

机密稳健复杂系统安全性评估方法

左金鑫^{1,2}, 郭子裕^{1,2}, 李瑾^{1,2}, 张洁³, 陆月明^{1,2}

(1. 北京邮电大学, 北京 100876;
2. 可信分布计算与服务教育部重点实验室, 北京 100876;
3. 军事科学院系统工程院, 北京 100091)

摘要: 机密稳健复杂系统具有高机密性要求、持续稳定运行需求、网络结构复杂等特点, 但现有评估模型安全目标维度单一, 缺乏指标间关联性分析。鉴于此, 提出了基于指标关联性分析的综合安全评估模型, 确立涵盖产品、系统和服务 3 个层面的机密性、可用性、可控性、可鉴别性、人员组织、风险管理、企业定级、可持续性 8 个安全目标。以智慧医疗物联网机密性为例, 构建了基于指标关联性的排序确权算法, 采用模糊综合评价法, 对所选系统进行评估。

关键词: 机密稳健复杂系统; 信息安全评估; 排序算法; 模糊综合评价法

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019017

Security evaluation method for confidential and stable complex systems

ZUO Jinxin^{1,2}, GUO Ziyu^{1,2}, LI Jin^{1,2}, ZHANG Jie³, LU Yue ming^{1,2}

1. Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing 100876, China
3. Institute of Systems Engineering, Academies of Military Science, Beijing 100091, China

Abstract: Confidential and stable complex systems are characterized by high confidentiality requirements, continuous and stable operation requirements, and complex network structure, but existing evaluation models has a single dimension of security objectives and lack the correlation analysis among indicators. In view of this, a comprehensive security evaluation model based on the correlation analysis of indicators is proposed and eight security objectives covering confidentiality, availability, controllability, identifiability, personnel organization, risk management, enterprise grading and sustainability at three levels of product, system and service have been established. Taking the confidentiality of the smart medical IoT as an example, a sorting and weight confirmation

收稿日期: 2018-11-25; 修回日期: 2018-12-20

通信作者: 左金鑫, zuojx@bupt.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2016YFF0204001)

Foundation Item: The National Key Research and Development Program (No.2016YFF0204001)

论文引用格式: 左金鑫, 郭子裕, 张洁, 等. 机密稳健复杂系统安全性评估方法[J]. 网络与信息安全学报, 2019, 5(2): 58-65.
ZUO J X, GUO Z Y, ZHANG J, et al. Security evaluation method for confidential and stable complex systems[J]. Chinese Journal of Network and Information Security, 2019, 5(2): 58-65.

algorithm based on index correlation is constructed, and the fuzzy comprehensive evaluation method is used to evaluate the selected system.

Key words: confidential and stable complex system, information security evaluation, sort algorithm, fuzzy comprehensive evaluation method

1 引言

物联网等各类服务系统机密性、稳健性的需求逐渐提升,如智能电网、智慧医疗物联网应用领域逐渐普及,针对机密稳健复杂系统(CSCS, confidential and stable complex system)的系统安全评估需求也日益凸显。然而,当前 CSCS 领域缺乏宏观的安全评估框架指导,要解决对 CSCS 的安全等级评估问题,首先需要建立统一的安全度量模型,随后确定合理的安全目标及评估方案,根据评估结果提高和改善系统安全质量。

2 现有机密稳健复杂系统存在的问题

机密稳健复杂系统是指具有信息不被泄露给非授权的用户、实体或过程的特性,以及可以在规定时间和条件下完成预定功能,并持续稳定运行,构成较为复杂的物联网类系统,如智能电网系统、银行系统、智慧医疗系统等。

针对不同的具体系统,当前科研领域做了相应具体化研究。对于银行系统,Grunbauer 等^[1]使用 AUTOFOCUS 工具改进安全标准系统,提出了一种安全可靠的信息系统安全管理与评估方法,并将其应用到德国银行的安全评估中进行实例验证,取得了理想的效果。对于智能电网,CIGRE Task Force^[2]提出了电网运行风险的正式定义,业界普遍认为基于风险进行电网运行控制在很多方面优于确定性的控制,因此成为学术界和工程界努力追逐的目标。Xiao 等^[3]提出了基于风险的多目标优化模型用于协调实时运行阶段的安全性及经济性。针对物联网的分层评价系统,Yang 等^[4]分析了物联网不同层面(感知层、传输

