测技术和访问控制. 其中防火墙又可根据防御能力分为工业防火墙和商业防火墙; 入侵检测技术[13] 的关键是如何从已知的数据中获得系统的正常行为或有关入侵行为的知识, 可以分成模式匹配、神经网络、数据挖掘和数据融合; 访问控制[14] 根据管理性质和安全级别又可分为基于授权规则的自主管理访问控制 (Discretionary access control, DAC)、基于安全级的集中管理强制访问控制 (Mandatory access control, MAC) 和基于授权规则的集中管理角色访问控制 (Role-based access control, RBAC).

4) 物理屏障: 主要指采取的物理防御手段, 包括对外接口数量、组件所处位置、防静电、防火、防雷等.

1.1.2　攻击强度

1) 攻击者数量: 对某一漏洞利用的人越多, 则脆弱性越高. 本文参考 NIST 7176 标准, 将攻击者数量分为三个等级: 小于 100、100～300 和大于 300.

2) 攻击者知识水平: 经验丰富的攻击者显然比首次参与攻击的初学者具有更高的攻击成功概率, 据此将知识水平按表 1 进行分级.

表 1　攻击者知识水平

Table 1　Knowledge of attackers

标识	定义
低	攻击者对工控系统的运行方式、安全策略和网络拓扑不太熟悉
中	攻击者对工控系统的运行方式、安全策略和网络拓扑比较熟悉
高	攻击者对工控系统的运行方式、安全策略和网络拓扑非常熟悉

3) 威胁频率: 参考《集散控制系统安全评估指南》中对威胁频率的赋值, 如表 2 所示.

表 2　威胁分级

Table 2　Classification of threats

标识	定义
低	威胁几乎不可能发生
中	出现的频率中等 (或 $\geq$ 1 次/半年)
高	出现的频率较高 (或 $\geq$ 1 次/月)
很高	出现的频率很高 (或 $\geq$ 1 次/周)

1.2　漏洞危害性

漏洞危害性 Vul_{haz} 指攻击者利用漏洞对工控系统造成的损失, 包括物理损失和信息损失两方面. 物理损失与组件相关, 组件在整个工控系统中所占的比例或者重要度越大, 则可能的物理损失越高; 信息损失参考 CVSS (Common vulnerability scoring system) 标准[15], 从信息机密性、信息完整性和信息可用性来衡量一个漏洞的危害性.

1.2.1 物理损失

工控系统中每个组件根据其扮演的角色不同, 具有不同的价值量. 例如, 一台数据库服务器具有的价值量要比一般的主机具有的价值量高, 因为一旦数据库服务器被攻击者控制, 许多重要信息将会被泄露、修改或删除. 在工控系统中根据组件所处的位置分为上位机和下位机, 其中上位机包括用户机、SCADA (Supervisory control and data acquisition) 服务器、工程师站、操作员站、WWW (World wide web) 服务站、MES 服务器/数据库和 OPC 服务器/数据库; 下位机分为远程终端单元 RTU (Remote terminal unit)、可编程逻辑控制器 PLC 和可编程自动化控制器 PAC (Programmable automation controller). 各个组件价值量的分级参考《集散控制系统安全评估指南》, 如表 3 所示.

表 3 组件价值量分级

Table 3 Classification of component value

标识	定义
小	如果被利用, 对工控系统产生较小影响
中	如果被利用, 对工控系统产生一般影响
大	如果被利用, 对工控系统产生严重影响

1.2.2 信息损失

工控系统组件之间传输的数据或指令的正确性对于整个系统的正常运行起着十分重要的作用, 因此利用漏洞来对这些重要信息进行攻击便成为攻击者的一大目标. 信息的损失主要体现在机密性、完整性和可用性上.

1) 机密性: 要求信息免受非授权的披露, 不被泄露和窃取, 涉及到对数据和程序文件读取的控制;

2) 完整性: 要求信息必须是正确和完全的, 而且能够免受非授权、意料之外或无意的更改, 还要求程序的更改要在特定或授权状态下进行;

3) 可用性: 要求信息在需要时能够及时获得以满足需求, 确保用户不受干扰的获得相关系统信息和资源.

漏洞被利用后对信息的三种属性的影响分级, 如表 4 所示.

1.3 等级划分标准打分

综合漏洞利用难度和漏洞危害性中对各个因素的分级, 参考国内外脆弱性标准来对所有因素进行赋值打分, 如表 5 和表 6 所示 (假定各影响因素都采用一种等级).

