(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108881157 B
(45)授权公告日 2021.01.22

(21)申请号 201810420755.5

(22)申请日 2018.05.04

(65)同一申请的已公布的文献号
申请公布号 CN 108881157 A

(43)申请公布日 2018.11.23

(73)专利权人 国家计算机网络与信息安全管理中心
地址 100029 北京市朝阳区裕民路甲3号
专利权人 北京理工大学

(72)发明人 杨鹏 黄元飞 王鹏翩 李燕伟 罗森林 潘丽敏 郝靖伟 胡雅娴

(74)专利代理机构 北京华夏泰和知识产权代理有限公司 11662
代理人 陈英

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 105072045 A,2015.11.18
CN 106992904 A,2017.07.28
CN 102799822 A,2012.11.28
US 2017238056 A1,2017.08.17
CN 107610765 A,2018.01.19
CN 106027516 A,2016.10.12

审查员 刘金鑫

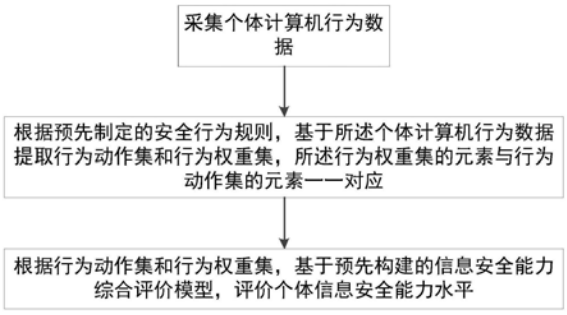
权利要求书3页 说明书10页 附图1页

(54)发明名称

一种基于PC终端行为的个体信息安全能力评价方法及系统

(57)摘要

本发明提出的一种基于PC终端行为的个体信息安全能力评价方法及系统，通过对个体计算机行为数据的客观评测，来确定个体信息安全能力，解决了现有评价方法单一、评价全面性不足的问题，不仅考虑到个体的主观意识，更着重考虑到更重要的客观行为对本体分析的重要性，能够更加真实的反映用户的信息安全能力。



CN 108881157 B

1.一种基于PC终端行为的个体信息安全能力评价方法,其特征在于,包括:

采集个体计算机行为数据;

根据预先制定的安全行为规则,基于所述个体计算机行为数据提取行为动作集和行为权重集,所述行为权重集的元素与行为动作集的元素一一对应;

根据行为动作集和行为权重集,基于预先构建的信息安全能力综合评价模型,评价个体信息安全能力水平;

所述安全行为规则,如下所示:

SBR::=\{Action,Rule\}

其中,SBR表示安全行为规则,Action表示用户安全行为,Rule表示推理规则集,用来对用户安全行为进行安全性识别;

其中,所述根据行为动作集和行为权重集,基于预先构建的信息安全能力综合评价模型,评价个体信息安全能力水平,包括:

所述预先构建的信息安全能力综合评价模型包括本征力、警觉力和学习力,根据行为动作集和行为权重集,计算个体的本征力、警觉力和学习力;

根据个体的本征力、警觉力和学习力,确定个体信息安全能力水平;

其中,根据动作集和行为权重集,计算个体的本征力的公式如下所示:

$Instinctive(u)=Action(u)*Alpha^{T}(u)$

其中,u表示用户,Instinctive(u)表示用户u的本征力,Action表示用户u的行为动作集,$Alpha^{T}(u)$用户u的行为权重集的转置;

其中,所述根据动作集和行为权重集,计算个体的警觉力的计算公式如下所示:

$$Alertness(u)=\frac{1}{1+\frac{\sum_{i=1}^{n}Right(S_i)}{Sum_j(u)}}$$

其中,Alertness(u)表示用户u的警觉力,$Sum_j(u)$表示用户u所产生的第j类不安全动作的总数,S_i表示第i种存在的不安全行为的总数,Right(S_i)表示第i种存在的不安全行为的总数S_i的带权综合长度,n表示存在n种不安全行为;

所述Right(S_i)的计算公式如下所示:

$$Right(Si)=\sum_{k=1}^{l}\sum_{i=1}^{n}I\{a_k\in S_i\wedge a_k\in b_i\}a_i$$

其中,I表示指示函数,当I\{true\}=1,I\{false\}=0,true和false表示个体计算机行为数据的安全特征,根据安全行为规则确定,true用于表示安全取值为0,false表示不安全取值为1,a_k表示行为动作集中第k个元素,a_i表示行为动作集中第i个元素,b_i为行为权重集中第i个元素,l表示行为动作集的元素总数,n表示行为权重集的元素总数,l=n都和存在的安全行为总数相同;