层、应用层)存在的安全问题,仅考虑到技术层面的攻击类型,讨论了身份验证和访问控制的机制和体系结构,未考虑物联网系统提供的服务层面上的安全需求。目前,针对智慧医疗设备存在的风险,研究人员提出了一种设备安全框架用来检测智能医疗设备^[5],为了保护隐私数据,提出一种针对云端隐私数据共享^[6]等数据传输某一环节的保护方法。

同时,现有的信息安全评估标准也存在评估目标维度单一、标准众多、缺乏统一的安全评估框架、无法满足新兴机密稳健复杂系统评估要求的局限性。赵庆兰^[7]针对 CC (common criteria) 标准只规定准则不设计方法的问题,提出了一种定性定量相结合的网络安全评估模型,但缺少系统及服务层面的安全指标考量;陈勇等^[8]扩展了 CC 标准的安全功能类从而对智能电视应用软件进行评估,缺少针对服务层面的安全功能类;Yang 等^[9]从等级保护标准角度出发,在分类对象和安全目标受到损害时对分类对象的损害程度这两个分类因素进行定性和定量分析,但缺少产品组件层面和服务层面的安全考量;赵艳玲^[10]分析了 NIST (national institute of standards and technology) “提升关键基础设施网络安全框架”,指出该框架提供一整套安全风险管控的标准和程序,是一套动态规范流程,要求评估实体具备识别、保护、检测、响应、恢复 5 种基本能力,却忽略了实体组件层面的安全需求和分析。因此,可以看出现有标准的应用场景和安全目标的定义不统一,包含的安全目标不完整,同时针对机密稳健复杂系统缺乏明确的指导和评估模型。

由此不难发现,目前面向机密稳健复杂系统

的安全评估策略和方法多局限在具体系统领域, 现有的众多标准评估目标维度单一、应用领域有限, 缺乏一个宏观统一的综合评价模型。

3 评估模型的构建

针对机密稳健复杂系统的安全评估缺乏统一评估模型的问题, 本文依据现有 CC 标准的评估流程, 在考虑指标间存在相互影响关系的基础上, 提出了如图 1 所示的基于指标关联性分析的多级分解反馈综合安全评估模型, 该评估模型阐述了机密稳健复杂系统的评估流程及关键考量点。首先, 其安全目标体系的建立是在综合参考 CC 标准、等级保护标准、NIST “提升关键基础设施网络安全框架” 等系列标准的基础上进行安全目标策略分解得来; 其次, 在安全目标形式化时, 考虑到评估指标间的相互关联性, 建立了基于指标关联性分析的指标体系; 最后, 利用相应的系统安全等级评估度量模型进行评估, 得到相应的量化或等级评测结果, 经过验证确认机制, 以评测结果作为反馈来增强系统的安全特性。

安全目标体系的建立旨在按照选定的评估标准, 将选定的评估对象进行安全目标策略分解。现有 CC 标准的基本概念、安全功能需求、安全

保证需求 3 部分相互依存, 从宏观角度阐述了对产品 and 系统安全评估的指导思想和技术要求^[1], 但对于如机密性这类具体要求, CC 标准的阐述并不详尽。公安部提出的信息安全等级保护标准 1.0 版本定义了信息系统的安全等级及要求项, 但其等级测试项目繁多, 与实际应用有些许偏差, 在等级保护 2.0 征求意见稿版本中, 仅考虑技术和管理两个角度, 应用领域有一定局限性, 未考虑到系统持续运行所需要的安全目标和提供服务层面的安全目标。NIST “提升关键基础设施网络安全的框架” 是一套着眼于安全风险、应用于关键基础设施广阔领域的安全风险管控流程, 相对于评估而言, 该框架更倾向于分析风险发生时的管控问题, 对于机密性方面的评估, 较少提及。

