doi:10.11959/j.issn.1000-436x.2016262

无感状态下基于行为本体的手机用户信息安全能力评估方法

麦丞程[1]，陈波[1]，周嘉坤[1]，于泠[2]
（1. 南京师范大学计算机科学与技术学院，江苏 南京 210023；2. 江苏省大规模复杂系统数值模拟重点实验室，江苏 南京 210023）

摘 要：提出了一种基于安全行为本体的员工安全行为检测方法。通过在用户无感状态下的真实手机使用行为采集，解决了安全行为的真实性问题；通过建立手机用户的静态和动态安全行为本体，对用户的通话、短信、网络与 App 应用等行为进行形式化描述，制定了不安全行为判定规则和行为关联规则；借鉴攻击图的概念，提出了一种基于行为关联图的不安全行为检测算法，发掘不安全行为路径。进一步，提出了信息安全能力评估的胜任力模型，实现了从员工信息安全行为的定性检测到能力的定量评估的过程。实验表明，该方法能够有效检测出用户不安全行为路径，得到安全能力值。

关键词：安全行为本体；行为分析；能力评估；移动安全
中图分类号：TP391 **文献标识码**：A

Evaluation method for information security capability of mobile phone user based on behavior ontology under unconscious condition

MAI Cheng-cheng[1], CHEN Bo[1], ZHOU Jia-kun[1], YU Ling[2]
(1. School of Computer Science and Technology, Nanjing Normal University, Nanjing 210023, China;
2. Jiangsu Provincial Key Laboratory for Numerical of Large Scale Complex System, Nanjing 210023, China)

Abstract: A security capacity assessment method based on security behavior ontology, was proposed to collect users' behavior data from their smartphones under unconscious condition to solve the problem of detecting mobile phone users' real existing insecure behaviors. A security behavior ontology was set up for formalizing the phone, message, network and App behavior data of mobile phone users and relevant rules were also set down for determining and associating insecure actions. Referring to the notion of attack graph, an insecure behavior detection algorithm was proposed based on behavior association graph for analyzing the paths of insecure behaviors dynamically. Furthermore, a competency model of information security capability assessment was presented for realizing the quantitative evaluation of information security capability of users. The experiment results prove the effectiveness of present competency model for insecure behavior path detection and security ability assessment.

Key words: security behavior ontology, behavior analysis, capability assessment, mobile security

1 引言

随着移动办公模式的兴起，组织员工可以携带自己的设备办公（BYOD, bring your own device），在提高工作效率的同时也引入了安全隐患[1]。Intel security 发布的《McAfee Labs 2016 年威胁预测》[2]指出，组织内部员工发起的攻击将是未来 5 年企业面临的主要安全威胁之一。由于员工可以在自己的

收稿日期：2016-08-31
通信作者：陈波，1520990286@qq.com
基金项目：“赛尔网络”下一代互联网技术创新基金资助项目（No.2016-61）；江苏省教育科学“十二五”规划重点基金资助项目（No.B-a/2013/01/013）；中国学位与研究生教育学会研究课题基金资助项目（No.B1-2015Y11-026）；江苏省高等教育教学改革重点课题基金资助项目（No.2015JSJG034）
Foundation Items: Innovation Project of CERNET Next Generation Internet Technology (No.2016-61), Major Program of the 12th Five Years Education Science Plans of Jiangsu Province (No.B-a/2013/01/013), Research Subject of Chinese Society of Degree and Postgraduate Education (No.B1-2015Y11-026), Key Subject of Higher Education Teaching Reform of Jiangsu Province (No.2015JSJG034)

设备上安装企业软件以方便访问公司内部资源，一旦员工连接不安全的 Wi-Fi 信号、安装恶意应用或是被勒索软件攻击，就会成为攻击者威胁企业安全的跳板。

《McAfee Labs 2016 年威胁预测》描述了许多攻击事件是如何入侵那些连接到咖啡店或酒店的公司笔记本电脑、或员工手机，然后攻破公司网络防线的[2]。2016 年 Symantec 公司发布的《Internet security threat report》表明，“欺诈短信”“钓鱼 Wi-Fi”“钓鱼邮件”“社交网络诈骗”等事件是导致员工引发企业内部安全问题的主要因素[3]。例如，美国前国务卿希拉里曾利用私人移动设备和服务器收发 62 320 封政府公务邮件，招致黑客攻击，导致其服务器被迫关闭[4]。

将上述这些安全事件进行汇总可以发现，通话行为、读信行为、网络行为以及 App 应用行为是员工在使用手机的过程中存在的 4 类典型不安全行为。

图 1 描述了 2 种涉及这 4 类不安全行为的攻击路径示例。图 1 中路径{1,2,3,4,5}描述的攻击过程是，如果用户手机收到内容为同学集会照片或是孩子考试成绩的信息（或通话）及链接地址，用户如果点击了该链接，手机会从链接的网址中下载恶意 App 软件，如果用户同意安装恶意 App 软件，该病毒就会伺机窃取用户隐私或是勒索敲诈等。路径{6,7,9}描述的攻击过程是，攻击者会利用大众爱“蹭网”心理，诱骗手机用户连接到免费钓鱼 Wi-Fi 中，如果该用户随后访问了组织内部邮箱或是访问了网银类 App 等应用，其输入的密码等敏感信息会被攻击者截获，导致账户泄露。由上述 2 个示例可知，攻击者利用员工不安全的手机使用行为，可以达到其攻击目的。

因此，员工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，对组织内员工进行信息安全能力评估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。为此，本文提出了一种基于安全行为本体的信息安全能力评估方法，可以在无感状态下检测用户真实的不安全行为并进行安全能力的定量评估，为组织进行信息安全管理提供帮助。

2　相关工作

现有的用户安全能力检测或评估方法可分为以下 3 种。

1) 问卷调查。常见做法是发放调查问卷。Sari[5]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智能手机用户的安全能力，行为因素发挥重要作用。Ngoqo[6]通过向调查者发送钓鱼短信的方式，观察研究对象的应对行为，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。

