

高安全属性价值设备威胁态势量化评估方法

韩磊^{1,2}, 刘吉强³, 王健³, 石波¹, 和旭东³

(1. 北京计算机技术及应用研究所, 北京 100854;

2. 信息保障技术重点实验室, 北京 100072;

3. 北京交通大学智能交通数据安全与隐私保护技术北京市重点实验室, 北京 100044)

摘要: 传统的网络安全态势量化评估方法主要面向宏观网络安全态势, 未针对安全价值较高的网络设备, 给出了高安全属性价值设备的定义, 设计了针对设备的威胁态势量化评估框架和评估指标, 根据评估框架和指标提出了高安全属性价值设备威胁态势量化评估方法。对具体网络中实际设备的评估结果表明, 该方法能够准确、有效地量化评估高安全属性价值设备的威胁态势。

关键词: 态势感知; 安全威胁; 量化评估; 高安全属性价值设备

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020070

Quantitative threat situational assessment method for higher secure attribute value device

HAN Lei^{1,2}, LIU Jiqiang³, WANG Jian³, SHI Bo¹, HE Xudong³

1. Beijing Institute of Computer Technology and Applications, Beijing 100854, China

2. Science and Technology on Information Assurance Laboratory, Beijing 100072, China

3. Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China

Abstract: Traditional network security situational assessment is mainly for the macro network security situation, not for the specific equipment, especially for the key network device. A conception about the higher secure attribute value device was introduced, based on which a threat situational assessment research framework was presented and assessment indexes were discussed. A quantitative threat situational assessment method for higher secure attribute value device was proposed based on assessment research framework and assessment indexes. The experiment results

收稿日期: 2020-01-03; 修回日期: 2020-03-21

通信作者: 韩磊, hanlei316@126.com

基金项目: 国家自然科学基金(61672092); 国防基础科研(JCKY2017204B063); 中央高校基本科研业务费专项基金(2018JBZ103); 山东省重大科技创新工程(2019JZZY020128); 中国博士后科学基金(2018M633698)

Foundation Items: The Natural Science Foundation of China (61672092), National Defense Basic Research (JCKY2017204B063), The Fundamental Research Funds for the Central Universities of China (2018JBZ103), The Major Scientific and Technological Innovation Projects of Shandong Province, China (2019JZZY020128), China Postdoctoral Science Foundation (2018M633698)

论文引用格式: 韩磊, 刘吉强, 王健, 等. 高安全属性价值设备威胁态势量化评估方法[J]. 网络与信息安全学报, 2020, 6(5): 54-66.

HAN L, LIU J Q, WANG J, et al. Quantitative threat situational assessment method for higher secure attribute value device[J]. Chinese Journal of Network and Information Security, 2020, 6(5): 54-66.

show that the proposed method can assess device threat situation accurately and effectively. Meanwhile, the method is more general and objective than traditional methods.

Key words: situational awareness, security threat, quantitative evaluation, higher security attribute value device

1 引言

网络信息智能化防御中,网络安全态势感知是前提和基础。网络安全态势感知能够对引起网络安全态势变化的要素进行获取、理解、评估、可视化及预测未来发展趋势。其中,网络安全态势评估能够从宏观上动态反映网络的安全状态,当前网络层面的态势评估方法相对成熟^[1],虽有差异,但从研究思路及对态势感知的诠释^[2]上接受并延续了JDL(joint directors of laboratories)数据融合思想^[3]和Endsley态势感知层次模型^[4]。

网络安全态势评估常规过程是:利用网络探针或网络传感器收集全网态势数据^[5-8],利用数据融合的方式处理态势要素^[9-12],使用数学模型、知识推理、模式识别等基于知识的方法对网络安全态势进行量化评估。随着网络攻防博弈的不断演进,大数据分析和机器学习等基于数据的方法^[13-16]在感知、察觉网络状态、检测网络攻击、预测网络风险等方面不断有所突破,逐渐形成了针对网络安全的态势感知体系,并通过基于知识、基于数据及知识和数据融合的方法,建立了对网络安全要素认知-理解-评估的模式,在评估网络宏观安全态势方面给出了有效的解决途径。但在微观具体化、针对性方面还存在不足,具体表现为:该评估方法仅反映出单位时间内网络宏观安全状态及变化趋势,无法在微观层有针对性地呈现出网络中高安全属性价值设备(这种设备通常处于网络信息系统的关键位置,是对系统安全、稳定运行具有决定性作用的核心设备。例如,铁路、电力、核能等国家基础设施中的工业控制器、云数据中心的边界防火墙、主干网中的高速率大容量核心路由或交换设备、用于保护金融交易安全的网络密码设备、政府机构存储秘密信息的服务主机等)面临的威胁、脆弱性的危害程度、安全事件发生的可能性及拒绝服务性能劣化程度等设备威胁态势。例如,张勇^[17]、席荣荣^[18]等分别利用马尔可夫博弈模型和隐马尔可夫模型对网络安全状态建模,基于网络下一时刻的安全状态只与当

前时刻安全状态相关的马尔可夫特性这一假设条件,通过博弈论方法确定网络的状态变化。前者采用攻击方、防守方和中立方的三方博弈;后者采用防护措施与安全事件的双方博弈,两种方法均以博弈的结果推演出网络的安全态势,解决网络安全态势量化评估的问题,该类方法基于网络状态遵循马尔可夫随机过程的假设,在多步攻击的实际场景中具有局限。例如,当网络受到多步攻击时,网络被攻破的状态和多步攻击持续的作用相关,并且与网络边界或核心位置设备的状态相关;甚至在特定多步攻击场景中,高安全属性价值设备的状态对全网的安全状态具有决定性影响。某种意义上,攻破了该类设备等价于攻破了网络。杨豪璞等^[19]从网络受到多步攻击的角度描述网络状态,该方法利用节点状态确定攻击场景,用以评估网络安全态势,但仅考虑节点状态与漏洞、安全事件及前置状态“与”“或”关系,无法客观反映节点状态与网络环境、设备属性相关的实际情况。席荣荣等^[18]利用网络环境属性判定安全事件发生的可能性,解决威胁感知量化评估准确性的问题,但该方法没有考虑节点性能劣化对威胁量化评估的影响,也无法确定节点所处的安全状态。杨君刚等^[20]通过安全风险因子和安全风险影响因子对路由器设备进行了威胁态势评估,该方法能够直观地反映出路由器的安全威胁风险,给出了描述路由器这种网络关键节点设备的威胁量化评估方法,但该方法仅针对路由器的具体特征,用路由器的位置和交换容量来衡量设备对安全风险影响的程度,没有抽象出路由器这种高安全价值设备威胁量化评估的普适特征。Yu等^[21]提出了基于熵的态势评估方法,该方法采用对设备进行威胁评估的方式,评估整体网络的威胁态势,为基于设备威胁实现网络整体安全态势评估提供了一种新的思路,但在设备威胁评估方面还有不足。具体来说,该方法利用同种攻击对不同设备的不同威胁程度来评估设备在网络中的安全状态,以此给出整体网络的态势,其评估过程关注网络中的所有设备,这种方式关注“点”多,