因此, 针对机密稳健复杂系统的评估, 因评估系统的独特性和重要性, 其安全目标的体系建立延续了 CC 标准, 并组合了我国的等级保护标准要求, 同时考虑到 NIST “提升关键基础设施网络安全的框架” 要求等, 从产品、系统、服务 3 个层面的需求进行分析, 构建机密稳健复杂系统的安全目标体系, 并将该类系统的安全目标体系形式化, 分为安全目标 (M_ST_i)、一级指标 (u_j)、二级指标 (u_{jp})。安全目标分为 8 个, 覆盖产品级

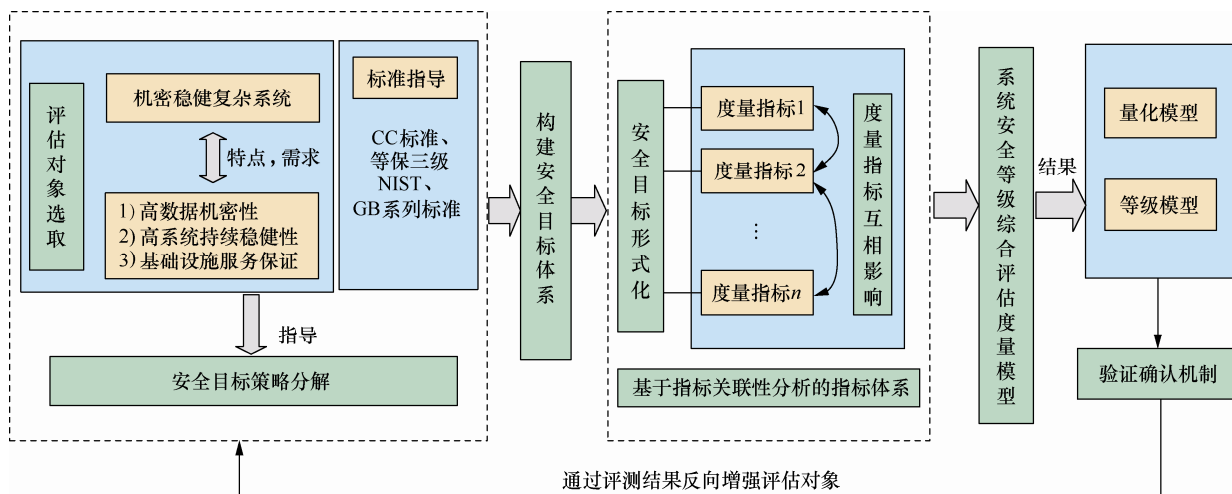


图 1 基于指标关联性分析的多级分解反馈综合安全评估模型

别、系统级别以及服务级别要求，分别为机密性、可用性、可控性、可鉴别性、人员组织、风险管理、企业定级和可连续性，如图2所示。

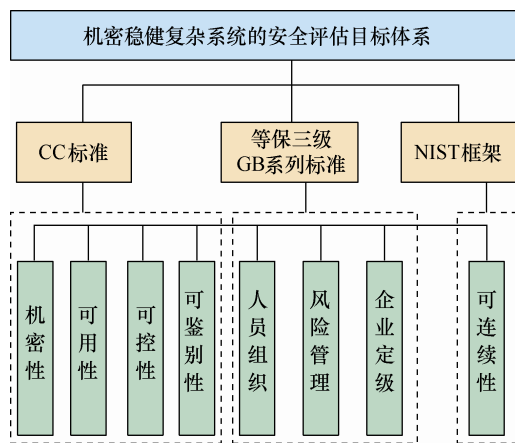


图2 机密稳健复杂系统的安全目标体系

考虑到机密稳健复杂系统是由不同的产品组件依据一定的连接原则，构成一个功能完备的系统，进而提供相应的服务，因此从产品、系统、服务3个层面进行评估对象的安全目标体系形式化，使评估对象的考量更加完备，同时也弥补了现有信息安全评估标准评估目标单一、功能有限的局限性。CC标准是安全评估领域底层最基本的考量，根据CC标准的指导将安全目标分为机密性、可用性、可控性、可鉴别性，从4个角度对产品组件的安全性进行衡量。等级保护标准是从威胁度矩阵的角度，对控制和管理进行了一定的分析，基于此，添加了人员组织、风险管理和企业定级的安全目标。考虑到NIST“提升关键基础设施网络安全的框架”是着眼于风险管控流程，更加注重系统在风险发生时的运转能力和动态服务的保持性，故增加系统的可持续性。