其中,所述根据动作集和行为权重集,计算个体的学习力的计算公式如下所示:

$$Learning(u)=\frac{1}{1+\frac{\sum_{i=1}^{n}a_iR_i(u)}{sum(u)}}$$

其中，Learning(u)表示用户u的学习力，Sum(u)表示用户u所产生的不安全动作的总数，$R_i(u)$表示用户u第i种不安全动作发生重复的次数，a_i表示行为动作集中第i个元素，n表示存在n种不安全行为；

其中，所述根据个体的本征力、警觉力和学习力，确定个体信息安全能力水平，包括：

根据个体的本征力、警觉力和学习力按下式计算个体信息安全能力水平：

$$\text{Ability}(u)=\varphi\,\text{Instinctive}(u)+\lambda\,\text{Alertness}(u)+\eta\,\text{Learning}(u)$$

其中，Ability(u)表示用户u的信息安全能力水平，Instinctive(u)表示用户u的本征力，Alertness(u)表示用户u的警觉力，Learning(u)表示用户u的学习力，φ、λ、η均为可调参数。

2.根据权利要求1所述的个体信息安全能力评价方法，其特征在于，采个体计算机行为数据，包括：

通过全局事件监听接口和行为监听方法采集个体计算机行为数据；

将采集到的个体计算机行为数据的数据格式转换为符合安全行为规则提取的格式。

3.根据权利要求1所述的个体信息安全能力评价方法，其特征在于，根据所述个体计算机行为数据和预先制定的安全行为规则，提取行为动作集和行为权重集，包括：

根据预先制定的安全行为规则，量化个体计算机行为数据；

根据量化后的个体计算机行为数据，得到用于表示个体计算机行为数据的安全特征的行为动作集；

基于个体计算机行为数据，通过德尔菲专家咨询法，得到与行为动作集对应的行为权重集。

4.根据权利要求1-3任一所述的个体信息安全能力评价方法，其特征在于，所述个体计算机行为数据包括：计算机防火墙信息、用户密码配置信息、注册表配置信息、网络配置信息、系统配置信息、软件安全配置信息和日志信息。

5.一种基于PC终端行为的个体信息安全能力评价系统，其特征在于，用于执行如权利要求1所述的基于PC终端行为的个体信息安全能力评价方法，包括：

采集模块，用于采集个体计算机行为数据；

提取模块，用于根据预先制定的安全行为规则，基于所述个体计算机行为数据提取行为动作集和行为权重集，所述行为权重集的元素与行为动作集的元素一一对应；

评价模块，用于根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平。

6.根据权利要求5所述的个体信息安全能力评价系统，其特征在于，所述提取模块根据所述个体计算机行为数据和预先制定的安全行为规则，提取行为动作集和行为权重集，包括：

根据预先制定的安全行为规则，量化个体计算机行为数据；

根据量化后的个体计算机行为数据，得到行为动作集；

基于个体计算机行为数据，通过德尔菲专家咨询法，得到行为权重集。

7.根据权利要求5所述的个体信息安全能力评价系统，其特征在于，所述评价模块根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平，包括：

所述预先构建的信息安全能力综合评价模型包括本征力、警觉力和学习力，根据行为动作集和行为权重集，计算个体的本征力、警觉力和学习力；

根据个体的本征力、警觉力和学习力，确定个体信息安全能力水平。

一种基于PC终端行为的个体信息安全能力评价方法及系统

技术领域

[0001] 本发明实施例涉及信息安全能力评价技术领域，具体涉及一种基于PC终端行为的个体信息安全能力评价方法及系统。

背景技术

[0002] 随着网络安全事件日益频发，社会工程学在网络攻击中广泛使用，个体信息安全能力的重要性逐渐提升。个体信息安全能力淡薄，对于PC终端存在的问题，如对密码设定不合理、防火墙开启、端口开放设置不当等，给个人、企业带来了极大的信息安全风险。2003年Donner提出了安全本体，并将其定义为“在信息系统中，描述与安全相关的概念以及这些概念之间相互关系的一种本体”。随着移动办公模式的兴起，BYOD(bring your own device)模式提高了工作效率的同时也引入了安全隐患。对个体的信息安全能力的客观评价就显得尤为重要。