2) 试题测试。针对问卷调查的缺陷，笔者设计并实现了一款基于 Android 的个人信息安全素养测评手机软件[7]。通过试题测试的方式，确认个体信

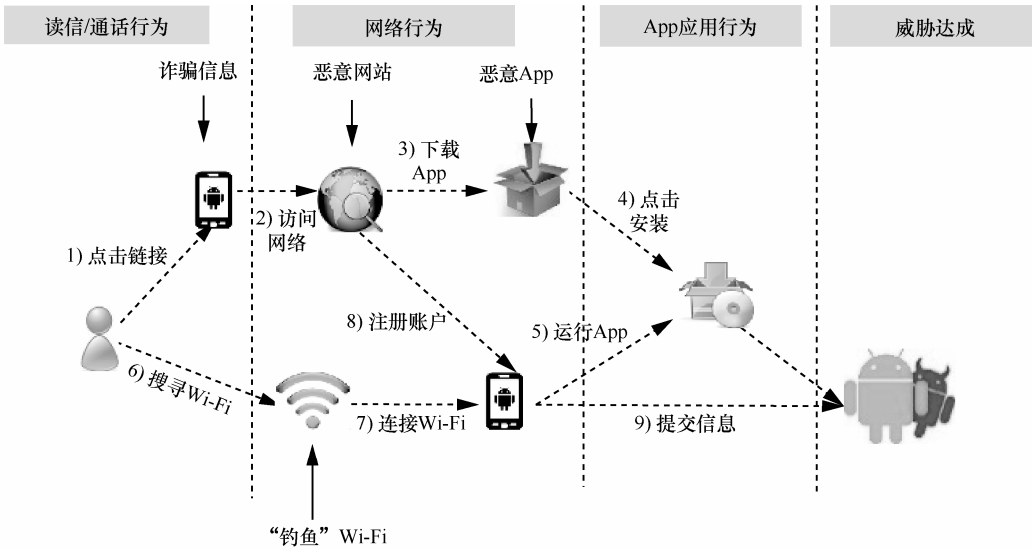


图 1　Android 安全威胁实例

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。

3) 严肃游戏。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）技术被引入到信息安全意识教育和技能培养中。美国 NPS 中心联合 Rivermind 公司开发了一款用于信息安全知识教育和技术培训的模拟训练平台——CyberCIEGE[8]。该平台能够提供良好的虚拟现实环境，具有场景灵活、界面互动性强等特点。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。

综上所述，当前用户安全能力评估研究尚存在 3 个方面的不足。1) 有感。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真实落实情况。2) 不通用。用户行为安全性分析缺乏统一的形式化描述，检测范围局限，可扩展性较弱。3) 固定。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。

为了解决上述 3 类问题，本文提出的基于安全行为本体的信息安全能力评估方法具有如下 3 个方面的特色。1) 行为评估。通过行为分析，实现真实场景下用户真实手机使用行为采集，解决安全行为检测的真实性问题，并进一步评估员工信息安全意识与技能的落实情况。2) 本体描述。提出安全行为本体，解决行为统一建模与形式描述问题。3) 动态分析。实现基于行为关联图的不安全行为检测算法，解决不同场景下用户行为动态分析问题，解决从行为的定性检测到能力的定量评估的问题。

本文研究由 3 个部分组成。

1) 无感状态下行为数据收集。利用 Android 系统提供的事件监听接口和自主开发的行为监听方法采集数据。该部分具体内容在 5.1 节的实验部分详述。

2) 安全行为本体建模。对行为数据进行统一组织和形式化表示，建立行为推理规则集。

3) 信息安全能力评估研究。首先，提出不安全行为检测算法，建立行为关联图，再根据推理规则集实现不安全行为检测算法。然后，构建基于胜任力的信息安全能力评估模型，实现能力定量评估。

2014 年，Google 发起的 BeyondCorp[9]项目提出了一种不区分内外网的一致性防御手段。该项目要求企业员工移动客户端是受控的设备，且必须通过证书来访问企业资源。这说明在 BYOD 场景下利用组织员工客户端设备搜集其行为数据，进行安全行为检测是可行的。

3 手机用户行为检测

3.1 安全行为本体

安全本体是本体概念应用在信息安全领域的一种产物，最早由 Donner[10]于 2003 年提出，他将安全本体描述为“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”。目前，安全本体的研究焦点大多聚集在外部攻击行为检测，研究方向以入侵检测[11~13]、风险分析[14,15]、访问控制[16]、安全教育[17]为主，而以“人”为目标的安全能力检测方面鲜有研究。由于本体在知识组织、形式化描述、推理规则构建等方面的优势，本文通过构建安全行为本体进行用户行为的组织、描述与推理。

安全行为本体（*SBO*, security behavior ontology）由静态安全行为本体和动态安全行为本体构成。安全行为本体形式化定义为

定义 1 *SBO*:: = { *SSBO* , *DSBO*, *Rule* }

其中，静态安全行为本体（*SSBO*, static security behavior ontology）用来描述收集到的行为的静态特征及其之间关系；动态行为本体（*DSBO*, dynamic security behavior ontology）用来描述行为参与者之间以及行为之间的动态关系。*Rule* 表示推理规则集，用来关联用户行为并进行安全性识别。

1) 静态安全行为本体

本文将 *SSBO* 进一步形式化。

定义 2 *SSBO*::={ *Behavior*, *Rel*, *Pros*}

其中，*Behavior* = {*phoneBehavior*, *smsBehavior*, *webBehavior*, *appBehavior*}；*Rel* 用来描述行为之间的关系；*Pro* 表示行为所包含的具体特征。

本文以前述的员工在使用手机过程中存在的 4 类典型不安全行为为例，根据定义 2，静态行为本体如图 2 所示，图 2 中矩形框代表抽象概念类，椭圆形框表示 4 种具体的行为，箭头表示行为之间及其特征之间的关系，实线上方为对应行为的特征。

静态安全行为本体包含 4 种具体行为，分别为通

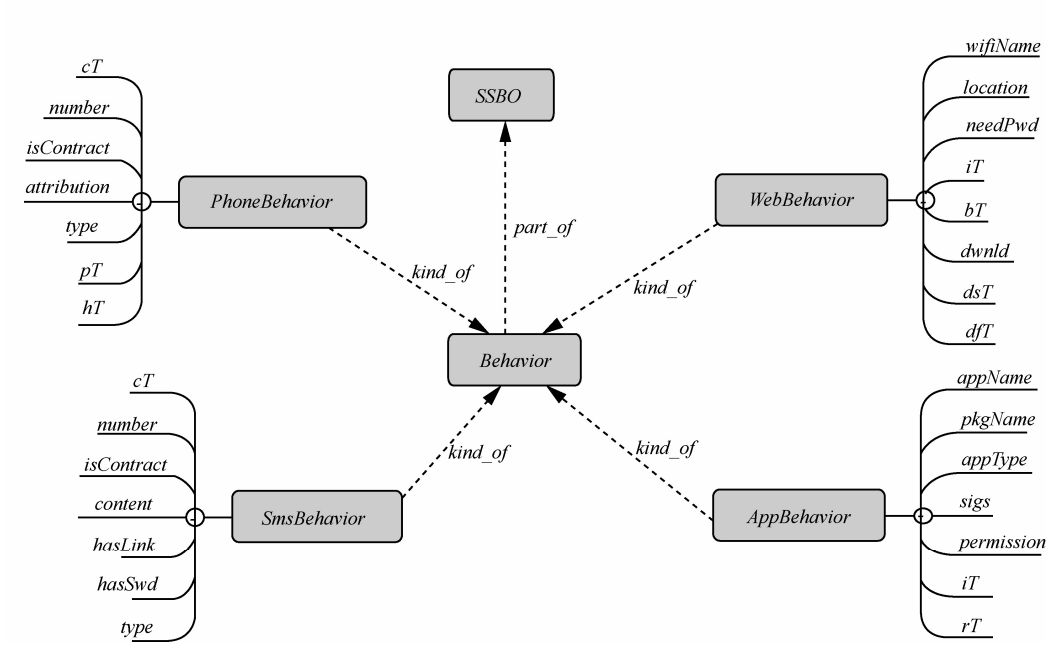


图 2　静态安全行为本体

话行为、短信行为、网络行为和应用行为；行为之间以及行为与其特征之间通过 2 种关系来描述：*kind_of* 表示某种特定行为是一种行为，例如 *phoneBehavior* 是一种 *Behavior*; *part_of* 表示概念之间属于组成关系，例如 *Behavior* 是 *SSBO* 的一个组成部分。