评估分析的“面”较大,导致评估方法在运行时效率性方面表现不足。此外,自“震网”病毒针对工业基础设施进行攻击后,针对关键基础设施及关键设备的安全态势感知引起广泛关注。Cristina^[22]在网络安全态势感知的基础上提出了针对关键基础设施安全的广域态势感知^[23](WASA, wide-area situational awareness)框架及一系列针对关键基础设施构建态势感知的原则,该框架在宏观层面给出了针对关键基础设施的安全态势感知方法论;Cristina 等^[23]在 WASA 的基础上进一步讨论了关键基础设施存在的脆弱性及易遭受到的网络攻击,并给出了降低网络攻击的防护措施。Ceeman 等^[24]利用网络拓扑、系统日志及配置信息通过贝叶斯网络对关键基础设施建模,计算网络安全指数来评估关键基础设施所处的安全等级。该类工作关注关键基础设施,将泛在网络空间感知对象聚焦到关键基础设施上,但仍然缺少对基础设施中高安全价值设备的威胁评估,无法在微观层面呈现出关键基础设施设备中存在的薄弱环节。

针对上述研究存在的问题,本文首先给出高安全属性价值设备定义,在此基础上提出了针对设备的威胁态势量化评估框架和评估指标,并根据评估框架和指标提出了高安全属性价值设备威胁态势量化评估方法。该方法以设备的性能、配置和脆弱性为基础,验证威胁警报、评估威胁警报的有效性,基于有效警报,构建设备状态评估算法,评估设备所处安全状态,并利用评估指标量化计算设备威胁态势。对具体网络中实际设备的评估结果表明,该方法能够准确、有效地量化评估高安全属性价值设备的威胁态势。

2 相关定义

本节给出本文工作将用的相关定义。

定义 1 (设备) 网络环境中的物理实体,单个设备用 $e\text{-device}=(id_e, name_e, type_e, attrvalue_e, config_e)$ 表示,其中, id_e 为设备标识, $name_e$ 为设备名称, $type_e$ 为设备类型,包括安全设备、保密设备、网络设备、服务设备和终端设备等; $attrvalue_e$ 为设备安全属性价值, $config_e$ 为设备的配置信息。

定义 2 (安全属性价值) 网络环境中设备有保密性、完整性和可用性 3 种安全属性,设备在网络中的价值由其安全属性达成或安全属性未达成时所造成的影响程度来衡量。设备安全属性价值用 $attrvalue_e=f(conf_e, int_e, avail_e)$ 表示,其中 $conf_e$ 、 int_e 、 $avail_e$ 分别表示设备的保密性属性、完整性属性和可用性属性,每个属性分 5 级,用 1,2,3,4,5 表示^[25]。为表示不同信息系统所属设备安全属性的差异,用 $w_i(i=1,2,3)$ 表示设备 3 种安全属性的权重, w_i 值的选取参考文献[18]。

$$f(conf_e, int_e, avail_e) = \text{lb} \frac{w_1 2^{conf_e} + w_2 2^{int_e} + w_3 2^{avail_e}}{3} \quad (1)$$

定义 3 (高安全属性价值设备) 根据 GB/T 20984—2007^[26]对资产价值等级及标识的赋值,定义当设备安全属性价值 $attrvalue_e \geq \varepsilon$ 时,其中, $4 \leq \varepsilon \leq 5$, 设备为高安全属性价值设备。

定义 4 (设备配置) 用来表征设备配置及服务的属性信息。设备配置用 $config_e=(ip_e, name_e, port_e, service_e, confdescription_e)$ 表示,其中, ip_e 为设备的 IP 地址池, $name_e$ 为设备的名称, $port_e$ 为设备配置的端口组, $service_e$ 为设备可以提供的服务, $confdescription_e$ 为设备的其他配置信息,包括设备固件、软件类型、版本、硬件配置等。

定义 5 (设备警报) 由设备发出的针对可疑安全事件或异常事件的通知,单个警报信息用 $alert_e=(id_a, name_a, time_a, souIP_a, desIP_a, souPort_a, desPort_a, alertdescription_a, id_e, name_e)$ 表示,其中, id_a 表示警报的标识, $name_a$ 表示警报的名称, $time_a$ 表示警报产生的时间, $souIP_a$ 、 $desIP_a$ 分别表示警报事件发起的源 IP 地址和目标 IP 地址, $souPort_a$ 、 $desPort_a$ 分别为警报事件发起的源端口及设备目标端口, $alertdescription_a$ 为警报的其他描述性信息,如威胁类型、异常类型、协议类型及操作内容等, id_e 、 $name_e$ 分别是警报产生设备的标识及名称。

定义 6 (设备脆弱性) 由设备软硬件中自身存在的、可以被威胁利用的异常或漏洞,用 $vulnerabilities_e=(abnormities.id_{abn}, name_{abn}, description_{abn}, type_{abn}, severity_{abn}, bug.cve-id_b, name_b, description_b, cvss_b)$ 表示,其中 $abnormities.id_{abn}$ 、

$name_{abn}$ 、 $description_{abn}$ 分别为异常标识、名称及异常行为描述, $type_{abn}$ 为异常类型, 包括保密性异常、可用性异常及完整性异常, $severity_{abn}$ 表示异常的严重程度; $bug.cve-id_b$ 、 $name_b$ 、 $description_b$ 分别为漏洞 cve 编号、名称及漏洞描述, $cvss_b$ 表示漏洞的严重程度, 用 CVSS 评分衡量^[26]。severity 表示设备脆弱性 (包括异常和漏洞) 的严重程度。

定义 7 (设备性能) 设备提供服务的基本能力, 设备性能信息用 $perinfo_e = (id_p, c_p, tem_p, b_p, m_p, ses_p, loss_p, id_e, name_e)$ 表示, 其中 id_p 表示设备性能标识, t_p 表示采集性能的时刻, c_p 表示设备 CPU 利用率, tem_p 表示设备内部温度, b_p 表示设备带宽利用率, m_p 表示设备内存利用率, ses_p 表示会话连接数, $loss_p$ 表示丢包率, id_e 、 $name_e$ 表示采集性能信息设备的标识及名称。基于文献[27], 扩展定义设备性能值为 6 个参数 ($c_p, tem_p, b_p, m_p, ses_p, loss_p$) 的函数。

$$per_e(c_p, tem_p, b_p, m_p, ses_p, loss_p) = 1 - \frac{1}{6} \left(c_p + \frac{tem_p - tem_{\min}}{tem_{\max} - tem_{\min}} + b_p + m_p + \frac{ses_p}{ses_{\max}} + loss_p \right) \quad (2)$$

定义 π ($0 \leq \pi \leq 1$) 为设备性能劣化对设备态势的影响程度, $\Delta per_{e(i)}$ 为第 i 个采样点与第 $i-1$ 个采样点间的性能变化量, $\sum \Delta per_{e(i)}$ 为性能变化累积量, 当设备性能劣化时 $\sum \Delta per_{e(i)} < 0$ 。

定义 8 (设备状态) 用来表征威胁作用到设备上, 设备所处的安全状态, 用 $E_status = \{X_1, X_2, \dots, X_i, X_j, \dots, X_n\}$, $i \leq j$, $n \in \mathbb{N}$ 表示, $status_probability = p_{threat}(X_j)$ 为设备所处状态 X_j 的可能性, $status_loss$ 为威胁有效作用到设备上造成的损失。

