文献引用格式：赵波，刘贤刚，刘行，等 .Android 应用程序个人信息安全量化评估模型研究 [J]. 通信技术，2020，53（08）：2019-2026.
ZHAO Bo,LIU Xian-gang,LIU Xing,et al.Quantitative Evaluation Model of Personal Information Security for Android Applications[J].Communications Technology,2020,53(08):2019-2026.

doi:10.3969/j.issn.1002-0802.2020.08.030

Android 应用程序个人信息安全量化评估模型研究 *

赵　波，刘贤刚，刘　行，胡　影

（中国电子技术标准化研究院，北京 100007）

摘　要：移动互联网应用程序的个人信息安全问题已经引起了社会大众的普遍关注，现有信息安全检测指标和衡量方法无法较好地满足移动互联网应用程序的个人信息安全评估。在此方向进行初步探索，以 Android 应用程序为评估对象，分析国内当前监管条件下移动互联网应用程序个人信息安全的相关要求，结合 Android 应用程序个人信息安全检测技术，利用层次分析法，提出了 Android 应用程序个人信息安全量化评估模型。通过 12 款不同类型的 Android 应用对比评估，验证了评估模型的有效性。

关键词：Android 应用；个人信息安全；层次分析法；量化评估
中图分类号：TP309　　**文献标志码：**A　　**文章编号：**1002-0802(2020)-08-2019-08

Quantitative Evaluation Model of Personal Information Security for Android Applications

ZHAO Bo, LIU Xian-gang, LIU Xing, HU Ying

(China Electronics Standardization Institute, Beijing 100007, China)

Abstract: The personal information security issues of mobile Internet applications have aroused general concern of the public. The existing information security detection indicators and measurement methods cannot meet the personal information security assessment of mobile Internet applications. This paper makes a preliminary exploration in this direction, takes the Android application as the evaluation object, analyzes the relevant requirements of personal information security of mobile Internet applications under the current domestic regulatory conditions, combines with the personal information security detection technology of Android applications, and uses AHP (analytic hierarchy process) to propose a quantitative assessment model of personal information security of Android applications. The comparative evaluation of 12 different types of Android applications indicates the effectiveness of this evaluation model.

Key words: Android application; personal information security; AHP (analytic hierarchy process); quantitative evaluation

* **收稿日期：**2020-04-05；**修回日期：**2020-07-10　Received date:2020-04-05;Revised date:2020-07-10
基金项目：国家重点研发计划项目“新型智慧城市技术标准体系与标准服务平台”（No.2018YFB2101400）
Foundation Item: National Key R&D Plan Project “New Smart City Technology Standard System and Standard Service Platform” (No.2018YFB2101400)
通讯联系人：liuxg@cesi.cn　Corresponding author:liuxg@cesi.cn

0 引 言

随着移动互联网的飞速发展，移动智能终端及运行于各类移动智能终端上的移动互联网应用程序（Mobile Internet Application，以下简称 App）已全面渗透入人们的工作和生活。中国互联网络信息中心发布的《第 45 次中国互联网络发展状况统计报告》[1] 显示，截至 2020 年 3 月，我国网民规模达 9.04 亿，其中使用手机上网的网民达 8.97 亿，占比达 99.3%。同时，根据中国网信网发布的《2019 年我国移动应用程序（APP）数量增长情况》[2]，截至 2019 年 12 月末，我国国内应用市场上监测到的 App 数量已达 367 万款。在依赖性上，2020 年第一季度国内手机网民人均安装 App 63 款，人均单日 App 使用时长达 6.7 h[3]。可见，App 已经成为人们工作和生活离不开的基础软件。

然而，App 在为用户提供便捷服务的同时，也带来了严重的个人信息安全问题，如 App 强制授权、过度索权、超范围收集个人信息的现象大量存在。中国消费者协会于 2018 年进行的 App 个人信息泄露情况调查显示，遇到个人信息泄露情况的人数占比达 85.2%[4]。全国信息安全标准化技术委员会秘书处发布的文件显示，App 存在的典型个人信息安全问题包括超范围收集个人信息、设置不合理账号注销条件、强制索取权限、无隐私政策、默认选择同意以及未充分明示个人敏感信息使用规则等 [5]。