表 4 三种属性影响分级

Table 4 Classification of three properties

标识	定义
小	漏洞被利用后最多一种属性被破坏
中	漏洞被利用后两种属性被破坏
大	漏洞被利用全部属性都被破坏

2 多指标归一与攻击图生成

2.1 灰色关联度分析法

对某对象进行评价时, 如果仅从单一指标的角度, 评价结果存在片面性, 因此往往需要将反映被评价对象的多项指标加以汇聚, 得到一个综合指标来从整体上反映被评价对象的整体情况, 即多指标综合评价方法.

目前存在的综合评价方法包括层次分析法、主成分分析法、TOPSIS (Technique for order preference by similarity to ideal solution) 法[16] 和灰色关联度分析法[17] 等. 其中灰色关联度分析法具有计算简单、数据不必进行归一化、无需大量样本和无需经典的分布规律等特点, 因此本文采用该方法来对多指标进行综合评价.

灰色关联度分析法的基本原理为: 从样本中确定一个理想化的最优样本, 以此为参考数列, 通过计算各样本序列与参

表 5 漏洞利用难度打分

Table 5 Scoring of $Vul_{\exp}$

影响因素	等价细分	打分	说明
加密	无/DES/AES	1/2/3	AES 密钥更长且破解更困难, 因此安全性最高
认证	数字摘要/数字证书/数字签名/数字信封	1/2/3/4	数字签名采用双重加密技术, 安全性最高; 数字摘要实现最简单, 安全性最低
防火墙	商业防火墙/工业防火墙	1/2	工业防火墙设置的过滤规则更多更复杂, 故安全性更高
入侵检测技术	模式匹配/神经网络/数据挖掘/数据融合	1/2/3/4	模式匹配只能检测已知攻击, 而数据融合不仅可以检测已知攻击, 还可以预估未知攻击
访问控制	DAC/MAC/RBAC	1/2/3	RBAC 在灵活性和控制细节上更有优势
对外接口数量	≥ 5 个/< 5 个	1/2	接口数量越多, 为攻击者提供的攻击入口就越多
防静电、防火、防雷	最多采用一种/采用两种/采用三种	1/2/3	采用的物理防护措施越多, 攻击者越难进行攻击
攻击者数量	$> 300/100 \sim 300/ < 100$	1/2/3	攻击者数量越多, 系统安全性越低
攻击者知识水平	高/中/低	1/2/3	见表 1
威胁频率	很高/高/中/低	1/2/3/4	见表 2

表 6　漏洞危害性打分

Table 6　Scoring of Vul_{haz}

影响因素	等价细分	打分	说明
SCADA 服务器	大	3	使整个控制系统和管理者的台式机能随时使用来自 SCADA 远程终端的重要信息
工程师站	中	2	既安装 STEP 7 编程组态软件, 又安装 Win CC 监控操作组态软件
操作员站	小	1	仅需安装 Win CC 监控操作组态软件
用户机	小	1	存放传输给管理层的数据
WEB 服务站	小	1	提供 WEB 服务的功能, 在某些工控系统中不是必需的
MES 服务器/数据库	大	3	存放制造执行层的重要数据
OPC 服务器/数据库	大	3	存放下位机采集的原始现场数据和上位机传来的指令
RTU	大	3	主要进行数据采集和本地控制, 与传输可靠性、主机负担等相关
PLC	大	3	主要进行过程控制、信息控制和远程控制, 是重要的下位机
PAC	小	1	作为开放型的自动化控制设备, 其应用在工控系统中并不常见
信息属性	小/中/大	1/2/3	见表 4

考序列的关联度, 对被评价对象做出综合比较和排序.

设有 n 个被评价对象, 每个被评价对象有 p 个评价指标, 则第 i 个对象描述为

$$x_i = (x_{i1}, x_{i2}, \cdots, x_{ip})$$

具体步骤如下:

1) 确定参考序列. 在 n 个被评价对象中选出各项指标的最优值组成参考序列 x_0

$$x_0 = (x_{01}, x_{02}, \cdots, x_{0p})$$

2) 计算两极最大差 $\triangle_{\max}$ 和最小差 $\triangle_{\min}$. 计算被评价对象序列与最优参考序列间的绝对差列 $\triangle_{ij}$

$$\triangle_{ij} = |x_{ij} - x_{0j}|, \quad i = 1, 2, \cdots, n, \ \ j = 1, 2, \cdots, p \tag{2}$$