4 综合评估算法

针对机密稳健复杂系统的评价，考虑到所涉及指标间的影响关系，采用基于排序的确权算法

计算权重，然后选择使用模糊综合法计算整体的安全评估等级。

常用的确权方法如层次分析法(AHP, analytic hierarchy process)，由于知识、经验等客观因素存在，导致评估结果缺乏客观性，过分依赖于专家所得的评估结果。TOPSIS是基于距离的一种排序算法，在正理想解和负理想解的选取上过分依赖于专家的评价结果，应用在安全评估的场景时，不能很好地量化指标的权值。基于马尔可夫链的风险转移概率确权算法是根据指标间的风险转移概率来确定指标权重，但指标的风险转移概率较难准确获取^[12]。构建的基于指标关联性评估排序的确权方法，利用马尔可夫链的基本原理和指标间的关联性，结合PageRank^[13]的思想，根据专家的集体评估结果确定其间的影响程度，通过不断迭代计算，最终达到稳定的状态，以此确定指标的权重大小。利用此算法确定指标权重，不仅考虑到指标间的关联性，而且集合了众专家的评价结果，达到评价人数越多、评价结果越客观的效果，消除了单一专家评价的主观性问题。

4.1 建立模糊综合评价因素集合 U

1) 将 U 根据其具体属性及内容，划分成为 n 个子集，记为 $U = \{U_1, U_2, \dots, U_n\}$ 。

2) 对于每个子集，若其因素 U_i 包含 m 个下级指标，则可根据其情况继续进行划分记为 $U_i = \{U_{i1}, U_{i2}, \dots, U_{im}\}$ 。

4.2 基于排序的确权算法计算指标权重

基于排序的确权算法的权值计算基于以下假设：如果一个节点接收到的其他指向链入权重越大，那么这个节点越重要，同时，指向节点 A 的链入节点质量不同，质量高的节点通过链接向其他节点传递更多的权重，所以质量越高的节点指向节点 A ，则节点 A 越重要。

计算每个节点 PR 值的公式为

$$PR_{(p_i)} = \alpha \sum_{p_j \in M_{p_i}} \frac{PR_{(p_i)}}{L_{(p_j)}} + \frac{1-\alpha}{N} \quad (1)$$

其中, M_{p_i} 是所有对 p_i 节点有出链的节点集合, $L_{(p_j)}$ 是节点 p_j 的出链数目, N 是节点总数, α 为用户随机到达一个节点的概率, 一般取 0.85, 根据式(1)可以计算每个节点的 PR 值, 当迭代趋于平稳时, 即为最终结果。

4.3 建立评价集 V 及进行综合判断

评价集是指评价者对指定指标可能产生评价结果的集合, 记为 $V = \{V_1, V_2, \dots, V_t\}$ (假设共有 t 个评价结果)。

通过对某一具体指标对评判集中评价结果的映射关系, 得到被评价指标对评价集结果的隶属度, 假设因素集 U 中包含 n 个下级指标, 对其中的第 i 个指标进行评价, 通过评价得到第 i 指标对评价集 V 中第 j 个元素的隶属度, 记成 r_{ij} , 以 r_{ij} 为行构成隶属度矩阵, 即

$$R = \begin{bmatrix} r_{11} & \cdots & r_{1t} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mt} \end{bmatrix}_{n \times t} \quad (2)$$