[0003] 目前在信息安全评价中主要着眼于评价设备、方法、系统的信息安全能力，缺少以人为对象的个体信息安全能力评价方法，而个体的不安全行为是组织内信息安全事件频发的一个重要原因，对组织内个体进行信息安全能力评价是进行安全意识教育、构建安全防护体系、实现安全生产的重要环节和必要保障。现有的PC终端用户行为安全能力检测或评价方法可分为以下3种：问卷调查法、在线测验法和严肃游戏法。

[0004] 1.问卷调查法

[0005] 问卷调查法是目前个体信息安全能力评价的主要方法。常见做法是发放调查问卷。采用问卷调查的方式对企业人员进行信息安全知识与行为方面的调查，采用确定因子分析的方法对结果进行分析，发现仅从安全知识层面不足以充分检测PC终端用户的安全能力，可见行为因素会发挥重要作用。或者通过向调查者发送钓鱼邮件的方式，观察检测对象的应对行为，进一步验证了安全意识与安全行为具有强关联性。但这类研究方法受问卷题目容量、行为采集技术的限制，导致其研究范围较窄且效率较低，主观性较强，忽略了客观行为因素特征，影响了评价结果的客观性和准确性。

[0006] 2.在线测验法

[0007] 针对问卷调查的缺陷，设计实现了信息安全评测及能力促进系统(MEERKAT)。通过试题测试的方式，确认个体信息安全水平的高低，并向用户推荐能够强化训练其认知短板的针对性学习内容。但是，该类方法的问题是：即使个体在测试中有较高的信息安全素养，但在其实际活动中是否能将这些安全意识落实到具体行为中也是难以保证的，同时在测试或填写调查问卷等有感条件下，用户会有意识地根据试题进行准备与针对性的应对，难以反映用户安全意识的真实落实情况。

[0008] 3.严肃游戏法

[0009] 为了解决在真实场景下搜集用户数据、检测用户不安全行为等难题，严肃游戏(serious game)技术被引入到个体信息安全能力教育和技能培养中。最初被定义为“以应用为目的的游戏”，具体来讲，是指以那些以教授知识技巧、提供专业训练和模拟为主要内

容的游戏。比如美国NPS中心联合Rivermind公司开发的CyberCIEGE，该平台能够通过在线游戏的方式给出参与者在信息安全能力方面的评级或者具体分数。但该类方法的不足在于只针对某项技能进行训练，不能很好地适应当前层出不穷的安全风险，且开发代价较高。

[0010] 综上所述，当前PC终端行为的个体信息安全能力评价研究尚存在主观性强，用户行为安全性分析形式化描述缺失，调查问卷或测试的内容固定，难以检测不同场景下用户应对复杂多变的安全威胁的能力等问题。

发明内容

[0011] 为了解决上述技术问题或者至少部分地解决上述技术问题，本发明实施例提供了一种基于PC终端行为的个体信息安全能力评价方法。

[0012] 有鉴于此，第一方面，本发明实施例提供一种基于PC终端行为的个体信息安全能力评价方法，包括：

[0013] 采集个体计算机行为数据；

[0014] 根据预先制定的安全行为规则，基于所述个体计算机行为数据提取行为动作集和行为权重集，所述行为权重集的元素与行为动作集的元素一一对应；

[0015] 根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平。

[0016] 采个体计算机行为数据，包括：

[0017] 通过全局事件监听接口和行为监听方法采集个体计算机行为数据；

[0018] 将采集到的个体计算机行为数据的数据格式转换为符合安全行为规则提取的格式。

[0019] 根据所述个体计算机行为数据和预先制定的安全行为规则，提取行为动作集和行为权重集，包括：

[0020] 根据预先制定的安全行为规则，量化个体计算机行为数据；

[0021] 根据量化后的个体计算机行为数据，得到用于表示个体计算机行为数据的安全特征的行为动作集；

[0022] 基于个体计算机行为数据，通过德尔菲专家咨询法，得到与行为动作集对应的行为权重集。

[0023] 所述安全行为规则，如下所示：

[0024] SBR::＝{Action,Rule}

[0025] 其中，SBR表示安全行为规则，Action表示用户安全行为，Rule表示推理规则集，用来对用户安全行为进行安全性识别。

[0026] 根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平，包括：

[0027] 所述预先构建的信息安全能力综合评价模型包括本征力、警觉力和学习力，根据行为动作集和行为权重集，计算个体的本征力、警觉力和学习力；

[0028] 根据个体的本征力、警觉力和学习力，确定个体信息安全能力水平。

[0029] 根据动作集和行为权重集，计算个体的本征力的公式如下所示：

[0030] $Instinctive(u)＝Action(u)*Alpha^{T}(u)$

[0031] 其中，u表示用户，Instinctive(u)表示用户u的本征力，Action表示用户u的行为动作集，$Alpha^T$(u)用户u的行为权重集的转置。