在此基础上, 根据

$$\triangle_{\max} = \max_{1\le i\le n} \max_{1\le j\le p} (\triangle_{ij}) \tag{3}$$

$$\triangle_{\min} = \min_{1\le i\le n} \min_{1\le j\le p} (\triangle_{ij}) \tag{4}$$

3) 计算关联系数. 计算第 i 个评价对象的第 j 个指标与最优参考序列间的关联系数 δ_{ij}

$$\delta_{ij} = \frac{\triangle_{\min} + \rho\triangle_{\max}}{\triangle_{ij} + \rho\triangle_{\max}} \tag{5}$$

其中, ρ 为分辨系数, 用以削弱 $\triangle_{\max}$ 过大而使关联系数失真的影响.

4) 计算关联度. 各评价对象与参考序列间的关联关系用关联度 Υ_{0i} 表示

$$\Upsilon_{0i} = \frac{1}{p}\sum_{k=1}^{p} \delta_{ij}, \quad i = 1, 2, \cdots, n \tag{6}$$

若各指标权重不同, 则式 (6) 表示为

$$\Upsilon_{0i} = \frac{1}{p}\sum_{k=1}^{p} W_k \times \delta_{ij}, \quad i = 1, 2, \cdots, n \tag{7}$$

其中, W_k 为权重, $W_k \in (0, 1)$.

关联系数和关联度能够把影响工控系统脆弱性的各个指标进行多属性决策, 采用一个综合量化值来替代多个指标量化值, 使得量化结果没有片面性, 同时能够从整体上反映脆弱性的大小, 关联度越大, 则对应的系统脆弱性也越大.

2.2　攻击图生成算法

攻击图作为一种描述攻击者从攻击起点到攻击目标的所有可视化路径的方法, 已经成为分析系统脆弱性的主流评估模型. 攻击图 G 可以表示为 $G = \langle V, E\rangle$, 其中 V 为图中节点的集合, E 为节点之间链路的集合. 透过攻击图可以很明确的得到从某一节点到目标节点的所有潜在攻击路径.

本文采用广度优先算法[18] 来生成攻击图, 并将该算法与量化指标相结合, 生成攻击图的同时计算每一步的原子攻击期望. 广度优先算法一般用于求解最优值的问题, 而且相比于深度优先算法, 它可以控制队列的长度, 不容易产生堆栈溢出等问题. 算法基本步骤为:

步骤 1. 根据工控系统的拓扑和组件相关信息建立参数向量;

步骤 2. 确定工控系统的初始状态, 加入状态队列;

步骤 3. 执行循环: 当状态队列不为空, 则从队列中取出一个节点作为当前节点, 并生成该节点可能进行的所有状态转移, 得到新的状态节点, 如果该节点为新, 则加入队列, 并计算实现状态转移时的攻击期望, 更新攻击图节点和边的信息;

步骤 4. 重复执行步骤 3, 直到队列为空.

在生成攻击图前, 需要收集系统的拓扑信息以及其中组件的相关脆弱性信息, 以此作为该算法的输入, 输出为潜在的攻击路径和每条攻击路径的原子攻击期望.

3　案例分析

以真实的锅炉控制系统[19] 作为实验背景, 参考锅炉工艺流程和 SCADA 系统的一般架构, 模拟攻击者通过外网攻击用户并逐步入侵工控系统的过程. 实验拓扑如图 2.

由图 2 可知, 该系统一共包含 6 个组件, 每个组件上的漏洞信息如表 7 所示.

3.1　漏洞利用难度量化

参考表 5, 对各个漏洞的利用难度进行具体的赋值打分, 结果如表 8 所示.