一般设备在遭受到实质性攻击前, 会被各种手段进行侦测。例如, IP 扫描、端口扫描、存活性扫描、漏洞扫描等, 设备处于被扫描状态; 扫描确定设备为攻击对象后, 付诸相应手段进行非法提权, 试图访问设备资源, 此时设备处于被攻击状态; 如果敌手能够有效利用设备存在的脆弱性, 则设备将处于被攻破状态, 进而遭到破坏, 敌手达成攻击目的; 如果敌手无法有效利用设备脆弱性, 也可以发起拒绝服务, 最终致瘫设备, 安全状态示例如图 1 所示。

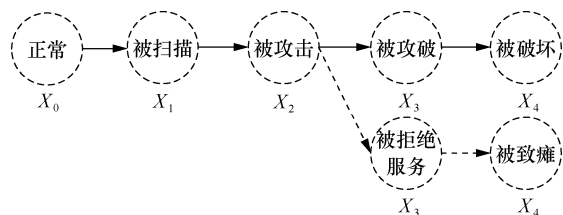


图 1 安全状态示例

Figure 1 An example of secure status

3 设备威胁态势量化评估框架与评估指标

本节提出了针对设备的威胁态势量化评估框架、评估流程及评估指标。

设备的威胁态势不仅与设备受到的威胁有关, 还与设备的安全属性 (保密性、可用性 & 完整性) 价值、设备脆弱性 (异常及漏洞)、设备配置、设备警报、设备性能及设备状态等因素有关, 基于以上因素, 本文提出设备威胁态势评估框架, 如图 2 所示。根据评估框架, 具体评估流程如下。

Step 1 获取设备态势相关的属性信息 $devattrinfo = (\{alert_e\}, config_e, vulnerabilities_e, perinfo_e)$, 其中, $\{alert_e\}$ 为警报集合。

Step 2 建立评估指标, 如表 1 所示, $indexsys = (attrvalue_e, \Delta t, \pi, \sum \Delta per_{e(i)}, severity, status_loss, status_probability)$ 。

Step 3 以设备性能、配置、脆弱性为基础, 验证警报、评估威胁警报的有效性。

Step 4 基于有效警报, 构建设备受到威胁后的状态评估算法, 评估设备所处安全状态。

Step 5 综合利用评估指标, 量化计算设备威胁态势 (ETSA, e-device threat situational awareness)。

4 设备威胁态势量化评估方法

根据第 2 节提出的设备威胁态势量化评估框架, 本节设计了高安全属性价值设备威胁态势量化评估方法。该方法在获取设备威胁态势相关的属性信息 $devattrinfo$ 及建立评估指标体系 $indexsys$ 后, 需要以设备性能、配置、脆弱性为基础, 验证警报、评估威胁警报的有效性; 进而基于有效警报, 构建设备受到威胁后的状态评估算法, 评估设备所处安全状态; 最后综合利用评

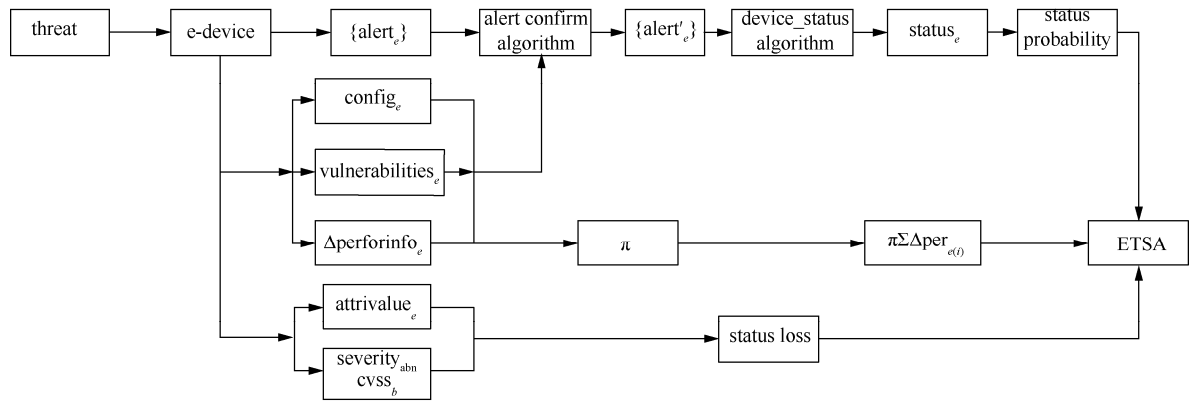


图 2 设备威胁态势量化评估框架

Figure 2 The framework of quantitative device threat situational assessment

表 1 评估指标
Table 1 Assessment indexes

attrvalue _e	$\Delta t/\pi$	Δper_e	severity	Status loss	Status probability
conf _e	t_i	per _{e(i)} time= t_i	severity _{abn}	attrvalue _e	$p_{threat}(X_j)$
int _e	t_{i-1}	per _{e(i-1)} time= t_{i-1}	cvss _b	severity	—
avail _e	$\Delta t = t_i - t_{i-1}$	$\Delta per_e = per_{e(i)} - per_{e(i-1)}$	—	—	—
w_i	π	$\sum \Delta per_{e(i)}$	—	—	—

估指标量化计算设备威胁态势。

4.1 威胁警报有效性评估算法

威胁警报有效性评估算法流程如图 3 所示。

算法 1 威胁警报有效性评估算法

输入 设备属性信息 devattrinfo = ({alert_e}, config_e, vulnerabilities_e, perinfo_e), {alert_e} = {a₁, a₂, ..., a_i, ..., a_M, i ≤ M};

输出 有效警报集合 {alert'_e} = {a'₁, a'₂, ..., a'_i, ..., a'_m, i ≤ m, m ≤ M}, {alert'_e} ∈ {alert_e} 及威胁警报有效性评估值 $p_{threat}(a'_i)$ 。

begin

1) select {config_e.x₁, config_e.x₂, ..., config_e.x_j, ..., config_e.x_n, j ≤ n} from devattrinfo.config_e

2) select {vulnerabilities_e.y₁, vulnerabilities_e.

y₂, ..., vulnerabilities_e.y_r, ..., vulnerabilities_e.y_u, r ≤ u} from devattrinfo.vulnerabilities_e

3) select {perinfo_e.z₁, perinfo_e.z₂, ..., perinfo_e.z_g, ..., perinfo_e.z_h, g ≤ h} from devattrinfo.perinfo_e

4) n + u + h = k; /*提取设备属性信息*/

5) for each config_e.x_j, j = 1, 2, ..., n, v₁ = 0

6) if a_i ∈ config_e.x_j a'_i = a_i, v₁++, p_{config}(a'_i) =

$$\frac{v_1}{k}$$

7) for each vulnerabilities_e.y_r, r = 1, 2, ..., u, v₂ = 0

8) if a_i ∈ vulnerabilities_e.y_r, a'_i = a_i, v₂++,

$$p_{vul}(a'_i) = \frac{v_2}{k}$$

9) for each perinfo_e.z_g, g = 1, 2, ..., h, v₃ = 0

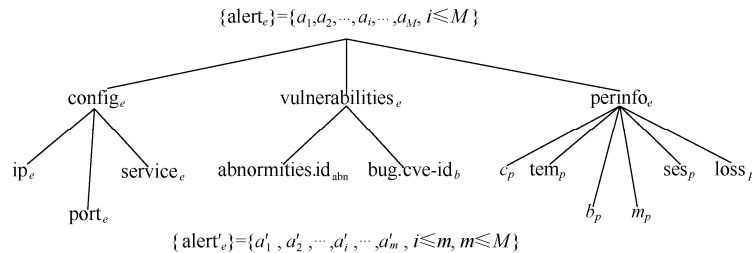


图 3 威胁警报有效性评估算法

Figure 3 The algorithm for assessing effectiveness of threat alerts

10) if $a_i \in \text{perinfo}_{e,z_g}$, $a'_i = a_i, v_3++$, $p_{\text{per}}(a'_i) = \frac{v_3}{k}$