[0032] 根据动作集和行为权重集，计算个体的警觉力的计算公式如下所示：

[0033] $$Alertness\ (u)=\frac{1}{1+\frac{\sum_{i=1}^{n}Right\ (S_i)}{Sum_j(u)}}$$

[0034] 其中，Alertness(u)表示用户u的警觉力，Sum_j(u)表示用户u所产生的第j类不安全动作的总数，S_i表示第i种存在的不安全行为的总数，Right(S_i)表示第i种存在的不安全行为的总数S_i的带权综合长度，n表示存在n种不安全行为；

[0035] 所述Right(S_i)的计算公式如下所示：

[0036] $$Right\ (Si)=\sum_{k=1}^{l}\sum_{i=1}^{n}I\{a_k\in S_i\ \wedge\ a_k\in b_i\}a_i$$

[0037] 其中，I表示指示函数，当I{true}＝1，I{false}＝0，true和false表示个体计算机行为数据的安全特征，根据安全行为规则确定，true用于表示安全取值为0，false表示不安全取值为1，a_k表示行为动作集中第k个元素，a_i表示行为动作集中第i个元素，b_i为行为权重集中第i个元素，l表示行为动作集的元素总数，n表示行为权重集的元素总数，l＝n都和存在的安全行为总数相同。

[0038] 8、根据权利要求5所述的个体信息安全能力评价方法，其特征在于，根据动作集和行为权重集，计算个体的学习力的计算公式如下所示：

[0039] $$Learning\ (u)=\frac{1}{1+\frac{\sum_{i=1}^{n}a_iR_i(u)}{sum(u)}}$$

[0040] 其中，Learning(u)表示用户u的学习力，Sum(u)表示用户u所产生的不安全动作的总数，R_i(u)表示用户u第i种不安全动作发生重复的次数，a_i表示行为动作集中第i个元素，n表示存在n种不安全行为。

[0041] 根据个体的本征力、警觉力和学习力，确定个体信息安全能力水平，包括：

[0042] 根据个体的本征力、警觉力和学习力按下式计算个体信息安全能力水平：

[0043] $$Ability\ (u)=\varphi\ Instinctive\ (u)+\lambda\ Alertness\ (u)+\eta\ Learning\ (u)$$

[0044] 其中，Abil ity(u)表示用户u的信息安全能力水平，Instinctive(u)表示用户u的本征力，Alertness(u)表示用户u的警觉力，Learning(u)表示用户u的学习力，φ、λ、η均为可调参数。

[0045] 所述个体计算机行为数据包括：计算机防火墙信息、用户密码配置信息、注册表配置信息、网络配置信息、系统配置信息、软件安全配置信息和日志信息。

[0046] 第二方面，本发明实施例提供一种基于PC终端行为的个体信息安全能力评价系统，包括：

[0047] 采集模块，用于采集个体计算机行为数据；

[0048] 提取模块，用于根据预先制定的安全行为规则，基于所述个体计算机行为数据提取行为动作集和行为权重集，所述行为权重集的元素与行为动作集的元素一一对应；

[0049] 评价模块，用于根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平。

[0050] 所述提取模块根据所述个体计算机行为数据和预先制定的安全行为规则，提取行为动作集和行为权重集，包括：

[0051] 根据预先制定的安全行为规则，量化个体计算机行为数据；

[0052] 根据量化后的个体计算机行为数据，得到行为动作集；

[0053] 基于个体计算机行为数据，通过德尔菲专家咨询法，得到行为权重集。

[0054] 所述评价模块根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平，包括：

[0055] 所述预先构建的信息安全能力综合评价模型包括本征力、警觉力和学习力，根据行为动作集和行为权重集，计算个体的本征力、警觉力和学习力；

[0056] 根据个体的本征力、警觉力和学习力，确定个体信息安全能力水平。

[0057] 第三方面，本发明实施例还提出一种非暂态计算机可读存储介质，所述非暂态计算机可读存储介质存储计算机指令，所述计算机指令使所述计算机执行如第一方面所述方法的步骤。