所以, 模糊综合评估模型为

$$B = AR = (\phi_1, \phi_2, \dots, \phi_n)_{1 \times n} \begin{pmatrix} r_{11} & \cdots & r_{1t} \\ \vdots & \ddots & \vdots \\ r_{m1} & \cdots & r_{mt} \end{pmatrix}_{n \times t} = (b_1, b_2, \dots, b_t)_{1 \times t} \quad (3)$$

其中, $b_i (i=1, 2, \dots, t)$ 表示机密性对评价集 V 中第 i 个评价等级的隶属度。

4.4 评价指标的处理

评价指标选取最大隶属度法 $v = \{v_i | \max(b_i) \rightarrow v_i\}$, 即将模糊评价结果 B 中隶属度最大的评价集作为最终的评价结果。

5 分析建模与算法实现

机密稳健复杂系统领域中的智慧医疗物联网系统具有互联性、协作性、预防性、普及型、可靠性、创新性等特点^[14]。但医疗数据在多家医疗单位

之间的共享, 使用户医疗隐私信息泄露的风险加大^[15]。此外, 业内缺乏完备的监管规则、电子标签易被恶意追踪等现状也加剧了风险威胁^[16]。

机密性指信息不被泄露给非授权的用户、实体或过程, 或供其利用的特性。由于机密稳健复杂系统对可靠性要求很高, 而其隐私数据又存在泄露风险, 故机密性的评估显得尤为重要。因此, 选取智慧医疗物联网系统的机密性这一安全目标作为评估对象, 应用综合评估算法对其进行评估。

5.1 模型指标选取及评价因素集合 U 的确定

选定机密性作为评估目标, 并将其安全轮廓形式化为安全目标 (M_ST_i)、一级指标 (u_j)、二级指标 (u_{jp}) 这 3 部分, 具体如表 1 所示。

5.2 确定指标权重

在计算指标的权重时, 考虑到不同指标间风险概率的影响, 利用基于排序的确权算法计算指标的权重。

根据表 2 的专家评测结果构造邻接矩阵 Q , 再对矩阵 Q 列向量进行归一化处理推出概率转移矩阵 S 。其中, 专家评判的第 i 行 j 列值代表专家中认为第 i 个指标会影响第 j 个指标的人数。

构造完成的邻接矩阵 Q 和概率转移矩阵 S 如下。

$$Q = \begin{bmatrix} 0 & 10 & \cdots & 5 \\ 8 & 0 & \cdots & 8 \\ \vdots & \vdots & \ddots & \vdots \\ 8 & 4 & \cdots & 0 \end{bmatrix}_{16 \times 16}$$

$$S = \begin{bmatrix} 0 & 0.1 & \cdots & 0.05 \\ 0.08 & 0 & \cdots & 0.08 \\ \vdots & \vdots & \ddots & \vdots \\ 0.08 & 0.04 & \cdots & 0 \end{bmatrix}_{16 \times 16}$$

假设在计算 U 下 n 个二级指标的指标权重过程中, 计算每个二级指标的权重值, 即

表 1 机密性指标分析

安全目标 M_ST_i	一级指标 u_j	二级指标 u_{jp}
机密性 (M_ST_1)	基础安全设施和安全服务 (u_1)	密钥管理 (u_{11})
		用户名、密码的存储、操作 (u_{12})
		证书管理机构 CA (u_{13})
		证书发布 (u_{14})
		安全管理设备 (u_{15})
		安全算法 API (u_{16})
		增强的安全代理 (u_{17})
	用户数据保护 (u_2)	数据传输加密处理, 保证数据完整性 (u_{21})
		访问控制 (u_{22})
		数据鉴别-签名 (u_{23})
		数据源认证 (u_{24})
		数据存储加密 (u_{25})
		导入数据的控制 (u_{26})
	统一隐秘管理 (u_3)	隐私数据分布存放 (u_{31})
		密文搜索 (u_{32})
		提供隐私处理服务 (u_{33})

$$G = \alpha S + \frac{1-\alpha}{N} U \quad (4)$$

其中, U 为全 1 的 $n \times n$ 的矩阵, N 为指标节点的数量, G 为最终的转移矩阵。

表 2 指标关系专家打分情况

	u_{11}	u_{12}	...	u_{33}
u_{11}	0	10	...	5
u_{12}	8	0	...	8
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
u_{33}	8	4	...	0