11) $p_{\text{threat}}(a'_i) = p_{\text{config}}(a'_i) + p_{\text{vul}}(a'_i) + p_{\text{per}}(a'_i)$

12) return $\{\text{alert}'_e\} = \{a'_1, a'_2, \dots, a'_i, \dots, a'_m, i \leq m, m \leq M\}$ and $p_{\text{threat}}(a'_i)$

end

4.2 基于有效威胁警报的设备状态评估算法

设备威胁状态评估算法如图4所示。

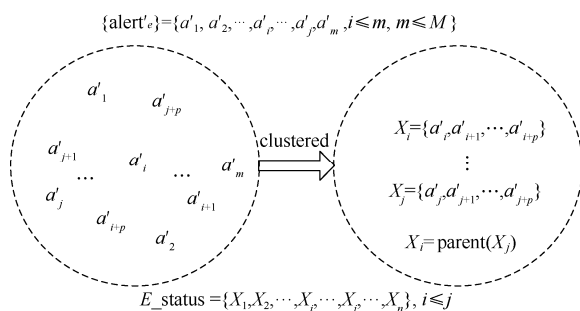


图4 设备威胁状态评估算法
Figure 4 The algorithm for threat status assessing

算法2 基于有效威胁警报的设备状态评估算法

输入 有效警报集合 $\{\text{alert}'_e\} = \{a'_1, a'_2, \dots, a'_i, \dots, a'_m, i \leq m, m \leq M\}$, $\{\text{alert}'_e\} \in \{\text{alert}_e\}$ 及威胁警报有效性评估值 $p_{\text{threat}}(a'_i)$;

输出 设备当前状态 X_j , $X_j \in E_status$, $E_status = \{X_1, X_2, \dots, X_i, \dots, X_j, \dots, X_n\}, i \leq j, n \in N$ 和设备所处安全状态的概率 $\text{status_probability} = p_{\text{threat}}(X_j)$ 。

begin

1) for each alert'_e $a'_1, a'_2, \dots, a'_i, \dots, a'_m$

2) let X_i, X_j represent the status of device

3) $E_status = \text{clustered}(\{\text{alert}'_e\})$; /* 聚合警报 */

4) $X_i = \{a'_i, a'_{i+1}, \dots, a'_{i+p}\}$, $X_j = \{a'_j, a'_{j+1}, \dots, a'_{j+q}\}$

/* 用警报聚合表示设备状态 */

5) $X_i = \text{parent}(X_j)$; /* 根据攻击模式确定状态父子关系 */

6) let E_status_t represent the device status on

7) time t , $E_status_{t'}$ represent the device status

8) on time t' , $t < t'$

9) $E_status_t = X_i$, $E_status_{t'} = X_j$, and $X_i = \text{parent}(X_j)$

10) device status from E_status_t to $E_status_{t'}$; /* 设备状态由 X_i 转换到 X_j */

11) return $E_status_{t'} = X_j$ and $\text{status_probability} = p_{\text{threat}}(X_j) = \frac{1}{q-1} \sum_{i=0}^q p_{\text{threat}}(a'_{j+1})$

end

4.3 性能劣化对设备威胁态势的影响

设备性能的非正常劣化表征设备受到拒绝服务的严重程度。设备性能中 CPU 利用率 cp 、内存利用率 mp 的劣化程度表征计算消耗型拒绝服务攻击的强度；带宽利用率 bp 、会话连接 seps 、丢包率 lossp 的劣化表征了带宽消耗型拒绝服务的强度。设备内部温度过高，表征了运行环境对设备计算及带宽性能的综合影响。利用性能劣化累积量 $\sum \Delta \text{pere}(i)$ （设备性能劣化时 $\sum \Delta \text{pere}(i) < 0$ ）综合表示单位时间内拒绝服务的攻击强度， π 表示性能劣化对设备态势的影响程度，用 $\pi \times (-1) \times \sum \Delta \text{pere}(i)$ 表示设备威胁态势中的性能分量。

4.4 有效威胁对设备造成的损失

威胁利用设备脆弱性将给设备带来损失，损失与设备安全属性价值和脆弱性严重程度相关，该种威胁为有效威胁，有效威胁对设备造成的损失用 status_loss 表示。

$$\text{status_loss} = \text{attrvalue}_e \cdot \text{severity} \quad (3)$$

安全属性价值 attrvalue_e 通过定义2计算得出。设备脆弱性的严重程度 severity 包括异常的严重程度 $\text{severity}_{\text{abn}}$, $0 \leq \text{severity}_{\text{abn}} \leq 10$ 和漏洞的严重程度 cvss_b , $0 \leq \text{cvss}_b \leq 10$, 具体表示为

$$\text{severity} = \frac{1}{20} (\text{severity}_{\text{abn}} + \text{cvss}_b), 0 \leq \text{severity} \leq 1 \quad (4)$$

参考 CVSS^[27]对漏洞的评分，给出设备异常的严重程度的计算得分。

$$\text{severity}_{\text{abn}} = 10(1 - (1-A)(1-I)(1-C)) \quad (5)$$

设备异常分类如表2所示。

漏洞的严重程度 cvss_b 可以直接参考 CVSS 给出的评分。

表 2 设备异常分类
Table 2 Classification of device abnormality

可用性异常 $A(0.3)$	完整性异常 $I(0.3)$	保密性异常 $C(0.4)$
计算性能劣化	启动关键库异常	Ipssec 报文异常
带宽性能劣化	硬件检测失败	非策略访问
环境性能劣化	完整性校验失败	加解密错误
服务业务失败	查询状态失败	更换数据失败
管理业务失败	格式解析失败	密钥及算法过期

4.5 设备威胁态势量化评估

通过评估指标、威胁警报有效性评估算法(算法 1)、设备状态评估算法(算法 2), 量化计算设备的威胁态势, 具体为

$$ETSA = \begin{cases} (1-\pi) \cdot (\text{status_probability} \cdot \text{status_loss}) + \\ \pi \cdot (-1) \cdot \sum \Delta \text{per}_{e(i)} \cdot \sum \Delta \text{per}_{e(i)} < 0 \\ (1-\pi) \cdot \text{status_probability} \cdot \\ \text{status_loss} \sum \Delta \text{per}_{e(i)} \geq 0 \end{cases} \quad (6)$$