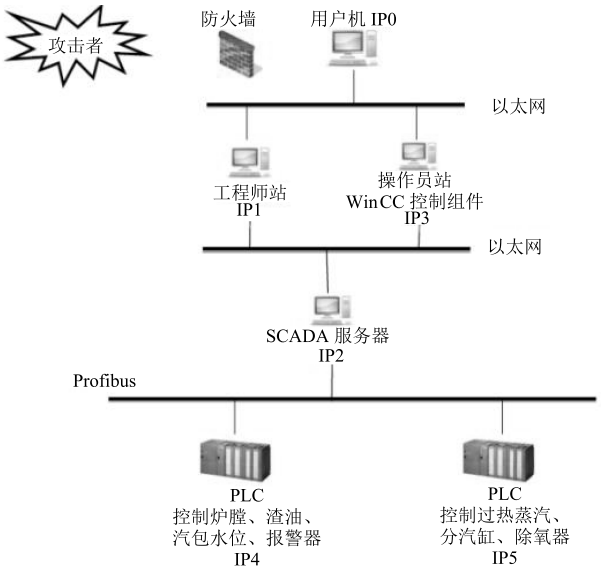

图 2 实验拓扑图

Fig. 2 Topology of experiment

表 7 组件漏洞信息

Table 7 Information of component vulnerability

编号	组件	漏洞
IP0	用户机	CVE-1999-0917
IP1	工程师站	CVE-2013-5056
IP2	SCADA 服务器	CVE-2013-3175
IP3	操作员站	CVE-2013-3957
IP4	某品牌 PLC	CVE-2013-0659
IP5	某品牌 PLC	CVE-2013-0675

之后根据灰色关联度分析法对上述指标进行综合评价, 其中 n 为 6, p 为 10. 参考序列 x_0 为

$$x_0 = (3, 4, 2, 4, 3, 2, 3, 2, 3, 4)$$

最大差 $\triangle_{\max}$ 和最小差 $\triangle_{\min}$ 分别为

$$\triangle_{\max} = 3$$

$$\triangle_{\min} = 0$$

根据式 (5) , 并取 $\rho = 0.5$, 则漏洞 CVE-1999-0917 加密的关联系数为 $\delta_{1j} = 0.6$.

同理可以得到其他漏洞的关联系数. 根据各个指标的不同取不同的权重系数, 表 8 中的各个指标依次对应权重为 (0.2, 0.05, 0.1, 0.05, 0.15, 0.2, 0.05, 0.05, 0.05, 0.1). 之后根据式 (7) 可以求得各个漏洞的利用难度关联度, 如表 9 所示.

表 9 各个漏洞的利用难度关联度

Table 9 Degree of $Vul_{\exp}$ for various vulnerabilities

编号	1	2	3	4	5	6
Υ	0.053	0.052	0.041	0.046	0.043	0.039

3.2 漏洞危害性量化

参考表 6, 对漏洞危害的因素进行赋值打分, 如表 10 所示.

表 10 漏洞危害性量化值

Table 10 Values of Vul_{haz}

漏洞	物理损失	信息损失
CVE-1999-0917	1	1
CVE-2013-5056	2	2
CVE-2013-3175	3	3
CVE-2013-3957	1	2
CVE-2013-0659	3	2
CVE-2013-0675	3	3

同样采用灰色关联度分析法, 取对应权重分别为 0.7 和 0.3, 可以得到漏洞危害性的关联度, 如表 11 所示.

表 11 漏洞危害性关联度

Table 11 Degree of Vul_{haz} for various vulnerabilities

编号	1	2	3	4	5	6
Υ	0.25	0.165	0.125	0.225	0.137	0.125

3.3 攻击图生成

在计算得到漏洞利用难度和漏洞危害性的量化值后, 根据式 (1) 可以计算每个漏洞的攻击期望, 如表 12 所示.

表 12 漏洞攻击期望

Table 12 $Att_{\exp}$ for various vulnerabilities

编号	1	2	3	4	5	6
$Att_{\exp}$	0.013	0.009	0.005	0.010	0.006	0.005

表 8 漏洞利用难度量化值

Table 8 Values of $Vul_{\exp}$

编号	漏洞	加密	认证	防火墙	入侵检测	访问控制	接口数量	防静电、雷、火	攻击者数量	知识水平	威胁频率
1	CVE-1999-0917	1	2	1	1	2	2	1	1	1	1
2	CVE-2013-5056	1	3	2	3	2	1	2	1	1	1
3	CVE-2013-3175	3	4	2	4	3	1	3	2	2	2
4	CVE-2013-3957	1	3	2	4	3	2	2	1	2	1
5	CVE-2013-0659	2	2	2	3	3	1	2	2	3	3
6	CVE-2013-0675	2	3	2	2	2	2	3	2	3	4

之后结合图 2 的拓扑结构和攻击图生成算法, 采用 Graphviz 软件对攻击图进行输出, 如图 3 所示.