针对 App 个人信息安全问题，国家监管部门陆续开展了多项针对性的监管活动。例如，中央网信办、工信部、公安部和国家市场监管总局等四部门联合开展的 App 违法违规收集使用个人信息专项治理行动（以下简称“四部门专项治理行动”），工信部开展的 App 侵害用户权益专项整治工作等。同时，相继发布了多个 App 个人信息安全相关监管文件，如《数据安全管理办法（征求意见稿）》《App 违法违规收集使用个人信息行为认定方法》以及 GB/T 35273–2020《信息安全技术 个人信息安全规范》等。这些监管活动和监管文件的有效执行，均依赖于对 App 的个人信息安全进行检测评估。如前文所述，App 个人信息安全问题不同于恶意代码、系统漏洞等传统信息安全问题，在相应的检测方法和评估准则方面仍缺少相关研究，特别是在 App 个人信息安全量化评估方面，目前仍处于探索阶段。

本文以市场占有率 80% 以上的 Android 系统为研究对象，对国内监管要求和 Android 应用个人信息安全检测方法进行综合分析，在检测技术可实现的基础上提出 Android 应用个人信息安全评估指标体系，通过按层次细分评估指标和层次分析法，对 Android 应用个人信息安全进行量化评估。需要说明的是，本研究仅关注移动设备端 App 的个人信息安全，暂不考虑 App 后端服务处理个人信息的行为。

1 App 个人信息安全要求与标准

App 个人信息安全量化评估通常应当以 App 个人信息安全评估标准为准则。然而，国内目前缺少直接针对 App 个人信息安全评估的标准。因此，本文对当前已发布的针对个人信息安全的部门规章、政策文件、标准文件进行分析，作为评估指标依据。

1.1 部门规章

为配合《网络安全法》中对个人信息保护的基本要求，有关行业主管和监管部门积极制定了细化的部门规章，其中和 App 个人信息安全保护相关的主要包括工信部发布的《电信和互联网用户个人信息保护规定》《移动智能终端应用软件预置和分发管理暂行规定》，网信办发布的《移动互联网应用程序信息服务管理规定》等。这些部门规章提出了收集、使用用户的个人信息，应当明确告知用户收集、使用个人信息的目的、方式和范围；收集、使用用户的个人信息须经用户同意；不得收集与所提供服务无关的个人信息或调用与所提供服务无关的终端功能；应当提供给用户选择终止服务、停止收集其个人信息以及注销账号等要求。

1.2 政策文件

《App 违法违规收集使用个人信息行为认定方法》是四部门专项治理行动的工作成果，为监管部门认定 App 违法违规收集使用个人信息行为提供了参考。该文件给出了 App 未公开收集使用规则，未明示收集使用个人信息的目的、方式和范围，未经用户同意收集使用个人信息，违反必要原则收集与其提供的服务无关的个人信息，未经同意向他人提供个人信息，未公布投诉、举报方式等，共 6 大类违法违规收集使用个人信息行为，且每一类详细列举了认定准则。该政策文件为提出 Android 应用程序个人信息安全评估的指标提供了直接依据。

1.3 标准文件

个人信息保护标准对于个人信息保护工作具有基础性、规范性和引领性作用，是本文提出评估指标的主要依据。

在国家标准层面，针对个人信息保护要求，目前已有标准包括 GB/T 35273–2020《信息安全技术 个人信息安全规范》、GB/T 34978–2017《信息安全技术 移动智能终端个人信息保护技术要求》以及《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（送审稿）》等。其中，《信息安全技术 个人信息安全规范》对个人信息以及个人敏感信息的范围进行了界定，明确了个人信息控制者在开展个人信息处理活动中应当遵循的基本原则，及其在对个人信息进行收集、保存、使用和对外提供等环节应遵守的相关要求，是目前使用最广泛的个人信息安全保护标准。《信息安全技术 移动智能终端个人信息保护技术要求》规范了全部或部分通过移动智能终端进行个人信息处理的过程，根据移动智能终端个人信息的分类和不同的处理阶段，对相应的个人信息保护提出了技术要求。《信息安全技术 移动互联网应用程序（App）收集个人信息基本规范（送审稿）》明确了移动互联网应用程序收集个人信息时应满足的基本要求，用以规范移动互联网应用程序运营者收集个人信息的行为。该标准附录中给出了地图导航、网络约车、即时通信、网络社区等 38 类常用服务类型可收集的最小必要信息

在行业标准方面，中国通信标准化协会已发布 YD/T 2781–2014《电信和互联网服务 用户个人信息保护 定义及分类》、YD/T 2782–2014《电信和互联网服务 用户个人信息保护 分级指南》以及 YD/T 3082–2016《移动智能终端上的个人信息保护技术要求》等行业标准。