界定组织内用户的行为特征是进行安全行为检测的基础，按照构建的静态安全行为本体，本文采集的各类行为特征及具体含义如表 1 所示。

表 1　　静态安全行为本体的特征

行为	特征
PhoneBehavior	*cT,number,isContract,attribution,type,pT,hT*
SmsBehavior	*cT,number,isContract,content,hasLink,hasSwd,type*
WebBehavior	*wifiName,location, needPwd,iT,bT,dwnld,dsT,dfT*
AppBehavior	*appName,pkgName,appType,sigs,permission,iT,rT*

phoneBehavior 表示通话行为，其特征依次为：来电时间、号码、是否为联系人、归属地、类型标记、接听时间、挂断时间。*smsBehavior* 表示短信行为，其特征依次为：来信时间、号码、是否为联系人、短信内容、是否含超链接、是否包含敏感词汇、类型标记；*webBehavior* 表示网络行为，其特征依次为 Wi-Fi 名称、连接场合、是否要密码、连接时间、断开时间、下载内容、下载开始时间、下载结束时间；*appBehavior* 表示应用行为，其特征为应用名称、应用包名、应用类型、签名、权限列表、安装时间、运行时间。

2) 动态安全行为本体

动态安全行为本体 *DSBO* 的形式化定义如下。

定义 3　*DSBO*::={ *Actor*, *Action*, *Rel*}

其中，*Actor* 为行为参与者，包括外部参与者(*outsideActor*)和内部用户(*insideActor*)；*Action* 为动作语义集合，本文选取的 4 类行为被细化为 13 个动作；*Rel* 描述不同参与者以及动作之间的关系。动态安全行为本体如图 3 所示，虚线箭头表示参与者(*Actor*)、动作集(*Action*)与 *DSBO* 之间的关系。

每种行为由多种动作组成，动作集合 *Action* 中的动作及其语义如表 2 所示。*Rel* 集合包含 3 种关系{*contains*，*is_a*，*is_part_of*}，如 *is_part_of* 表示 *Actor* 是 *DSBO* 的一个组成部分，*contains* 表示 *Action* 集合包含 *click*、*call*、*send* 等动作。

3.2　推理规则 *Rule*

本文采用基于产生式的规则语言对行为本体进行语义扩展，具体如下 *Rule*::={ *dRule*, *rRule*}。其中，*dRule* 用来确定不安全动作；*rRule* 表示不安全动作关联规则集合，用来将 *dRule* 中确定的不安全行为进行两两关联，具体内容如下。

1) 不安全行为判定规则

为了从大量用户行为中过滤出具有潜在安全风险的行为，本文基于专家知识制定了 13 条不安全行为判定规则。限于篇幅，下文仅列出 1 例，用来进行判定规则的语法和语义说明。

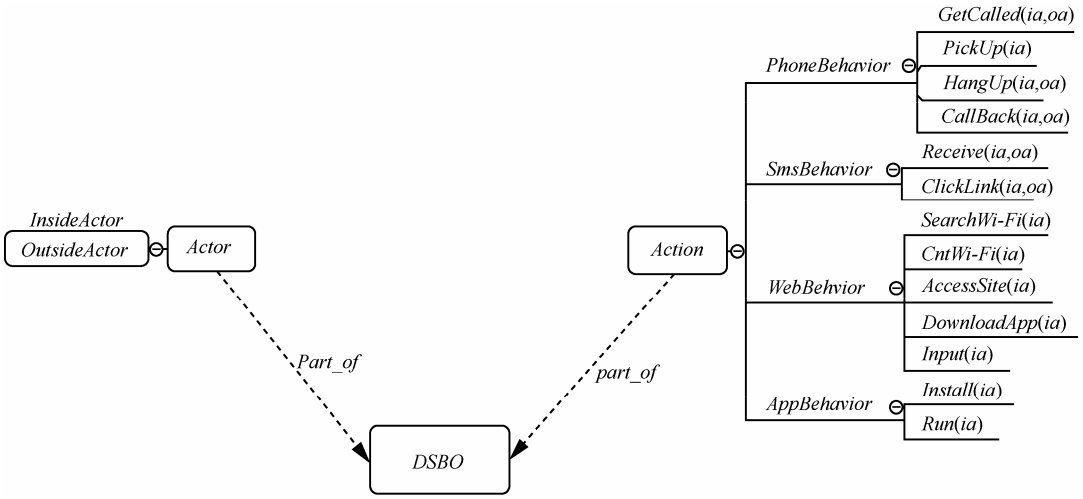


图 3　动态安全行为本体

表 2　　**动作语义集合**

所属行为	动作名称	动作语义
PhoneBehavior	*GetCalled*(*ia*,*oa*)	*oa* 给 *ia* 拨打电话
	PickUp(*ia*)	*ia* 接听电话
	HangUp(*ia*,*oa*)	*oa* 挂断给 *ia* 的电话
	CallBack(*ia*,*oa*)	*ia* 给 *oa* 回拨电话
SmsBehavior	*Receive*(*ia*,*oa*)	*oa* 给 *ia* 发送短信
	ClickLink(*ia*)	*ia* 点击短信中链接
WebBehavior	*SearchWi-Fi*(*ia*)	*ia* 搜寻 Wi-Fi 热点
	CntWi-Fi(*ia*)	*Ia* 连接 Wi-Fi
	AccessSite(*ia*)	*ia* 访问站点 site
	DownloadApp(*ia*)	*ia* 下载 App
	Input(ia)	*ia* 输入信息
AppBehavior	*Install*(*ia*)	*ia* 安装 App
	Run(*ia*)	*ia* 启动 App

dRule-7:*cntWi-Fi*(*ia*) ∧ *location*='*public*' ∧ *needPwd*='*false*'→*insecure Action*

规则 *dRule*-7 含义为：*ia* 连接公共场所不需要密码的 Wi-Fi，则推断该动作存在连接钓鱼 Wi-Fi 的风险。依据该形式，本文对其余的动作节点也制定了相关的不安全行为判定规则，详见附录 A。

2) 行为关联规则

不同场景下相同的行为动作会具有不同的语义。例如点击运行组织内部邮箱，如果单独分析这个行为不能发现风险，但如果用户在公共场合下，链接了无密码的免费 Wi-Fi，再打开组织内部邮箱进行业务操作，则有可能其敏感账户信息或组织内部信息被第三方截获。因此，为了识别不同场景下据有关联关系的行为的安全性，本文制定了行为关联规则集 *rRule*，对不同类型的行为进行关联分析。

本文提出的关联规则基于如下 2 个假设。

1) 当 2 个动作的发生时间间隔在 δ 内，则认为 2 个行为具有先后顺序关系；

2) 当 2 个动作存在特征值相同的特征字段，则 2 个动作具有关联关系。

例如，当接听电话和回拨电话的号码相同且在一定的时间间隔内，则判定 2 个动作存在关联关系；当短信中的链接地址与访问的网站的地址相同，且先后发生，则可以判定用户通过点击短信中的链接被劫持到钓鱼网站。