5 实验分析

为了阐明高安全价值设备威胁评估的原理和过程, 验证本文方法的合理性及有效性, 本节介

绍如何构建实验网络, 在网络环境中评估设备的安全属性价值, 确定高安全属性价值设备, 并对其进行威胁态势量化评估。

实验网络拓扑如图 5 所示。Web 服务 (Tomcat)、数据库服务 (MongoDB)、负载均衡服务 (LVS) 及版本管理服务 (SVN) 通过交换机置于网络的 DMZ 域; 桌面云服务 (Fusion Access) 及文件存储服务 (NFS) 通过 Vlan 置于网络的 Trust 域; 系统性能、日志服务 (Log Server) 及安全文件传输服务 (SFTP) 置于网络的 Management 域, 具有 IPsec 功能的防火墙位于 Trust 域和 Untrust 域的边界。外部连接通过 Untrust 域到 Trust、DMZ 域间的映射实现, 整体网络在 DMZ 和 Trust 域部署 Snort^[28] (IDS)。防火墙警报及 Snort 警报通过设备信息中心接入 Management 域的 LogServer 及 SFTP。

实验网络主要资产信息如表 3 所示。

根据定义 3, 当设备安全属性价值 $\text{attrvalue}_e \geq \varepsilon$ 时, 其中, $4 \leq \varepsilon \leq 5$, 设备为高安全属性价值设备。表 3 数据表明, de_011 和 de_006 为实验网络中的高安全属性价值设备, 其脆弱性信息如表 4 所示。

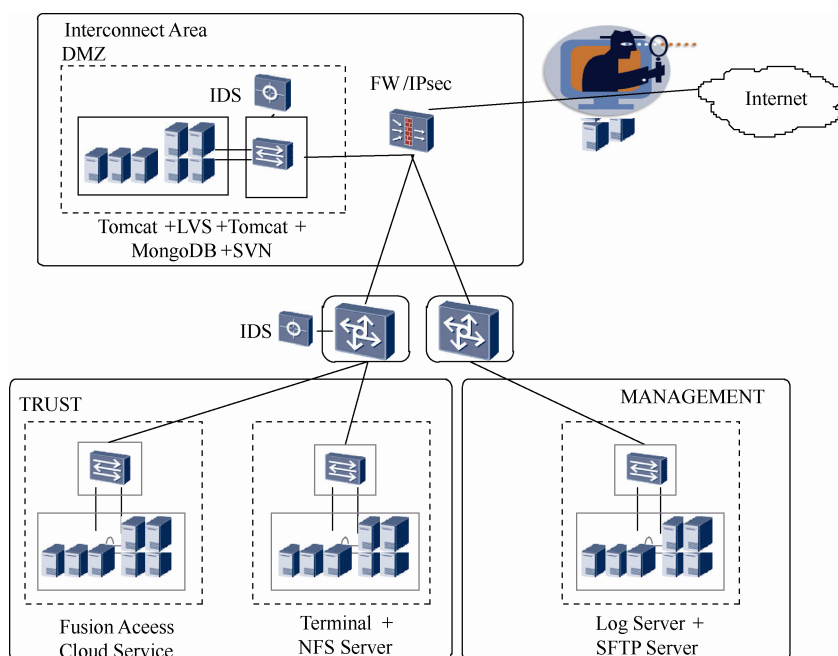


图 5 实验网络拓扑
Figure 5 Topology of experiment network

表 3 主要资产信息
Table 3 Asset information in experimental network

id _e	name _e	type _e	security attribute information _e				config _e		
			conf _e	int _e	avail _e	attrvalue _e	ip _e	port _e	servic _e
de_001	Snort	network	3	3	3	2.197	192.168.200.206	any	snort
de_002	LVS	service	2	3	4	2.393	192.168.200.100	112	lvs keepalived
de_003	Tomcat	service	3	3	4	2.654	192.168.200.101	8 080	tomcat
de_004	MongoDB	service	4	3	4	3.066	192.168.200.102	27 017	mongod
de_005	FA/DNS/AD/DHCP	service	2	3	4	2.393	192.168.100.103	53 389 67 68	dns ldap dhcp
de_006	NFS	service	5	4	5	4.066	192.168.200.104	2 049	rpcbind nfs
de_007	LogServer	service	4	3	3	2.737	192.168.0.105	514	syslog
de_008	SFTPServer	service	4	3	3	2.737	192.168.200.106	22	sftp
de_009	SVN	service	4	4	4	3.197	192.168.200.107	3 690	svn
de_010	Switcher	network	2	3	5	3.115	192.168.200.108	68	dhcp
de_011	FW IPSec	Security network	5	5	5	4.197	124.65.190.74 192.168.0.1 192.168.200.1 192.168.100.1	80 443 21 500 4500 137 2049 445 25 161 22 514 23 389	http https ftp ike ipsec netbios nfs smb smtp snmp ssh syslog telnet ldap

表 4 设备脆弱性
Table 4 The device vulnerabilities

id _e	name _e	type _e	vulnerabilities _e
de_006	NFS	service	CVE-2017-7645
			CVE-2017-7187
			CVE-2017-7494
de_011	FW	Security	Table 2

下面在不同场景中对高安全属性价值设备 de_011 和 de_006 进行威胁态势量化评估实验。

5.1 实验场景

场景 1 互联网流量场景

开放 de_011 设备 Untrust 域公网接口并开放 DMZ 域 Web 服务；在 de_011 设备上做 NAT，将公网 IP 及端口映射至 Web 服务的负载均衡服务。此时，de_011 设备直接暴露给 Internet 用户。de_011 设备接收 Internet 访问流量。

场景 1 测试从 16:00 开始至 19:00 终止。

主要特点：设备直接暴露在 Internet 上后，会有来自不同国家的恶意主机，对设备类型、端口、服务、存活性进行扫描、提权等攻击。

数据获取：从 LogServer 及 SFTP 中获取警报

数据，性能数据通过设备性能命令会话以文件形式记录。

场景 2 测试员在 Internet 侧对 de_011 设备进行模拟攻击

场景 2 在场景 1 的基础上，对 de_011 设备进行模拟攻击，de_011 同时接收 Internet 访问流量和测试员 DOS 攻击流量。

场景 2 测试从 19:00 开始至 21:30 终止。

具体在公网上利用 Nmap^[29]、Netwox^[30]、Kali^[31]分别对 de_011 进行端口、服务扫描，Large ICMP 攻击、Syn flood 和 Udp flood 攻击。

数据获取：从 LogServer 及 SFTP 中获取警报数据，性能数据通过设备命令性能会话以文件形式记录。

场景 3 测试员在内网侧对 de_006 设备攻击

该场景模拟内部用户非授权访问 de_006 文件系统的恶意行为，该场景采用 Nmap 对 de_006 设备的端口及服务开放情况进行扫描，之后试图通过 NFS 通用漏洞提权进入系统，由于该系统已经安装相应补丁，提权失败后发动 Syn flood 和 Udp flood 攻击。

场景3测试从21:30开始至次日0:30终止。

数据获取：利用 Snort^[28]获取警报数据，利用 Nmom^[32]和 Smokeping^[33]采集 Linux 性能数据。

5.2 结果分析

实验获得数据后首先对场景1~场景3的警报数据和性能数据进行对应时间窗口关联，满足警报时间和性能时间的一致性关系，利用 Java 程序和 MongoDB 对警报和性能数据进行入库预处理，满足评估算法要求，然后用本文方法对3个场景的数据进行分析。警报有效性评估结果如图6所示。