[0058] 相比现有技术，本发明实施例提出的一种基于PC终端行为的个体信息安全能力评价方法，通过对个体计算机行为的客观评测，来确定个体信息安全能力，解决了现有评价方法单一、评价全面性不足的问题，不仅考虑到个体的主观意识，更着重考虑到更重要的客观行为对本体分析的重要性，能够更加真实的反映用户的信息安全能力；

[0059] 相比于问卷调查法，本发明不受问卷题目容量、行为采集技术的限制，展宽了研究范围且极大地提高了测试效率，充分降低了主观因素的影响，提高了PC终端用户安全能力评价模型的客观性和准确性。

[0060] 相比于在线测验法，本发明克服了有感条件下，用户有意识地根据试题进行准备与针对性的应对的情况，可以真实的反映用户的安全意识落实情况，对个体信息安全能力的评价结果更加科学。

[0061] 相比于严肃游戏法，本发明不只针对某项技能进行训练，可以很好地适应当前层出不穷的安全风险，降低了开发成本。

附图说明

[0062] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0063] 图1为本发明提供的一种基于PC终端行为的个体信息安全能力评价方法流程图；

[0064] 图2为本发明实施例提供的一种基于PC终端行为的个体信息安全能力评价系统示意图。

具体实施方式

[0065] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例

中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0066] 参照图1，图1为本发明一个实施例提供的一种基于PC终端行为的个体信息安全能力评价方法，可包括以下步骤：

[0067] 采集个体计算机行为数据；

[0068] 根据预先制定的安全行为规则，基于所述个体计算机行为数据提取行为动作集和行为权重集，所述行为权重集的元素与行为动作集的元素一一对应；

[0069] 根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平。

[0070] 采集个体计算机行为数据，可以包括：

[0071] 步骤1.1，在个体无感状态下，利用Windows系统自身提供的全局事件监听API和自主开发的行为监听方法采集数据，采集个体计算机防火墙、用户级密码配置信息、注册表配置信息、网络配置信息、系统配置信息、软件安全配置信息和日志信息。

[0072] 步骤1.2，对采集到的数据进行预处理，使其数据格式符合下一步安全行为规则提取。

[0073] 根据预先制定的安全行为规则，基于所述个体计算机行为数据提取行为动作集和行为权重集，可以包括：

[0074] 步骤2.1，定义安全行为规则(SBR,security behavior rules)由用户安全行为和推理规则集构成，其形式化定义为SBR::＝{Action,Rule}其中，Action表示用户安全行为，用来描述收集到的行为特征及其之间关系，Rule表示推理规则集，用来关联用户安全行为并进行安全性识别，如防火墙关闭、用户密码设置未开启，密码复杂度较低、注册表访问权限。

[0075] 步骤2.2，定义个体在使用个人计算机过程中存在的典型不安全行为。如防火墙未开启、防火墙所处网站(public/private)、允许远程连接、有未启用的管理员账号，多个未启用的guest账号、有未启用网卡、共享文件夹开启、web安全等级低、系统服务数目过多以及UAC关闭等。

[0076] 步骤2.3，分别量化定义用户u的各个特征，行为动作集Action(u)＝{a_1,a_2,…a_k…a_l}，行为权重集为Alpha(u)＝{b_1,b_2,…b_k…b_l}；

[0077] 行为动作集元素的设定，例如：规定有未开启的防火墙为false＝1，防火墙全部开启为true＝0，UAC关闭为false＝1，UAC开启为true＝0，共享文件夹开启为true＝1，共享文件夹关闭为false＝0，用户密码永不过期为true＝1，非永不过期为false＝0等。

[0078] 根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平，可以包括：

[0079] 提出了一种信息安全能力综合评价模型，获得评价个体PC终端行为的信息安全能力的三大要素：本征力，警觉力，学习力，得出PC终端用户个体安全能力评测值。

[0080] 所述本征力用于表示避免发生不安全行为的能力；

[0081] 所述警觉力用于表示对不安全行为发生的警觉能力；

[0082] 所述学习力用于表示提升安全防范，避免重复发生不安全行为的能力。

[0083] 步骤3.1获取PC终端个体的本征力,用户u的本征力计算公式为:

[0084] $Instinctive(u)=Action(u)*Alpha^{T}(u)$ (1)