针对动作语义集合确定的 13 种动作，附录 A 中给出了相对应的关联规则。限于篇幅，这里选择性列举了 4 类行为中的部分关联规则如下。

rRule-6: *CntWi-Fi*(*ia*) ∧ *Run*(*ia*) ∧ *appType* ='*E-mail* ||*Pay*||*Shop*||*Bank*' ∧ |*Run.time-CntWi-Fi.time*|< δ →*insecure Association*

对 *rRule*-6 解析如下：*ia* 在公共场合连接无密码 Wi-Fi，并在时间间隔 δ 内运行组织内部邮箱或是金融支付类 App 应用，则推断这 2 个动作之间存在风险关联。

本文针对这些动作的安全性判定和关联关系制定的部分推理规则详见附录 A，通过这些规则的组合可以表示多种安全风险行为。

3.3　不安全行为检测算法

3.3.1　行为关联图的定义

用户不安全行为是一种复杂的多步骤行为，包含造成最终损失所进行的紧密关联的基本动作。基

本动作的发生能够帮助攻击者获取相应的资源与权限，继而进行下一步攻击行为，最终实现对用户的威胁。本文借鉴攻击图的概念，提出了一种行为关联图进行不安全行为分析。

定义 4　行为关联图（behavior associated graph）定义为一个有向无环图 $BAG=(V, E)$。

1) V 代表语义动作表中给出的动作节点集合，$V=\{A, P\}$，A 是该动作节点的静态属性集合，$A\in Pros$；P 为指向下一步动作的指针集合，$P\in Action$。

2) E 表示各动作节点之间有关联关系的有向边的集合。其中，$E\subseteq rRule$，表示当一个独立行为发生之后下一个独立行为才能够得到实施。

根据以上定义，图 4 展示了基于推理规则集 *dRule* 和 *rRule* 的行为关联图的可能情况。其中，独立行为节点用圆圈表示，行为之间的关联关系用箭头表示。

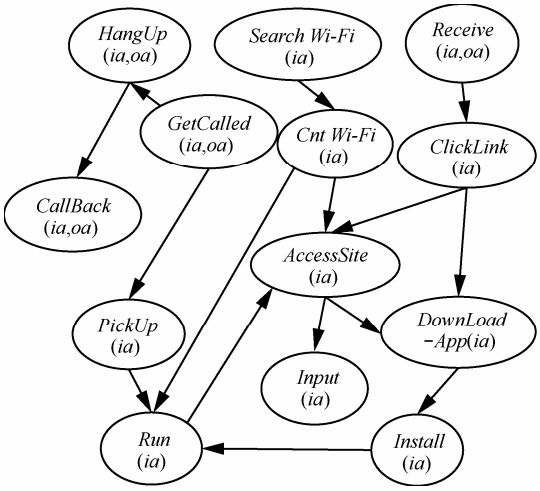


图 4　行为关联

3.3.2　算法描述

行为安全性检测算法分别根据推理规则 *dRule* 和 *rRule*，确定了风险动作节点和节点之间的关联关系。算法描述如下。

算法 1　行为关联图构建算法

输入　行为类型数目 N; 规则集 *dRule* 和 *rRule*; 安全行为本体 *SBO*

输出　行为关联图 *BAG*

1)　$V=\{\varnothing\}$;$E=\{\varnothing\}$;$F=\{\varnothing\}$;
2)　$BAG=\{V,E\}$
3)　for all $v\in SBO$
4)　　if *Match* (v, *bRule*)=True
5)　　$Type=GetActionType(v)$
6)　　Add v to V_{type}
7)　end for
8)　for i=1 to N do
9)　　$Type=GetType(i)$
10)　　for each v_p in V_{type}
11)　　$NextType=GetNextType(Type)$
12)　　for each v_n in V_{nextType}
13)　　if $Match(e(v_p,v_n),rRule)$=True
14)　　Add edge $e(v_p,v_n)$ to E
15)　　else
16)　　break
17)　　end for
18)　end for
19) end for

该算法复杂度为 $O(N_pN_n)$，N 为常数，即 2 个关联行为类型节点个数的乘积。

在算法 1 基础上，算法 2 实现了一个行为关联图的遍历算法，在遍历的过程中给出用户不安全行为路径。

算法 2　不安全行为路径发现算法

输入　行为关联图 $BAG=\{V,E\}$

输出　不安全行为路径 *tPath*

1) $tPath=\{\varnothing\}$;
2) for each v in V
3)　$Visited(v)$
4)　if $visited(v)$=False
5)　$Tmp_v=v\rightarrow next$;
6)　while(Tmp_v)
7)　Add Tmp_v to *tPath*
8)　$Visited(Tmp_v)$
9)　$Tmp_v = Tmp_v \rightarrow next$
10)　end while
11)　else
12)　break
13) end for

本算法复杂度为 $O(N_v)$，即安全行为本体中的行为节点的数量规模。

下面以一个简化的例子对算法进行说明。

根据规则集 *dRule*，图 5 中具有安全风险的动作 *CntWi-Fi* 发生了 3 次，表示为 v_1、v_2、v_3。根据规则集 *rRule*，v_1 的后续动作 *CntWi-Fi* 发生了 2 次，表示为 v_4、v_5。根据时间间隔和相同特征值可以判

断出 v_1 的后续动作节点为 v_4，因此，建立 v_1 和 v_4 之间的动作关联联系；同理，由于 v_2 没有和 *cntWi-Fi* 中任何动作节点存在关联关系，因此，v_2 的后续行为节点指向 null。同理，v_3 和 v_5，v_4 和 v_8，v_5 和 v_{10} 等节点之间建立了具有潜在安全风险的关联关系。

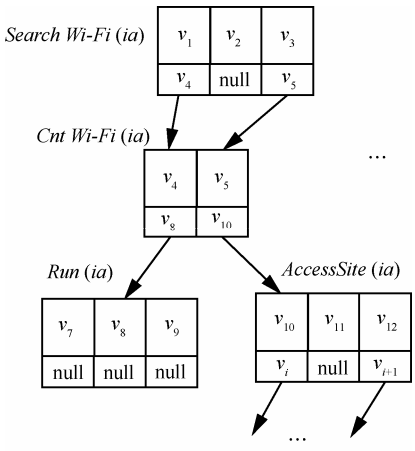


图 5 行为节点关联

最后，沿实线箭头不重复遍历途中所有节点，即可得到最终的不安全行为路径，算法结束。

4 基于胜任力模型的信息安全能力评估

4.1 胜任力模型

“胜任力”这一概念由美国著名心理学家 McClelland[18]于 1973 年提出，其给出的定义为，“与工作、工作绩效或生活中其他重要成果直接相似或相联系的知识、技能、能力、特质或动机，可区分卓越绩效者和一般绩效者”。1990 年，Prahalad 和 Hamel[19]将胜任力的研究拓展到了组织层面，提出了著名的“组织核心能力理论”，认为组织的核心能力和组织中员工的胜任力必须是相匹配的，员工的胜任力是组织运营、管理所依赖的必要基础。