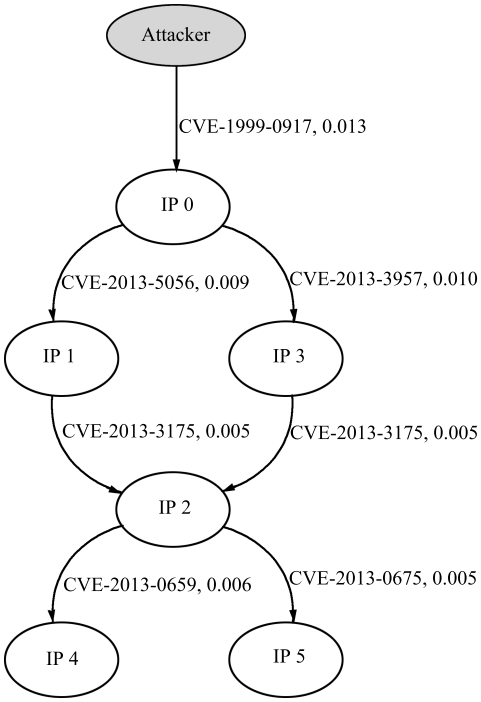

图 3　攻击图

Fig. 3　Attack graph

图 3 中, 深色椭圆表示攻击者, 椭圆内的数字表示漏洞编号, 边上的信息包括可利用的漏洞以及对应的漏洞攻击期望. 由此可以计算出每条攻击路径的总攻击期望, 定义为攻击路径上各个漏洞攻击期望之和, 结果如表 13 所示.

表 13　各条路径的总攻击期望

Table 13　$Att_{\exp}$ for various paths

序号	路径	总攻击期望
1	IP0 → IP1 → IP2 → IP4	0.033
2	IP0 → IP1 → IP2 → IP5	0.032
3	IP0 → IP3 → IP2 → IP4	0.034
4	IP0 → IP3 → IP2 → IP5	0.033

由表 13 可知, 同处于下位机的 PLC (IP4) 比 IP5 的重要性更高, 攻击 IP4 能获得更大的收益, 虽然 IP4 的利用难度大于 IP5, 但其被利用后的危害性更大, 这也证明单凭一个指标不能对各个组件的脆弱性进行比较, 否则得到的结果正确性不高; 操作员站和工程师站的重要性不同, 在本案例中操作员站 IP3 比工程师站 IP1 重要, 主要的影响因素是利用的危害性 (利用难度相差不多); 此外漏洞 CVE-1999-0917 的利用价值最大, 为 0.013, 漏洞 CVE-2013-0675 和 CVE-2013-3175 的利用价值最小, 为 0.005, 这表明越上层的组件越重要, 因为底层的组件被利用后仅仅这一个组件被控制, 造成的损失可能是一台 PLC 的爆炸或崩溃, 但若上层的组件被控制, 再加上工控系统的组件采用分布控制、集中管理, 则可以通过一台上位机向多个底层组件发送错误指令或数据, 导致大量的组件爆炸或崩溃, 造成的危害更大.

4　总结

工控系统的安全问题正受到越来越多人的关注, 对其进行安全评估刻不容缓. 本文在系统地研究工控系统存在的各类脆弱性后, 提出了漏洞利用难度和漏洞危害性两个量化评估指标. 根据实际工控系统中的工艺流程, 结合攻防强度、物理损失和信息损失等方面制定出一套较全面的漏洞等级划分标准, 使该标准更贴近工业环境. 同时, 根据广度优先算法生成攻击图来对工控系统进行建模, 最后以实际的锅炉控制系统为背景进行了实验模拟和仿真分析, 得到了总攻击期望最大的路径. 实验结果表明, 该方法综合了工控系统中潜在的安全威胁, 考虑了影响脆弱性的各个方面, 由此得到的评估结果更加科学合理.

References

1 Garcia J, Palomo F R, Luque A, Aracil C, Quero J M, Carrion D, Gamiz F, Revilla P, Perez-Tinao J, Moreno M, Robles P, Franquelo L G. Reconfigurable distributed network control system for industrial plant automation. *IEEE Transactions on Industrial Electronics*, 2004, **51**(6): 1168−1180

2 Munro K. Deconstructing flame: the limitations of traditional defences. *Computer Fraud and Security*, 2012, **2012**(10): 8−11

3 Langner R. Stuxnet: dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, 2011, **9**(3): 49−51

4 Liu Fang. Research on the Theories and Key Technologies of Information System Security Evaluation [Ph. D. dissertation], National University of Defense Technology, China, 2005.
(刘芳. 信息系统安全评估理论及其关键技术研究 [博士学位论文], 国防科技大学, 中国, 2005.)