[0085] 步骤3.2获取PC终端个体的警觉力,本发明用每种不安全行为的总数来衡量用户的警觉性,用户u的警觉力计算公式为:

[0086] $$Alertness(u)=\frac{1}{1+\frac{\sum_{i=1}^{n}Right(S_i)}{Sum_j(u)}} \quad (2)$$

[0087] 其中,$Sum_j(u)$表示用户所产生的第j类不安全行为总数,$Right(S_i)$表示不安全行为总数S_i的带权综合长度,计算公式为:

[0088] $$Right(Si)=\sum_{k}^{t}\sum_{i}^{n}I\{a_k \in S_i \wedge a_k \in b_i\}a_i \quad (3)$$

[0089] 比较步骤2.3,记指示函数I{true}=1,I{false}=0。

[0090] 步骤3.3获取PC终端个体的学习力,识别不安全行为是否被用户重复执行,并通过其中包含的行为来确定所属动作类型,以确定权重,PC终端个体学习力的计算公式为:

[0091] $$Learning(u)=\frac{1}{1+\frac{\sum_{i=1}^{n}a_iR_i(u)}{sum(u)}} \quad (4)$$

[0092] 步骤3.4本征力、警觉力和学习力共同构成PC终端用户安全能力评测值,通过下式计算个体信息安全能力水平Ability:

[0093] $$Ability(u)=\varphi\ Instinctive(u)+\lambda\ Alertness(u)+\eta\ Learning(u) \quad (5)$$

[0094] 其中,φ、λ、η为3个可调参数。

[0095] 在一个具体的例子中,

[0096] 以北京理工大学信息与电子学院BFS实验室30名学生为实验对象,使用C++语言实现了一个原型系统信息安全意识评估系统,客户端实验可以进行个人计算机行为扫描,利用Windows系统自身提供的全局事件监听API和自主开发的行为监听方法采集数据,包括(1)采集个体计算机防火墙信息、用户级密码配置信息、注册表配置信息、网络配置信息、系统配置信息、软件安全配置信息和日志信息;(2)针对包含是否开启防火墙等的PC端数据(2200维)属性进行量化处理,使其符合安全规则提取格式;(3)通过公式计算出本征力、警觉力和学习力以及专家经验设置参数值,共同得出每位PC终端用户的安全能力评测值。

[0097] 具体流程为:

[0098] 步骤1,对北京理工大学信息与电子学院BFS实验室30名学生在无感状态下,利用Windows系统自身提供的全局事件监听API和自主开发的行为监听方法采集数据,采集个体计算机防火墙、用户级密码配置信息、注册表配置信息、网络配置信息、系统配置信息、软件安全配置信息和日志信息,下表显示了采集PC端个体安全配置具体内容。

[0099]

安全配置	功能简述
防火墙配置	防火墙配置信息采集主要用于收集防火墙开启情况，所处网络和出入站规则的具体数据，并以 XML 格式输出
密码配置	实现对用户 PC 端数据配置情况的采集，其中主要获取的信息有所有用户的密码开启情况、用户密码强度、Guest 用户是否启用以及 Admin 用户数量的具体数据，并以 XML 格式输出。
注册表配置	采集注册表关键项取值、注册表键值权限设置、注册表远程访问设置、等信息。
网络配置	采集网络配置信息如端口开放信息，文件共享设置，地址解析协议，即 ARP（Address Resolution Protocol）设置的详细信息，并以 XML 格式输出数据。
浏览器配置	系统可以获取浏览器的安全设置比如本地 Internet 区域、受信任的站点区域、Internet 区域、受限制的站点区域的安全级别以及浏览器 SmartScreen 筛选器是否开启的状态信息，并以 XML 格式输出数据。
系统配置	系统配置信息主要包括系统重要服务组件，系统组策略设置等关键信息。收集到的数据以 XML 的格式输出。
软件配置	获取用户 Windows 系统中杀毒软件的安装内容和开启状态、WindowsSmartScreen 状态是否处于默认状态、PC 端 UAC 开启/关闭状态信息
日志信息	获取系统日志包括操作系统日志、应用程序日志和安全日志

[0100] 步骤2，安全行为规则提取，规定有未开启的防火墙为false＝1，防火墙全部开启为true＝0，UAC关闭为false＝1，UAC开启为true＝0，共享文件夹开启为true＝1，共享文件夹关闭为false＝0，用户密码永不过期为true＝1，非永不过期为false＝0等，原型系统获取了2017年11月10日～2017年11月15日期间共计30条行为数据，每条行为数据包括2200余维。