国内的研究文献中常将其译作“胜任特征”“胜任素质”或“胜任能力”等。其研究的内容一般以为高绩效员工选拔、人才培养、员工聘用标准制定、预测绩效等为主，在管理科学与组织管理实践等领域受到高度重视，相应的胜任力模型也被提出以满足员工选拔与人才培养的需求。

胜任力模型是指某一类特定工作所需胜任力的有机组合，一般由多个核心胜任力指标组成，通过行为化的方式加以展示。胜任力模型通常以 Spencer 与 McCleland 提出的胜任力冰山模型为理论基础。在冰山模型中，个体的胜任力特征被分为“水上冰山”和“水下冰山”这 2 个部分，即显性能力部分与隐性能力部分。显性能力部分主要指可见的、外显性的知识、技能、行为等；隐性能力部分主要指不可见的、内隐的意识、动机、个人特质、社会角色等。显性胜任力是员工落实工作计划、实现绩效指标的客观保障；隐性胜任力是员工完成工作任务、促进组织发展的潜在能力，也是区分高绩效者与一般绩效者的关键因素。

4.2 信息安全能力评估的胜任力模型

在移动环境下，组织员工具有个体差异性大、行为习惯迥异等心理和行为特征。因此，可以通过构建胜任力模型从隐性能力和显性能力这 2 个角度实现组织员工的信息安全能力评估研究。

本文基于胜任力理论提出了评估员工信息安全能力的胜任力模型。该模型由 3 个基本胜任力要素构成，每个要素又细化为若干行为指标，如表 3 所示。

模型中所涉及的动作集 $Action=\{a_1,a_2,\cdots,a_k,\cdots,a_t\}$；行为集 $Behavior=\{b_1,b_2,\cdots,b_i,\cdots,b_n\}$，不同类型的行为权重集为 $Alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_i,\cdots,\alpha_n\}$，文中取 t=13，n=4；路径集 $Path=\{p_1,p_2,\cdots,p_j,\cdots,p_m\}$。

表 3 信息安全能力评估胜任力模型

胜任力要素	要素定义	细化行为指标
健全性（显性）	衡量员工避免发生不安全行为的能力	不安全动作总数 动作所属行为类型：通话行为、短信行为、网络行为、应用行为 各类不安全动作发生次数
警觉性（隐性）	衡量员工对于不安全行为发生的警觉的能力	不安全行为路径数目 不安全路径深度 各路径涉及行为类型数
自省性（隐性）	衡量员工避免重复发生不安全行为的能力	行为相似度 行为重复度

1) 健全性

健全性（*comprehensive*）依据用户不安全行为发生的次数与类型能直接反映用户各方面的信息安全能力健全程度。用户不安全行为发生的次数越多、类型越多，则说明该用户的信息安全能力的健全度越低，反之越高。用户 u 的健全性计算式为

$$comprehensive(u)=1-\frac{\sum_{i=1}^{n}\alpha_i insecure_i(u)}{sum(u)} \quad (1)$$

其中，α_i 是可以调节的参数，表示第 i 类行为的权

值；$insecure_i(u)$表示第 i 类行为中不安全动作发生的次数；$sum(u)$表示用户 u 产生的不安全动作的总次数。

2) 警觉性

警觉性（*alertness*）是指用户在使用手机的过程中能够自觉意识到其操作中潜在的安全风险，并且能够及时终止不安全的行为。本文用每种不安全路径的平均深度来衡量用户的警觉性，计算式为

$$alertness(u)=\frac{1}{1+\frac{\sum_{j=1}^{m}Depth(P_j)}{Path_i(u)}} \tag{2}$$

其中，$Path_i(u)$表示用户所产生的第 i 类不安全行为路径总数。$Depth(P_j)$表示路径 P_j 的带权路径长度，计算式为

$$Depth(P_j)=\sum_{k=1}^{t}\sum_{i=1}^{n}I\{a_k\in P_j\wedge a_k\in b_i\}\alpha_i \tag{3}$$

记指示函数

$$I\{\text{true}\}=1, I\{\text{false}\}=0 \tag{4}$$

3) 自省性

自省性（*introspection*）描述用户是否会重复进行不安全的手机行为操作，用来衡量用户能够有意识地对已发生的安全事件进行自我反省，从而避免相同的不安全行为再次发生。

首先，需要对路径向量进行相似性计算。路径的相似性是用来比较 2 个由多个动作所组成的路径向量之间的相似程度，并以此来识别该不安全路径是否被用户重复执行。

本文采用 *Jaccard* 相似度实现重复路径的识别。用户的路径向量被表示为用户产生动作 a_i 的序列，如 $\boldsymbol{P}_h=\{a_1,a_2,\cdots,a_{i1}\}$、$\boldsymbol{P}_l=\{a_1,a_2,\cdots,a_{i2}\}$为任意 2 个行为向量，其相似度可表示为

$$Jaccard(\boldsymbol{P}_h,\boldsymbol{P}_l)=\frac{\boldsymbol{P}_h\cap\boldsymbol{P}_l}{\boldsymbol{P}_h\cup\boldsymbol{P}_l} \tag{5}$$

当 $Jaccard(\boldsymbol{P}_h,\boldsymbol{P}_l)$ 大于等于阈值 δ 时，则认为相似的路径重复发生。

然后，对所有路径向量计算相似度，根据相似度统计重复出现的路径次数，并通过其中包含的动作来确定所属行为类型，以确定权重。

用户的自省性计算式为

$$introspection(u)=1-\frac{\left(\sum_{i=1}^{n}\alpha_i R_i(u)\right)}{Path(u)} \tag{6}$$

其中，α_i 为可调参数，表示第 i 种不安全行为路径的权重；$R_i(u)$表示用户 u 第 i 类不安全行为重复的总次数；$Path(u)$表示用户 u 所产生的不安全行为路径总数。

最终，健全性、警觉性和自省性共同构成了用户安全能力评估值，φ、γ、η 为 3 个可调参数，计算式为

$$\begin{aligned}Ability(u)=&\varphi comprehensive(u)+\\&\gamma alertness(u)+\eta introspection(u)\end{aligned} \tag{7}$$

5　实验与数据分析

5.1　实验环境

本文使用 Java 语言实现了一个原型系统。客户端实验在 Android 系统版本为 4.4.4 的真机上测试完成，内存为 1 GB，数据以 cvs 格式上传到服务器。服务器端采用 Jsp+JavaBean+Servlet 方式实现，行为分析算法在内存为 2 GB，处理器为 Intel (R) Core(TM) i3-2120 CPU 3.30 GHz 的服务器上实现。