利用最终的转移矩阵, 经过不断迭代, 计算得出 P_n , 即

$$P_{n+1} = GP_n \quad (5)$$

其中, P_n 值为第 n 次迭代时各概率值组成的列向量, 最终的 P_n 值构成二级指标的权重值为

$$A = \{\phi_1, \phi_2, \dots, \phi_{33}\} = \{0.0748, 0.1243, \dots, 0.0622\}。$$

5.3 建立评价等级集 M 及综合判断

根据评价结果类型和要求, 以该指标对安全目标——机密性的影响程度作为评价基础, 建立评价等级集 $M = \{\text{安全很低, 安全低, 安全中等, 安全高, 安全很高}\}$, 简记为 $M = \{\text{很低, 低, 中等, 高, 很高}\}$ 。

模糊判断矩阵 R 的确定, 主要是通过专业评审人员或者部门内部成员对各个指标的打分, 最后对得到的 N 份有效打分表数据进行处理, 得到的整理数据如表 3 所示。

表 3 隶属度矩阵专家打分情况

评价项目	很低	低	中	高	很高
u_{11}	0.1	0.15	0.1	0.5	0.25
u_{12}	0.05	0.05	0.075	0.375	0.45
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
u_{33}	0.125	0.175	0.225	0.25	0.225

故得到的模糊判断矩阵 R 为

$$R = \begin{bmatrix} 0.1 & 0.15 & 0.1 & 0.5 & 0.25 \\ 0.05 & 0.05 & 0.075 & 0.375 & 0.45 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0.125 & 0.175 & 0.225 & 0.25 & 0.225 \end{bmatrix}_{16 \times 5}$$

5.4 模糊综合评价

针对机密性的模糊综合评判如下。

$$\begin{aligned} B &= AR = (0.074\ 8, 0.124\ 3, \dots, 0.062\ 2) \\ &= \begin{bmatrix} 0.1 & 0.15 & 0.1 & 0.5 & 0.25 \\ 0.05 & 0.05 & 0.075 & 0.375 & 0.45 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0.125 & 0.175 & 0.225 & 0.25 & 0.225 \end{bmatrix}_{16 \times 5} \\ &= (0.040\ 2, 0.099\ 6, 0.288\ 4, 0.388\ 1, 0.183\ 6) \end{aligned}$$

5.5 评判结果

对评价指标的处理选取最大隶属度法, 根据模糊评价集的最终结果 $B = (0.040\ 2, 0.099\ 6, 0.288\ 4, 0.388\ 1, 0.183\ 6)$ 和最大隶属度原则, 最终的评判结果为高。

针对智慧医疗系统的机密性安全目标, 利用综合评价法评价得出它的安全等级为高。

6 结束语

机密稳健复杂系统的安全质量评估尚在起步阶段, 缺乏统一的安全评估模型和指标体系, 本文通过综合参考通用准则 CC、公安部等级保

护标准等现有标准体系, 从产品、系统和服务 3 个层面确立了机密性、风险管理、企业定级、可持续性等 8 个安全目标为核心的评估体系。考虑到指标体系间的相互关联性, 本文提出了基于量化指标关系的安全评估模型。随后, 选取智慧医疗物联网系统的机密性这一安全目标作为评估对象, 构建了基于指标关联性的排序确权算法, 应用模糊综合评价方法进行实例化验证, 最终确定其机密性等级安全评价结果为高。

参考文献:

- [1] GRÜNBAUER J, HOLLMANN H, JÜRJENS J, et al. Modelling and verification of layered security protocols: a bank application[C]//International Conference on Computer Safety. 2003.
- [2] CIGRE Task Force 38. 03. 12. Power system security assessment: a position paper[J]. Electra, 1997, (175) : 49-77.
- [3] XIAO F, MCCALLEY J D. Risk-based security and economy tradeoff analysis for real-time operation[J]. IEEE Transactions on Power Systems, 2007, 22(4):2287-2288.
- [4] YANG Y, WU L, YIN G, et al. A Survey on security and privacy issues in Internet of things[J]. IEEE Internet of Things Journal, 2017, 4(5):1250-1258.
- [5] ASPINALL D, WOLTERS M. POSTER: weighing in eHealth security[C]//Sigsac Conference on Computer and Communications Security. 2016: 1832-1834.
- [6] YANG LEI, HUMAYED A, LI FENGJUN. A multi-cloud based privacy-preserving data publishing scheme for the Internet of things[C]//Conference on Computer Security Applications. 2016:30-39.
- [7] 赵庆兰. 一种基于 CC 的网络安全评估模型[J]. 计算机安全, 2008(3):42-43.
ZHAO Q L. A network security evaluation model based on CC[J]. Computer Security, 2008(3):42-43.
- [8] 陈勇, 莫玮, 王勇, 等. 一种基于 CC 的智能电视应用软件安全评估方法[J]. 电视技术, 2014, 38(8): 72-74+82.
CHEN Y, MO W, WANG Y, et al. Security assessment method of smart TV's application based on CC[J]. Video Engineering, 2014, 38(8):72-74.
- [9] YANG Y H, SHEN Y J, ZHANG G D, et al. The grading scheme based on fuzzy comprehensive evaluation and analytic hierarchy process for classified protection of information system[C]//5th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2014.
- [10] 赵艳玲. 浅谈美国《提升关键基础设施网络安全框架》[J]. 信息安全与通信保密, 2015(5): 16-21.
ZHAO Y L. Brief probe into "Framework for improving critical infrastructure cybersecurity"[J]. Information Security and Communications Privacy, 2015(5):16-21.
- [11] 逢淑宁, 封莎. 信息技术安全评估通用准则 CC 综述[J]. 电信网技术, 2011(8):59-63.
FENG S N, FENG S. Review on information technology security assessment common criteria CC[J]. Information and Communications Technology and Policy, 2011(8):59-63.
- [12] 张秋瑾. 云计算隐私安全风险评估[D]. 昆明: 云南大学, 2015.
ZHANG Q J. Cloud computing privacy security risk assessment[D]. Kunming: Yunnan University, 2015.
- [13] PANG H M, LIU H Z. Research on information engineering security surveillance risk assessment based on page rank algorithm[J]. Computer Security, 2014(8): 17-20.
- [14] 郑改成. 基于物联网下的智慧医疗体系架构及其应用[J]. 山西电子技术, 2016(5):66-68.
ZHENG G C. Architecture and application of the smart healthcare based on Internet of things[J]. Shanxi Electronic Technology, 2016(5): 66-68.
- [15] 张玉清, 周威, 彭安妮. 物联网安全综述[J]. 计算机研究与发展, 2017, 54(10): 2130-2143.

ZHANG Y Q, ZHOU W, PENG A N. Survey of Internet of things security[J]. Journal of Computer Research and Development, 2017, 54(10):2130-2143.

- [16] 杨颖, 朱君茹, 袁媛, 等. 医疗物联网的发展现状、问题与对策[J]. 中国卫生信息管理杂志, 2015(3): 298-303.

YANG Y, ZHU J R, YUAN Y, et al. Development status, problems and countermeasures of medical Internet of things[J]. Chinese Journal of Health Informatics and Management, 2015(3):298-303.

[作者简介]



左金鑫(1992-), 女, 山东德州人, 北京邮电大学博士生, 主要研究方向为网络空间安全。



李瑾(1996-), 女, 黑龙江齐齐哈尔人, 北京邮电大学硕士生, 主要研究方向为网络空间安全。



张洁(1981-), 女, 军事科学研究院系统工程院教授, 主要研究方向为信息安全。



郭子裕(1994-), 男, 河北石家庄人, 北京邮电大学博士生, 主要研究方向为网络空间安全。



陆月明(1969-), 男, 江苏苏州人, 北京邮电大学教授、博士生导师, 主要研究方向为分布式计算、网络空间安全。