[0101] 步骤3，获取PC终端个体的本征力，根据式(1)并结合德尔菲专家咨询法，将计算机防火墙、用户级密码配置信息、注册表配置信息、网络配置信息、系统配置信息、软件安全配置信息和日志信息设置行为权重依次确定为0.15、0.15、0.05、0.15、0.25、0.2、0.05，行为动作集的元素a_1～a_7的取值基于不安全行为规则，根据具体情况来确定，得到Instinctive

(u_1)～Instinctive(u_{30})。

[0102] 步骤4,获取PC终端个体的警觉力,7类行为的权重与式(1)中相同,通过统计得到不安全防火墙行为、用户密码行为、注册表配置行为、网络配置行为,系统配置行为、软件安全行为、日志安全行为的总深度与各类型的不安全行为总数,得到Alertness(u_1)～Alertness(u_{30})。

[0103] 步骤5,获取PC终端个体的学习力,计算出每个个体的不同不安全行为重复发生的次数,各类型行为的权重取值与式(1)中相同,将相似度阈值$\delta \geq 0.6$的行为归为一类,并计算各类行为的重复度,计算得到每个用户的学习能力值Learning(u_1)～Learning(u_{30}).

[0104] 步骤6,通过公式计算出本征力、警觉力和学习力以及专家经验设置参数值Φ、λ、η,得出每位PC终端用户的安全能力评测值Ability(u_1)～Ability(u_{30})。

[0105] 测试结果:本发明通过PC端多源、多类型、多精度的安全数据采集,能够检测用户真实存在的不安全PC端的客观行为;通过构造安全行为规则,完成了多类型行为的统一表示与形式化规则描述;通过构造行为规则集,解决了动态行为分析问题;通过构建信息安全能力评估模型,完成了安全能力的定量评估,客观展现出用户的信息安全能力级别。对这些具体的不安全行为进行解析,可以发现部分用户在密码设置、共享文件夹以及系统服务数目和UAC是否关闭识别上的警觉性不足,不能及时意识到行为中存在的安全风险,相关的安全意识与技能亟待强化。

[0106] 图2为本发明实施例提供的一种基于PC终端行为的个体信息安全能力评价系统,如图2所示,可以包括:

[0107] 采集模块,用于采集个体计算机行为数据;

[0108] 提取模块,用于根据预先制定的安全行为规则,基于所述个体计算机行为数据提取行为动作集和行为权重集,所述行为权重集的元素与行为动作集的元素一一对应;

[0109] 评价模块,用于根据行为动作集和行为权重集,基于预先构建的信息安全能力综合评价模型,评价个体信息安全能力水平。

[0110] 所述采集模块采个体计算机行为数据,包括:

[0111] 通过全局事件监听接口和行为监听方法采集个体计算机行为数据;

[0112] 将采集到的个体计算机行为数据的数据格式转换为符合安全行为规则提取的格式。

[0113] 所述安全行为规则,如下所示:

[0114] SBR::＝{Action,Rule}

[0115] 其中,SBR表示安全行为规则,Action表示用户安全行为,Rule表示推理规则集,用来对用户安全行为进行安全性识别。

[0116] 所述提取模块根据所述个体计算机行为数据和预先制定的安全行为规则,提取行为动作集和行为权重集,包括:

[0117] 根据预先制定的安全行为规则,量化个体计算机行为数据;

[0118] 根据量化后的个体计算机行为数据,得到行为动作集;

[0119] 基于个体计算机行为数据,通过德尔菲专家咨询法,得到行为权重集。

[0120] 所述评价模块根据行为动作集和行为权重集,基于预先构建的信息安全能力综合评价模型,评价个体信息安全能力水平,包括:

[0121] 所述预先构建的信息安全能力综合评价模型包括本征力、警觉力和学习力，根据行为动作集和行为权重集，计算个体的本征力、警觉力和学习力；

[0122] 根据个体的本征力、警觉力和学习力，确定个体信息安全能力水平。

[0123] 根据动作集和行为权重集，计算个体的本征力的公式如下所示：

[0124] $Instinctive(u)=Action(u)*Alpha^{T}(u)$

[0125] 其中，u表示用户，Instinctive(u)表示用户u的本征力，Action表示用户u的行为动作集，$Alpha^{T}(u)$用户u的行为权重集的转置。