5.2　数据来源

本文利用 Android 系统自身提供的全局事件监听接口和自主开发的行为监听方法采集数据，包括通话行为监听接口 phoneStateListener（获取来电号码、时间等）；smsReceiver（获取短信内容、时间等）；热点连接监听接口 Wi-FiLinkReceiver（获取所链接 Wi-Fi 热点的名称、是否需要密码等）；应用安装监听接口 AppInstallReceiver（获取 App 安装的时间、名称、包名和 MD5 码等）；应用运行监听接口 AppRunReceiver（获取应用启动的时间等）；地理位置及场所监听接口 LocationReceiver（获取用户所处的地理位置和场所等）；网络流量监听类 DownloadMonitor（获取流量内容、IP 地址、域名）等。原型系统获取到 2016 年 6 月 5 日~2016 年 7 月 9 日期间共计 288 条行为数据。

5.3　结果分析

1) 定性分析

借助 Java 编程语言，通过调用 Arbor.js 开源开发包，实现了用户不安全行为路径图的可视化，如图 6 所示。

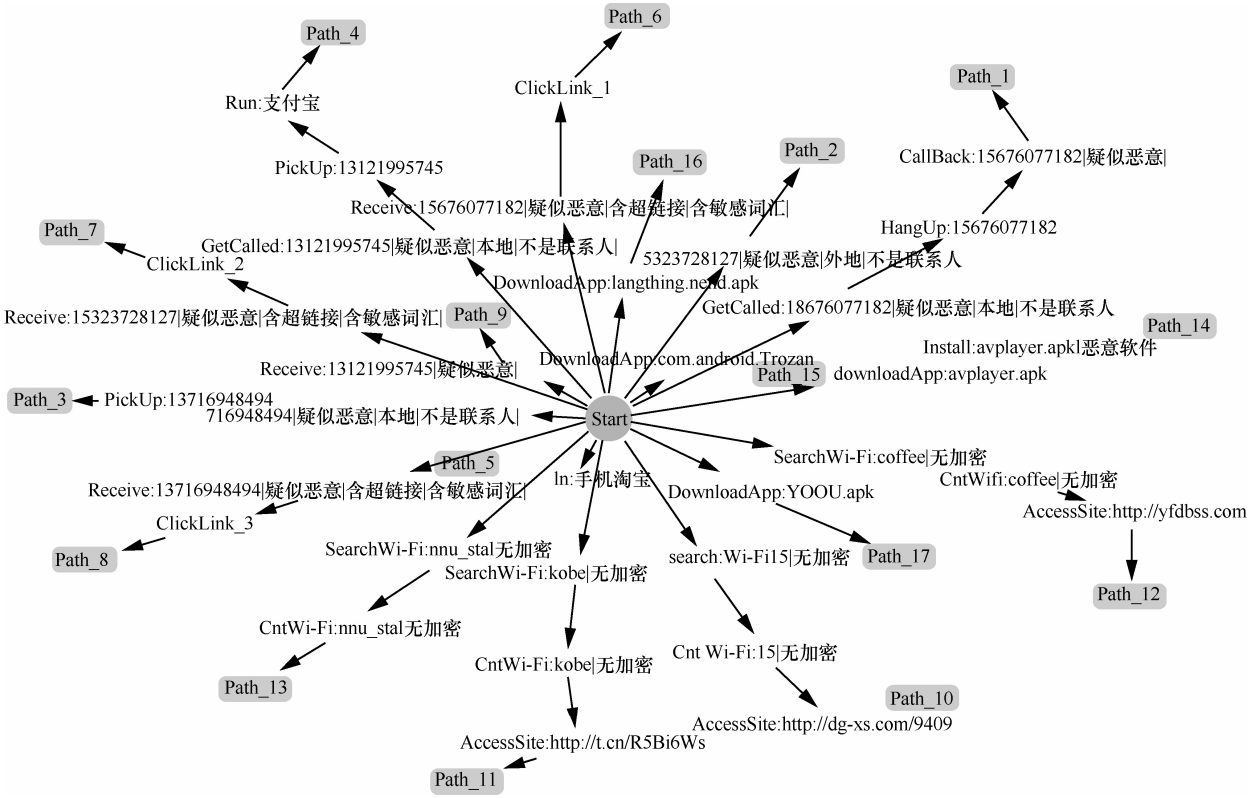


图 6　用户不安全行为路径

如图 6 所示，第 1 条不安全行为路径说明用户曾接到号码为“15676077182”的电话，该号码已被标记为恶意电话，该电话响铃后主动挂断，随后用户回拨该电话。这表明用户存在被诱骗回拨骚扰电话，骗取话费的可能。第 8 条不安全行为路径解释为：用户收到了来自“13716948494”的短信，短信包含超链接和“中奖”等敏感词汇，并且用户点击了其中的超链接。同样，第 5~7 条不安全行为路径说明该用户曾多次点击短信中的超链接。第 10~13 条不安全行为路径表明用户曾多次连接到不需要密码的公共 Wi-Fi 上，例如名为“coffee”、“nnu_sta”等 Wi-Fi 热点。第 14 条不安全行为路径上存在 3 个动作：下载 avplayer.apk 应用、安装该应用（安装时该应用被系统利用 MD5 码与第三方病毒库进行匹配的方式标记为恶意软件），并且运行了该应用。

2) 定量分析

根据获取的数据，利用本文提出的胜任力评估模型对用户进行信息安全能力的定量评估，评估算法由 Java 语言编程实现。

①健全性计算。根据式(1)，将通话行为、短信行为、网络行为、应用行为的权重依次确定为 0.1、0.2、0.3、0.4，即确定参数 a_1~a_4 的取值。其中，不安全通话行为、短信行为、网络行为与应用行为各发生 4、3、7、3 次，全部不安全动作发生次数为 17 次。

$$comprehensive(u)=1-(0.1\times\frac{4}{17}+0.2\times\frac{3}{17}+0.3\times\frac{7}{17}+0.4\times\frac{3}{17})=0.75 \quad (8)$$

最终，该用户的信息安全能力健全性为 0.75。

②警觉性计算。4 类行为的权重与式(1)中相同，通过统计得到不安全通话行为、短信行为、网络行为与应用行为的总深度依次为 9、7、11、6。各类型的不安全行为路径总数分别为 4、4、4 与 5，总计为 17。

$$alertness(u)=\frac{1}{1+(0.1\times2.25+0.2\times1.75+0.3\times3.5+0.4\times1.2)}=0.32 \quad (9)$$

计算得到该用户的警觉性为 0.32。

③自省性计算。该用户的不安全通话行为、短信行为、网络行为与应用行为重复发生次数依次为 1、2、3、2。各类型行为的权重取值与式(1)中相同，将相似度阈值 $\delta\geqslant0.6$ 的行为路径归为一类，并计算

各类行为的重复度。

$$introspection(u)=1-(0.1\times\frac{1}{17}+0.2\times\frac{2}{17}+0.3\times\frac{3}{17}+0.4\times\frac{2}{17})=0.87 \quad (10)$$

计算得到该用户的自省性能力值为 0.87。

得到健全性、警觉性与自省性的能力值后，将φ、γ、η分别设定为 0.5、0.25、0.25，代入式(7)，有

$$Ability(u)=0.5\times0.75+0.25\times0.32+0.25\times0.87=0.67 \quad (11)$$

得出该用户最终的信息安全能力值为 0.67。

依据专家知识与最大隶属度准则，本文给出了安全能力隶属度等级划分标准，如表 4 所示。

表 4　　信息安全能力隶属度等级

能力值	能力层级
0.0~0.2	很低
0.2~0.4	较低
0.4~0.6	中
0.6~0.8	较高
0.8~1.0	极高

该用户的信息安全能力属于较高级别，结合图 6 对这些具体的不安全行为路径进行解析，可以发现该用户在钓鱼 Wi-Fi、钓鱼短信以及恶意 App 应用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。