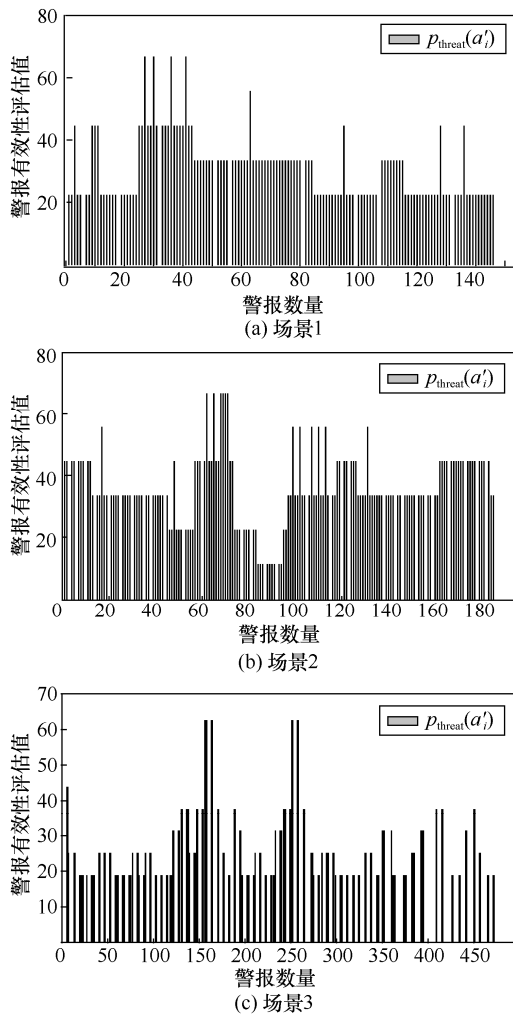


图6 警报有效性评估结果

Figure 6 The results for assessing effectiveness of threat alerts

图6结果表明，本文方法能够以设备的性能、配置、脆弱性为基础，验证威胁警报、计算警报有效性评估值，并通过评估结果反映出威胁对设

备作用的有效程度，具体表现在两个方面。一是算法1能够在大量警报数据中根据设备的属性信息提取出有效警报，从警报数量、警报频率层面评估威胁对设备的作用，警报约减率如表5所示，根据表5计算可得平均约减率为33.04%。有效的警报显式地反映出威胁的数量、频率，以场景1为例，根据表5可知在16:00-19:00这段时间内设备受到有效的可见攻击为26次。二是算法1能够通过警报的评估分值，反映出威胁对设备作用的有效程度。场景1中 de_011 设备在第25、28、33、38个警报的评估分值较高，达到了0.67，主要原因是设备在以上时刻受到不同恶意主机连续对其进行了远程 Telnet 提权攻击，攻击过程使设备网络会话连接、丢包率等性能劣化，导致警报评估分值较高，一定程度上反映出远程 Telnet 提权对设备作用的程度。场景2中 de_011 设备在第63~66警报时刻、第114~119警报时刻评估分值较高，分别达到了0.67和0.44，主要原因是设备分别受到 Syn flood 和 Udp flood 攻击，一定程度上反映出拒绝服务攻击对设备作用的程度。场景3中 de_006 设备在第155~163警报时刻、第250~257警报时刻评估分值较高，达到了0.625，主要原因是设备分别受到 Syn flood 和 Udp flood 攻击，曲线变化反映出拒绝服务攻击对设备作用的程度。

表5 警报约减率
Table 5 Alerts reduction ratio

条目	警报总次数	有效警报次数	警报约减率
场景1	147	26	17.69%
场景2	186	62	33.33%
场景3	472	178	37.71%

图7结果表明，设备性能变化和警报评估分值变化具有一致性。例如，场景1中评估分值较高的第25、28、33、38个警报，对应性能第6个采样周期；场景2中评估分值较高的第63~66警报和第114~119警报，分别对应性能第8个和第12个采用周期；场景3中评估分值较高的第155~163警报和第250~257警报，分别对应性能第18个和第32个采用周期。在有效警报对应的性能周期中均有性能劣化的情况，表明设备性能变化和警报评估分值变化的一致性。

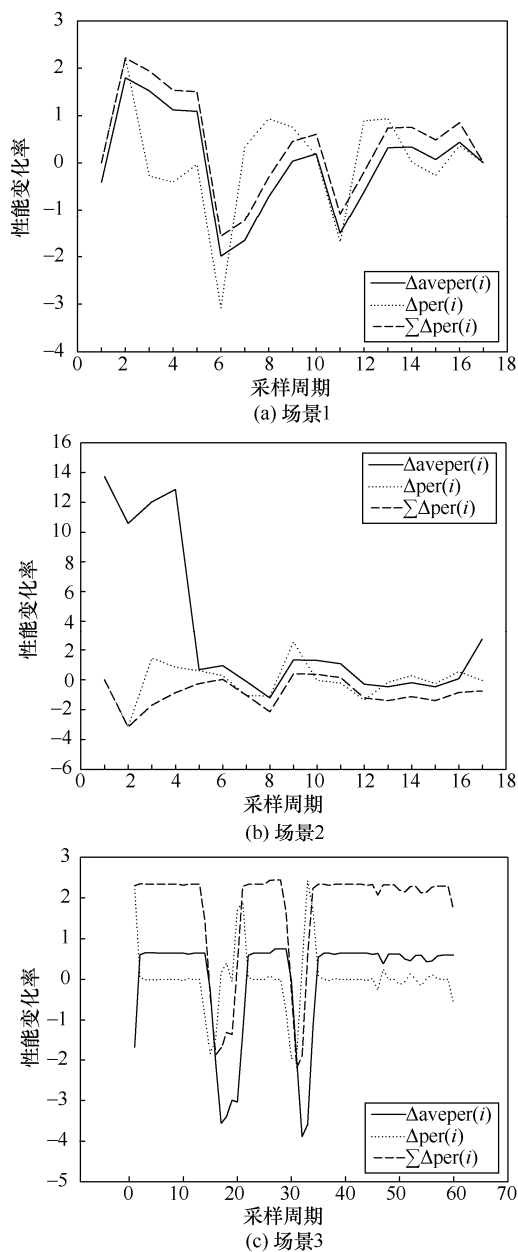


图7 设备性能变化率
Figure 7 The changing ratio of device performance

图8结果表明, 本文方法能够基于警报的有效性评估设备所处安全状态。设备状态评估值、状态特征及状态值如表6所示。表6依据实验中不同攻击类型发生期间对应威胁警报有效性评估值的均值区间界定 threshold 值范围。图8中场景1~场景3的状态变化与设备性能变化(图7)及警报有效性评估图变化(图6)的安全状态相对应, 表现出设备受到威胁后设备所处的安全状态。