5 Zhou Xiao-Feng, Chen Xiu-Zhen. Gray analytical hierarchical assessment model for industry control system security. *Netinfo Security*, 2014, (1): 15−20
(周小锋, 陈秀真. 面向工业控制系统的灰色层次信息安全评估模型. 信息网络安全, 2014, (1): 15−20)

6 Vintr Z, Valis D, Malach J. Attack tree-based evaluation of physical protection systems vulnerability. In: Proceedings of the 2012 IEEE International Carnahan Conference on IEEE Security Technology (ICCST). Boston, MA: IEEE, 2012. 59−65

7 Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs. In: Proceedings of the 15th IEEE Computer Security Foundations Workshop. Cape, Breton, NS, Canada: IEEE, 2002. 49−63

8 Sener E, Davraz A. Assessment of groundwater vulnerability based on a modified DRASTIC model, GIS and an analytic hierarchy process (AHP) method: the case of Egirdir Lake basin (Isparta, Turkey). *Hydrogeology Journal*, 2013, **21**(3): 701−714

9 Stewart S, Ivy M A, Anslyn E V. The use of principal component analysis and discriminant analysis in differential sensing routines. *Chemical Society Reviews*, 2014, **43**(1): 70−84

10 Scace G E, Miller W W. Reducing the uncertainty of industrial trace humidity generators through NIST permeation-tube calibration. *International Journal of Thermophysics*, 2008, **29**(29): 1544−1554

11 Byres E, Eng P, Fellow I S A. Using ANSI/ISA-99 Standards to Improve Control System Security. White paper, Tofino Security, 2012.

12 Talha S K, Barry B I A. Evaluating the impact of AES encryption algorithm on voice over internet protocol (VoIP) systems. In: Proceedings of the 2013 International Conference on Computing, Electrical and Electronics Engineering (ICCEEE). Khartoum: IEEE, 2013. 686−691

13 Shakshuki E M, Kang N, Sheltami T R. EAACK — a secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics*, 2013, **60**(3): 1089−1098

14 Hur J, Noh D K. Attribute-based access control with efficient revocation in data outsourcing systems. *IEEE Transactions on Parallel and Distributed Systems*, 2011, **22**(7): 1214−1221

15 Scarfone K, Mell P. An analysis of CVSS version 2 vulnerability scoring. In: Proceedings of the 3rd IEEE International Symposium on Empirical Software Engineering and Measurement. Lake Buena Vista, FL: IEEE, 2009. 516−525

16 Opricovic S, Tzeng G H. Compromise solution by MCDM methods: a comparative analysis of VIKOR and TOPSIS. *European Journal of Operational Research*, 2004, **156**(2): 445−455

17 Zhou Tao, Hu Hai-Ning, Zhou Li-Xing. Transformer fault diagnosis method based on factor analysis and grey relation degree analysis. *Journal of Electric Power Science and Technology*, 2013, **28**(1): 86−91
(周涛, 胡海宁, 周力行. 基于因子分析和灰色关联度分析法的变压器故障诊断. 电力科学与技术学报, 2013, **28**(1): 86−91)

18 Beamer S, Asanović K, Patterson D. Direction-optimizing breadth-first search. *Scientific Programming*, 2013, **21**(3−4): 137−148

19 Morilla F. Benchmark for PID control based on the boiler control problem. *Advances in Pid Control*, 2011, **2**(1): 346−351

黄家辉 浙江大学智能系统与控制研究所硕士研究生. 主要研究方向为工控系统脆弱性评估. E-mail: elninohjh@163.com
(**HUANG Jia-Hui** Master student at the Institute of Cyber-Systems and Control, Zhejiang University. His research interest covers vulnerability assessment of industrial control system.)

冯冬芹 浙江大学智能系统与控制研究所教授. 主要研究方向为现场总线, 实时以太网, 工业无线通信技术, 工业控制系统安全以及网络控制系统的研发与标准化工作. 本文通信作者.
E-mail: dqfeng@iipc.zju.edu.cn
(**FENG Dong-Qin** Professor at the Institute of Cyber-Systems and Control, Zhejiang University. His research interest covers field bus, real-time ethernet, industrial wireless communication technology, security of industrial control system, and network control system. Corresponding author of this paper.)

王虹鉴 浙江大学智能系统与控制研究所硕士研究生. 主要研究方向为半监督过程建模. E-mail: endless_whj@163.com
(**WANG Hong-Jian** Master student at the Institute of Cyber-Systems and Control, Zhejiang University. His research interest covers semi-supervised process modeling.)