6　结束语

本文通过行为获取技术解决了检测用户真实存在的不安全手机行为的问题；通过构造安全行为本体解决了多类型行为的统一表示与形式化建模问题；通过构造行为规则集和行为关联图解决了动态行为分析问题；通过构建基于胜任力的信息安全能力评估模型解决了安全能力的定量评估问题。

在 BYOD 环境下，可控移动设备的部署为手机用户行为数据的搜集提供了可行条件。本文下一步工作是扩充行为推理规则集，提升系统对更多行为的安全性检测能力；在更多的终端移动设备上部署系统，对有感和无感状态下用户信息安全意识与行为落实之间的差异性进行定量分析。

附录 A　规则

表 A1　　不安全行为判定规则（部分）

推理规则	规则解析
dRule-1:*GetCalled*(*oa*,*ia*) ∧ *phoneBehavior.type*='*malicious*'||(*attribution*= '*nonLocacal* ∧ *isContract*='*false*') →*insecure Action*	如果 *oa* 向 *ia* 打电话，该电话的标记类型为“恶意”又或该电话归属地为外地且不是常用联系人，则推断该电话存在风险
dRule-2:*HangUp*(*oa*,*ia*) ∧ |*eT*-*cT*|<*δ* ∧ (*location*='*nonLocal*' ∧ *isContract*='*no*')|| *type*= '*malicious*' →*insecure Action*	如果 *oa* 在响铃一声（或极短的时间内）挂断电话，并且来电号码是外地，且不是 *ia* 的常用联系人，或者该号码已被标记为“恶意”，则推断该电话存在风险
dRule-3:*CallBack*(*ia*,*oa*) ∧ (*location*='*nonLocal*' ∧ *isContract*='*no*')||*type*= '*malicious*' → *insecure Action*	如果 *ia* 回拨 *oa* 电话，且该电话来电号码是外地，且不是 *ia* 的常用联系人，或者该号码已被标记为“恶意”，则推断该动作存在风险
dRule-4:*SearchWi-Fi*(*ia*) ∧ *location*='*public*' ∧ *needPwd*='*false*')→ *insecureAction*	*ia* 在公共场合搜寻 Wi-Fi 热点，且该热点不需要密码，则推断该动作存在连接钓鱼 Wi-Fi 的风险。
dRule-5:*Receive*(*ia*,*oa*) ∧ *smsBehavior.hasLink*='*true*' ∧ *hasSWord*='*true*'→*insecure Action*	*oa* 向 *ia* 发送短信，短信中存在超链接和敏感词汇，则推断该动作存在点击钓鱼短信的风险
dRule-6:*PickUp*(*ia*) ∧ *phoneBehavior.type*='*malicious*'||(*attribution*= '*nonLoacal* ∧ *isContract*='*false*') → *insecure Action*	*ia* 接听电话，该电话被标记为“恶意”电话，又或者该电话归属地为外地且不是常用联系人，则推断该通话动作存在电话诈骗的风险
dRule-7:*appBehavior.appName*='*SMS*' ∧ *appBehavior.appName*='*Brower*' ∧ | *Browser.startTime*-*SMS.startTime*|<*δ*→*ClikLink* (*ia*)	如果在时间段 *δ* 内运行短信和浏览器应用，则推断点击了短信中的链接
dRule-8:*cntWi-Fi*(*ia*) ∧ *location*='*public*' ∧ *needPwd*='*false*' →*insecure Action*	*ia* 连接公共场所不要密码的 Wi-Fi，则推断该动作存在风险
dRule-9:*webBehavior.downloadCotent*='.*apk*' → *DownlaodApp*(*ia*)	当流量中出现“*.apk*”时，推断 *ia* 正下载应用的动作存在风险
dRule-10:*Run*(*ia*,*app*) ∧ *appBehavior.appName*='*Browser*' →*AccessSite*(*ia*,*site*)	运行浏览器类应用可以推断 *ia* 在进行访问网页的动作，存在风险隐患
dRule-11:*Install*(*ia*,*app*) ∧ *appBehavior.type*='*malicious*' →*insecure Action*	*ia* 安装恶意软件，则推断该动作存在风险
dRule-12:*Run*(*ia*,*app*) ∧ *hasSwd*='*true*' →*Input* (*ia*,*info*)	运行 App 并且网络流量中出现密码等敏感词时，推断存在信息泄露风险
dRule-13:*Run*(*ia*,*app*) ∧ *appBehavior.appType*='*E-mail*'||*shop*'||'*bank*'||'*pay*'→*insecure Action*	使用组织内部应用，如电子邮箱，或者使用购物、网银、支付类型的应用，则推断该动作存在风险