[0126] 根据动作集和行为权重集，计算个体的警觉力的计算公式如下所示：

[0127] $$Alertness\ (u)=\frac{1}{1+\frac{\sum_{i=1}^{n}Right\ (S_i)}{Sum_j(u)}}$$

[0128] 其中，Alertness(u)表示用户u的警觉力，$Sum_j(u)$表示用户u所产生的第j类不安全动作的总数，S_i表示第i种存在的不安全行为的总数，Right(S_i)表示第i种存在的不安全行为的总数S_i的带权综合长度，n表示存在n种不安全行为；

[0129] 所述Right(S_i)的计算公式如下所示：

[0130] $$Right\ (Si)=\sum_{k=1}^{l}\sum_{i=1}^{n}I\{a_k\in S_i\ \wedge\ a_k\in b_i\}a_i$$

[0131] 其中，I表示指示函数，当I{true}＝1，I{false}＝0，true和false表示个体计算机行为数据的安全特征，根据安全行为规则确定，true用于表示安全取值为0，false表示不安全取值为1，a_k表示行为动作集中第k个元素，a_i表示行为动作集中第i个元素，b_i为行为权重集中第i个元素，l表示行为动作集的元素总数，n表示行为权重集的元素总数，l＝n都和存在的安全行为总数相同。

[0132] 8、根据权利要求5所述的个体信息安全能力评价方法，其特征在于，根据动作集和行为权重集，计算个体的学习力的计算公式如下所示：

[0133] $$Learning\ (u)=\frac{1}{1+\frac{\sum_{i=1}^{n}a_iR_i(u)}{sum(u)}}$$

[0134] 其中，Learning(u)表示用户u的学习力，Sum(u)表示用户u所产生的不安全动作的总数，$R_i(u)$表示用户u第i种不安全动作发生重复的次数，a_i表示行为动作集中第i个元素，n表示存在n种不安全行为。

[0135] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0136] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明各个实施例所述的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说

对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法或者实施例的某些部分所述的方法。

[0137] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

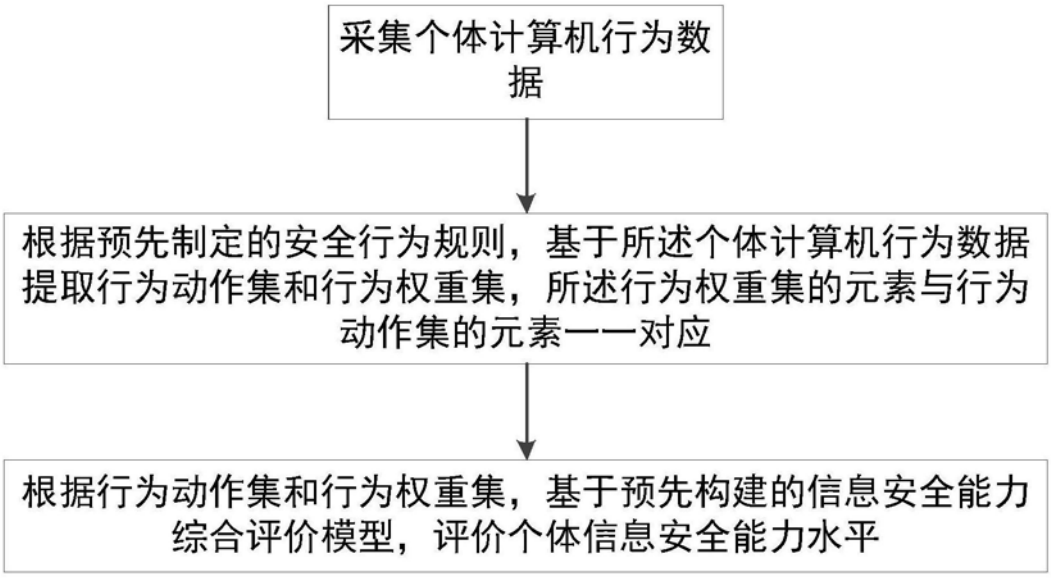

采集个体计算机行为数据
根据预先制定的安全行为规则，基于所述个体计算机行为数据提取行为动作集和行为权重集，所述行为权重集的元素与行为动作集的元素一一对应
根据行为动作集和行为权重集，基于预先构建的信息安全能力综合评价模型，评价个体信息安全能力水平

图1


采集模块
提取模块
评价模块

图2