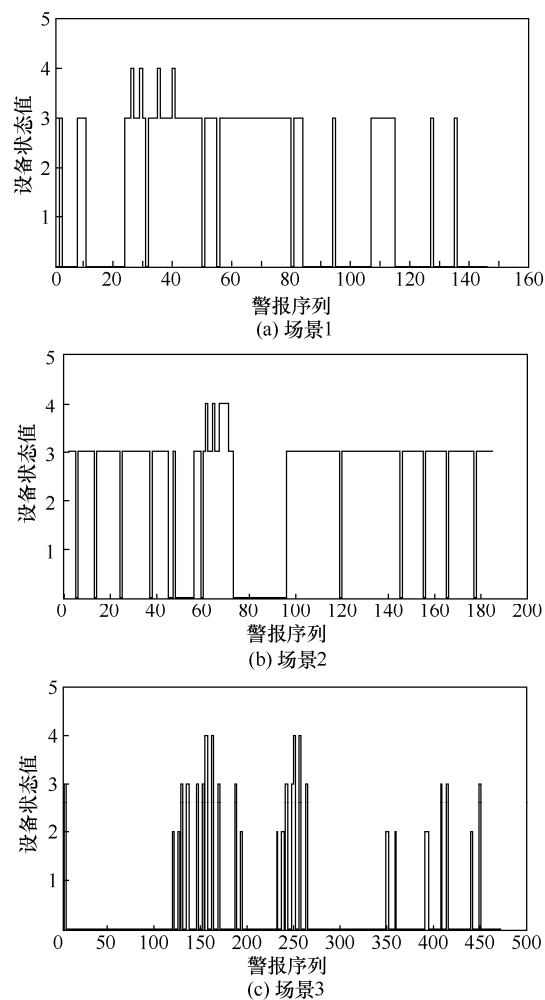


图8 设备威胁态势量化评估
Figure 8 The threat status assessing

表6 设备威胁状态评估值
Table 6 Value of threat status assessing

状态	界定区间	状态特征	状态值
X_0	$p_{\text{threat}}(X_j) < 0.29$	正常	1
X_1	$0.29 \leq p_{\text{threat}}(X_j) < 0.33$	扫描	2
X_2	$0.33 \leq p_{\text{threat}}(X_j) < 0.67$	威胁	3
X_3	$0.65 \leq p_{\text{threat}}(X_j) < 1$	威胁&拒服	4
X_4	$0.65 \leq p_{\text{threat}}(X_j) < 1$	达成目标	5

图9结果表明, 利用本文提出的设备威胁态势量化评估指标和评估方法, 计算得出的设备威胁态势与设备的安全状态对应, 评估结果与实验场景的实际测试一致, 结果能够准确、有效地量化评估设备的威胁态势。在 19:42、20:02、21:02、21:22、22:22 和 22:52 均发生了拒绝服务攻击,

图9中表现出在以上时刻设备具有较高的威胁量化评估值和较高等级的安全状态,并且威胁量化评估值和安全状态趋势相互对应,图形变化与实验场景的模拟攻击行为相符。由此,综合分析图6~图9,本文方法针对高安全属性价值设备,能够以设备性能、配置、脆弱性为基础,验证威胁警报、计算威胁警报的有效概率,评估设备所处安全状态,并利用评估指标准确地评估设备威胁态势。

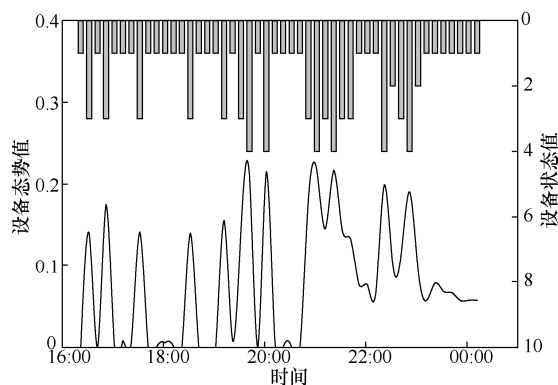


图9 设备威胁态势量化评估

Figure 9 The quantitative threat situational evaluation for device

5.3 对比分析

在介绍本文方法的基础上,本节综合其他评估方法,从不同的角度和本文方法进行对比分析,结果如表7所示。本节比较选择了7个指标,其中,评估对象、属性方法类型、结果形式反映了不同方法针对的评估对象、基于的理论方法及评估结果表现形式;普适程度反映方法应用的通用性;知识来源反映方法本身的客观程度;警报约减和警报聚合反映方法对数据的融合能力。

对比分析如下。

1) 针对网络的评估方法,在网络威胁态势量化评估方面体现出评估结果的宏观性、整体性及趋势性,针对设备的评估方法,能够立足具体设备对确定对象进行评估,评估结果在设备这种微观层面针对性较强,是对网络威胁态势评估在微观层面很好的补充。

2) 在针对设备的威胁评估方法中,本文方法抽象出设备安全属性相关的评估指标,比较文献[18]使用路由器的位置和交换容量来衡量设备对安全风险影响程度的方法更具通用性。

3) 在知识来源方面,本文方法较少地依赖领域专家和经验,评估方式基于概率方式,相比文献[18, 20]利用专家经验赋值环境属性相关度^[18]和威胁发生可能性^[20]的方式,在评估方法的客观程度方面更具有优势。

6 结束语

本文在给出高安全属性价值设备定义的基础上,提出了针对设备的威胁态势量化评估框架和评估指标,并根据评估框架和指标提出了高安全属性价值设备威胁态势量化评估方法。该方法以设备的性能、配置和脆弱性为基础,验证威胁警报、评估威胁警报的有效性。基于有效警报,构建设备状态评估算法,评估设备所处安全状态,并利用评估指标量化计算设备威胁态势,本文所提方法的评估过程、评估结果与网络规模变化不直接构成函数关系,网络规模的变化不影响方法的计算复杂度,体现出较强的网络规模适用性。对具体网络中实际设备的评估结果表明,该方法

表7 威胁态势评估方法比较
Table 7 Comparison of different threat situation assessment methods

评估方法	评估对象	属性	方法类型	结果形式	普适程度	知识来源	警报约减	警报聚合
文献[19]	网络	宏观	分类法	分数	中	概率方式	不支持	支持
文献[17]	网络	宏观	马尔可夫	分数	中	推理方式, 概率方式	不支持	不支持
文献[27]	网络	宏观	权重法	分数	高	领域专家	支持	不支持
文献[18]	网络	宏观	权重法	分数	中	领域专家	支持	不支持
文献[20]	设备	微观	公式法	分数	低	推理方式	不支持	不支持
文献[24]	基础设施	宏观	贝叶斯	分数	中	概率方式	不支持	不支持
本文方法	设备	微观	公式法	分数	高	概率方式	支持	支持

能够准确、有效地量化评估高安全属性价值设备的威胁态势。通过方案对比分析结论表明, 本文方法在应用的通用性及评估结果的客观性方面具有优势。

参考文献:

- [1] 龚正虎, 卓莹. 网络态势感知研究[J]. 软件学报, 2010, 21(7): 1605-1619.
GONG Z H, ZHUO Y. Research on cyberspace situational awareness[J]. Journal of Software, 2010, 21(7): 1605-1619.
- [2] CYRIL O. Understanding cyber situation awareness[J]. International Journal on Cyber Situational Awareness, 2016, 1(1): 11-30.
- [3] BLASCH E, PLANO S. JDL level 5 issues supporting situational assessment reasoning[C]//Proc of the Signal Processing, Sensor Fusion, and Target Recognition XI (SPIE). 2002: 270-279.
- [4] ENDSLEY M. Situation awareness global assessment technique (SAGAT)[C]//Proc of the IEEE'88 National Aerospace and Electronics Conf. 1988: 789-795.
- [5] AGGARWAL P, GONZALEZ C, DUTT V. Cyber-security: role of seception in cyber-attack detection[C]//International Conference on Applied Human Factors and Ergonomics. 2016: 85-96
- [6] SUN X, DAI J, LIU P, et al. Towards probabilistic identification of zero-day attack paths[J]. Communications and Network Security. 2017: 64-72.
- [7] ZHANG H, YAO D, RAMAKRISHNAN N, et al. Causality reasoning about network events for detecting stealthy malware activities[J]. Computers & Security, 2016, 58(C): 180-198.
- [8] SHAO P, LU J, WONG R K, et al. A transparent learning approach for attack prediction based on user behavior analysis[C]//International Conference on Information and Communications Security. 2016: 159-172.
- [9] 刘效武, 王慧强, 吕宏武, 等. 网络安全态势认知融合感控模型[J]. 软件学报, 2016, 27(8): 2099-2114.
LIU X W, WANG H Q, LYU H W, et al. Fusion-based cognitive awareness-control model for network security situation[J]. Journal of Software, 2016, 27(8): 2099-2114.
- [10] 文志诚, 陈志刚, 唐军. 基于信息融合的网络安全态势量化评估方法[J]. 北京航空航天大学学报, 2016, 42(8): 1593-1602.
WEN Z C, CHEN Z Q, TANG J. Assessing network security situation quantitatively based on information fusion[J]. Journal of Beijing University of Aeronautics and Astronautics, 2016, 42(8): 1593-1602.
- [11] 赵淦森, 吴杰超, 陈梓豪, 等. 网络空间安全态势感知研究[J]. 网络与信息安全学报. 2016, 2(10): 29-35.
ZHAO G S, WU J C, CHEN Z H, et al. Research on security situation awareness in cyberspace [J]. Journal of Network and Information Security. 2016, 2(10): 29-12.
- [12] 朱承, 缪嘉嘉, 毛捍东. 面向行为的内网空间安全态势建模与分析[J]. 网络与信息安全学报. 2016, 2(8): 17-22.
ZHU C, MIU J J, MAO H D. Behavior-oriented intranet space security situation modeling and analysis[J]. Journal of Network and Information Security. 2016, 2(8): 17-22
- [13] ELIAS B H, MARTIN H, MOURAD D, et al. Big data sanitization and cyber situational awareness: a network telescope perspective[J]. IEEE Transactions on Big Data, 2017, 99: 1-8.
- [14] MIN D, LEI F F, ZHENG G N, et al. DeepLog: anomaly detection and diagnosis from system logs through deep learning[C]//ACM Sigsac Conference(CCS'17). 2017: 1285-1298.
- [15] 寇广, 王硕, 张达. 基于深度堆栈编码器和反向传播算法的网络安全态势要素识别[J]. 电子与信息学报, 2019, 41(9): 2187-2193.
KOU G, WANG S, ZHANG D. Recognition of network security situation elements based on depth stack encoder and back propagation algorithm[J]. Journal of Electronics & Information Technology, 2019, 41(9): 2187-2193.
- [16] 程家根, 祁正华, 陈天赋. 基于 RBF 神经网络的网络安全态势感知[J]. 南京邮电大学学报(自然科学版), 2019, 39(4): 88-95.
CHENG J G, QI Z H, CHEN T F. Network security situation awareness based on RBF neural networks[J]. Journal of Njing University of Posts an Telecommunications(Natural Science Edition), 2019, 39(4): 88-95.
- [17] 张勇, 谭小彬, 崔孝林, 等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报, 2011, 22(3): 495-508.
ZHANG Y, TAN X B, CUI X L, et al. Network security situation awareness approach based on Markov game model[J]. Journal of Software, 2011, 22(3): 495-508.
- [18] 席荣荣, 云晓春, 张永铮. 一种改进的网络安全态势量化评估方法[J]. 计算机学报, 2015, 38(4): 749-758.
XI R R, YUN C X, ZHANG Y Z. An improved quantitative evaluation method for network security[J]. Chinese Journal of Computers, 2015, 38(4): 749-758.
- [19] 杨豪璞, 邱辉, 王坤. 面向多步攻击的网络安全态势评估方法[J]. 通信学报, 2017, 38(1): 187-198.
YANG H P, QIU H, WANG K. Network security situation evaluation method for multi-step attack[J]. Journal on Communication. 2017, 38(1): 187-198.
- [20] 杨君刚, 梁礼, 刘故箐, 等. 在线监测的路由器安全威胁态势量化评估方法[J]. 通信学报, 2013, 34(11): 59-70.
YANG J G, LING L, LIU G J, et al. Method for router online security risk assessment quantification[J]. Journal on Communications. 2013, 34(11): 59-70.
- [21] YU B L, ALI A K, SELVAKUMAR M, et al. An adaptive assessment and prediction mechanism in network security situation awareness[J]. Journal of Computer Sciences, 2017, 13 (5): 114-129.
- [22] CRISTINA A J. Wide-area situational awareness for critical infrastructure protection[J]. IEEE Computer, 2013, 46(4): 30-37.
- [23] CRISTINA A, SHERALI Z. Critical infrastructure protection:

requirements and challenges for the 21st century[J]. International Journal of Critical Infrastructure Protection. 2015, 8: 53-56.

- [24] CEEMAN V, ANURAG S, SAMAN Z. CPIndex: cyber-physical vulnerability assessment for power-grid Infrastructures[J]. IEEE Transactions on Smart Grid, 2017, 6 (2): 566-575.
- [25] 国家信息中心. GB/T 20984-2007 信息安全技术信息安全风险评估规范[S]. 北京: 中国标准出版社, 2007.
- Nation Informatics Centre. GB/T 20984-2007 Information security technology-Risk assessment specification for information security[S]. Beijing: Standards Press of China, 2007.
- [26] CVSS-Common Vulnerability Scoring System[EB].
- [27] 韦勇, 连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报, 2009, 32(4): 763-772.
- WEI Y, LIAN Y F. A network security situational awareness model based on log audit and performance correction[J]. Chinese Journal of Computers, 2009, 32(4): 763-772.
- [28] Snort-the open source network intrusion detection system[EB].
- [29] Nmap-free security scanner for network[EB].
- [30] Netwox-a toolbox for network[EB].
- [31] Kali linux-a Debian-derived linux distribution designed for digital forensics and penetration testing[EB].
- [32] Nmon-the linux system performance tools[EB].
- [33] Smokeping-a toolbox for tracking of your network latency[EB].

[作者简介]



韩磊 (1983-), 男, 内蒙古呼伦贝尔人, 博士(后), 北京计算机技术及应用研究所高级工程师, 主要研究方向为信息安全、密码应用、智能安全。



刘吉强 (1973-), 男, 山东烟台人, 博士, 北京交通大学教授、博士生导师, 主要研究方向为可信计算、隐私保护、云计算安全。



王健 (1975-), 男, 山东烟台人, 博士, 北京交通大学副教授, 主要研究方向为密码应用及区块链、网络安全。



石波 (1988-), 男, 江苏南通人, 北京计算机技术及应用研究所高级工程师, 主要研究方向为信息安全。



和旭东 (1993-), 男, 河北保定人, 北京交通大学博士生, 主要研究方向为网络安全、物联网安全。