表 A2　　行为关联规则（部分）

推理规则	规则解析
rRule-1:*GetCalled*(*ia*,*oa*) ∧ *phoneBehavior.type*='*Danger*' ∧ *Pick*(*ia*)→*insecure Association*	当 *oa* 向 *ia* 拨打电话，*ia* 接听电话，且该电话被标记为“恶意”，则推断这 2 个动作存在风险关联
rRule-2:*PickUp*(*ia*) ∧ *Run*(*ia*,*app*) ∧ *appType*='*Pay*||*Shop*||*Bank*' →*insecure Association*	*ia* 接听电话后，并开启了金融支付类的 App 应用，则推断 2 个动作存在电话诈骗的风险关联
rRule-3:*GetCalled*(*oa*,*ia*) ∧ *HangUp*(*oa*,*ia*) ∧ (*location*='*nonLocal*' ∧ *isContract*='*no*')||*type*='*malicious*' →*insecure Association*	如果 *oa* 向 *ia* 拨打电话，并快速挂断，且来电号码是外地，不是 *ia* 的常用联系人，或这该号码已被标记为“恶意”，则推断 2 个动作存在风险
rRule-4:*HangUp*(*oa*,*ia*) ∧ *CallBack*(*ia*,*oa*) ∧ (*location*='*nonLocal*' ∧ *isContract*='*no*')||*type*='*malicious*' →*insecure Association*	若 *ia* 回拨 *oa* 挂断的电话，且号码为外地，不是 *ia* 的联系人，则推断这 2 个动作存在关联风险
rRule-5:*SearchWi-Fi*(*ia*) ∧ *Cnt*Wi-Fi(*ia*) ∧ |*Search*Wi-Fi.*LinkTime*- *Cnt*Wi-Fi.*Time*|< *δ*→ *insecure Association*	*ia* 在公共场合搜索无密码 Wi-Fi，并且连接该 Wi-Fi，则推断这两个动作间存在风险关联
rRule-6:*cntWi-Fi*(*ia*) ∧ *Run*(*ia*) ∧ *appType*='*E-mail*||*Pay*||*Shop*||*Bank*' ∧ |*Run.time*-*CntWi-Fi.time*|< *δ*→ *insecure Association*	*ia* 在公共场合连接无密码 Wi-Fi，并且使用组织内部邮件或是金融支付类 App 应用，则推断该 2 个动作间存在风险关联
rRule-7:*CntWi-Fi*(*ia*) ∧ *AccessSite*(*ia*) ∧ |*Cnt*Wi-Fi.*time*-*AccessSite.time*|< *δ* ∧ *Site.type*= '*shop*||*pay*||*Bank*' →*insecure Association*	*ia* 连接公共场合无密码 Wi-Fi，并且访问金融支付类网站，则推断这 2 个动作之间存在风险关联
rRule-8:*AccessSite*(*ia*) ∧ *Input*(*ia*) ∧ *info.content*='*password*||*userName*' *insecure Association*	*ia* 访问网站，并且在表单中输入用户名或密码等信息，则推断这 2 个动作之间存在风险关联
rRule-9:*Receive*(*ia*,*oa*) ∧ *ClickLink*(*ia*) → *insecure Association*	*oa* 向 *ia* 发送短信，*ia* 点击其中的链接，则推断 2 个动作间存在风险关联
rRule-10:*ClickLink*(*ia*) ∧ *AccessSite*(*ia*) ∧ |*access*.*Time*-*ClickLink.time*|<*δ* ∧ *site.type*='*Shop*||*Pay*||*Bank*' →*insecure Association*	*ia* 点击了短信中的链接，并且访问了金融支付类网站，或是钓鱼网站，则推断这 2 个动作存在风险关联
rRule-11:*Run(ia)* ∧ *appType*='*E-mail*||*Social*' ∧ *AccessSite*(*ia*) → *insecure Association*	如果 *ia* 在使用组织内部邮箱或社交软件时，点击其中的钓鱼链接，访问第三方网站，则推断这 2 个动作存在风险关联
rRule-12:*ClickLink*(*ia*) ∧ *Download*(*ia*,*app*) →*insecure Association*	*ia* 点击短信中的超链接，并下载对应的 App 应用，则推断 2 个动作间存在风险关联
rRule-13:*AccessSite*(*ia*) ∧ *Download*(*ia*) ∧ |*Download.time*-*Access.Time*|<*δ*→ *insecure Association*	*ia* 访问网站，并且下载该网站上的 App 应用，则推断这 2 个动作之间存在安全风险关联
rRule-14:*DownloadApp*(*ia*) ∧ *Install*(*ia*,*app*) ∧ |*Install.time*- *Download.time*|<*δ* ∧ *Download.pkgName*=*Install.pkgName*→ *insecure Association*	*ia* 下载并安装被标记为“恶意软件”的 App 应用，则推断这 2 个动作存在风险关联`
rRule-15:*Install*(*ia*) ∧ *Run*(*ia*) ∧ *appType*='*malicious*' →*insecure Association*	安装并运行“恶意”软件的 2 个动作存在风险关联

参考文献：

[1] DHINGRA M. Legal issues in secure implementation of bring your own device (BYOD)[J]. Procedia Computer Science, 2016, 78: 179-184.

[2] Intel Security. Report of threat prediction in 2016 from McAfee labs [R/OL]. http://www.mcafee.com/cn/resources/reports/rp-threats-predictions-2016.pdf, 2016-06-10.

[3] Symantec. Internet security threat report[R/OL]. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, 2016-07-13.

[4] Wikipedia. Hillary clinton email controversy[EB/OL]. https://en.wikipedia.org/wiki/Hillary_Clinton_email_controversy, 2016-07-17.

[5] SARI P K, TRIANASARI N. Information security awareness measurement with confirmatory factor analysis[C]// International Symposium on Technology Management and Emerging Technologies,2014. ISTMET 2014. IEEE, 2014: 218-223.

[6] NGOQO B, FLOWERDAY S V. Information security behaviour profiling framework (ISBPF) for student mobile phone users[J]. Computers & Security, 2015, 53: 132-142.

[7] 陈波, 朱汉, 刘亚尚. 个人信息安全素养评测手机软件开发[J]. 信息安全与技术, 2014, 5(10): 50-55.
CHEN B, ZHU H, LIU Y S. Mobile software development for evaluation of personal information security literacy [J]. Information Security and Technology, 2014, 5(10): 50-55.

[8] Naval Postgraduate School. The center for information systems security studies and research, CyberCIEGE scenario development tool user's guide [EB/OL]. http://cisr.nps.edu/cyberciege/downloads/sdt.pdf. 2010-04-17.

[9] WARD R, BEYER B. Beyondcorp: a new approach to enterprise security[J]. The Magazine of USENIX & SAGE, 2014, 39(6): 6-11.

[10] DONNER M.Toward a security ontology[J], IEEE Security and Privacy,2003,1(3):6-7.

[11] RAZZAQ A, ANWAR Z, AHMAD H F, et al. Ontology for attack detection: an intelligent approach to Web application security[J]. Computers & Security, 2014, 45: 124-146.

[12] EKELHART A, KIESLING E, GRILL B, et al. Integrating attacker behavior in IT security analysis: a discrete-event simulation approach[J]. Information Technology and Management, 2015, 16(3): 221-233.

[13] BRAHMI I, BRAHMI H, YAHIA S B. A multi-agents intrusion detection system using ontology and clustering techniques[M]//Computer Science and Its Applications. Springer International Publishing,

2015: 381-393.

[14] MUNDIE D, MCINTIRE D M. An ontology for malware analysis[C]// International Conference on Availability, Reliability and Security, IEEE, 2013: 556-558.

[15] SOLIC K, OCEVCIC H, GOLUB M. The information systems' security level assessment model based on an ontology and evidential reasoning approach[J]. Computers & Security, 2015, 55: 100-112.

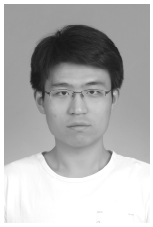
[16] MOULISWARAN S C, KUNMARC A, CHANDRASEKAR C. Inter-domain role based access control using ontology[C]// International Conference on Advances in Computing, Communications and Informatics,2015, 2015: 2027-2032.

[17] CHUN S A, GELLER J. Developing a pedagogical cybersecurity ontology[M]//Data Management Technologies and Applications. Springer International Publishing, 2014: 117-135.

[18] MCCLELLAND C D. Testing for competence rather than for intelligence[J]. American Psychologist,1973,28(1):1-24.

[19] PRAHALAD C K, HAMEL G. The core competence of the corporation[J]. Harvard Business Review, 1990, 68(3):79-91.

作者简介：



麦丞程（1990-），男，江苏南京人，南京师范大学硕士生，主要研究方向为移动安全、信息安全行为等。

陈波（1972-），男，江苏南通人，南京师范大学教授、硕士生导师，主要研究方向为移动安全、社会计算等。

周嘉坤（1992-），男，江苏南通人，南京师范大学硕士生，主要研究方向为安全人因分析、移动安全等。

于泠（1971-），女，江苏金坛人，南京师范大学副教授，主要研究方向为信息安全、社会计算。