2　App 个人信息安全检测技术

虽然 Android 应用个人信息安全检测的问题点与 Android 应用传统信息安全的检测点不同，但在基础检测技术上两者是一致的。Android 应用个人信息安全基础检测技术包括静态分析技术和动态分析技术。在静态分析和动态分析的基础上，要对个人信息安全问题进行判断，还需要人工进行分析。

2.1　静态分析技术

Android 应用静态分析技术包括资源文件扫描技术、代码特征扫描技术以及静态污点分析技术等。Android 应用的 APK 文件中包含 Dalvik 字节码文件和 AndroidManifest、图片、布局、so 文件等其他资源文件。资源文件扫描技术对 App 的 AndroidManifest 文件、布局文件等进行扫描，通过分析 App 的 AndroidManifest 文件可以获得 App 声明可能会使用的系统权限；通过分析布局文件可以获得 App 可能让用户输入的个人信息。代码特征扫描技术对反编译后的 Dalvik 字节码进行扫描，通过分析代码发现 App 调用的敏感 API、嵌入的第三方 SDK 等。其中，敏感 API 是指能够获取用户个人信息的 API。静态污点分析技术通过在反编译后的代码上进行静态污点追踪，识别特定数据在代码中的传播路径。静态污点分析可用于分析敏感 API 被调用时可能接收的参数值。静态分析技术的特点是覆盖的代码范围广，但准确度较低。

2.2　动态分析技术

Android 应用动态分析技术包括 App 动态运行技术、App 敏感 API Hook 技术、动态污点分析技术以及网络数据抓包技术等。App 动态运行技术是指在无人操作的情况下自动运行 App，自动触发 App 中的特定操作。在固定时间内，尽可能多地触发 App 中的不同操作，可提高动态运行代码的覆盖率。App 敏感 API Hook 技术通过在敏感 API 上添加 Hook，记录 App 在实际运行时调用敏感 API 的时间、传递的参数以及调用栈等。动态污点分析技术通过修改 Android 操作系统底层代码，追踪 App 在实际运行时污点数据的传播情况，在被打上污点标签的个人信息传播至文件、短信或网络出口时，记录该个人信息发送行为。网络数据抓包技术通过代理程序拦截 App 发送的网络数据包。结合在设备端的 Hook 技术和中间人攻击方法，可以在一定程度上拦截通过 SSL/TLS 等加密信道发送的明文数据。与静态分析相比，动态分析技术的特点是准确度较高，但代码覆盖率较低。

2.3　人工分析

对于 Android 应用的个人信息安全问题，技术分析通常用于收集基础数据。一款 App 是否确认存在个人信息安全问题，还需进一步进行人工分析判断。人工分析包括隐私政策分析、App 功能试用等。人工分析主要完成两方面的工作。一方面是对技术分析的结果进行问题判定，如通过技术分析可以获得 App 声明了哪些系统权限，但这些权限是否都是 App 实现业务功能所必须的权限，还需人工结合 App 的业务功能进行判定；另一方面是弥补技术分析无法进行的问题分析，如 App 的隐私政策是否说明个人信息收集使用情况、使用敏感系统权限时是否说明目的等。这些内容涉及到对自然语言语义的

理解，虽然当前有很多对自然语言处理的相关工作，但对隐私政策等的分析仍离不开人工判断。

3 App 个人信息安全量化评估模型

3.1 层次分析法

层次分析法（Analytic Hierarchy Process，AHP）[6]是一种定性与定量相结合、系统的、层次的分析方法。该方法将与最终的决策目标有关的要素按照其相互关联影响及相互隶属关系分解成目标、准则、方案等层次，通过对要素的两两比较，利用较少的定量信息使决策的思维过程数学化，从而为多目标、多准则或无结构特性的复杂决策问题提供简便的决策方法。

运用层次分析法构造决策模型时，可分为以下 4 个步骤。

（1）建立层次结构模型。按照决策的目标、考虑的要素、决策对象等建立层次结构，绘制层次结构图。

（2）构造判断矩阵。两两比较每一层的各要素，根据该要素对上一层要素的重要性构造判断矩阵。对比时采用相对尺度，以减少性质不同的要素相互比较的困难。成对比较矩阵的元素 a_{ij} 表示第 i 个要素相对于第 j 个要素的比较结果，这个值使用 Santy 的 1 ~ 9 标度方法给出。

表 1 Santy 1 ~ 9 标度表

标度	含义
1	两个要素具有相同的重要性
3	一个要素比另一个要素稍微重要
5	一个要素比另一个要素明显重要
7	一个要素比另一个要素强烈重要
9	一个要素比另一个要素极端重要
2、4、6、8	上述两相邻判断的中值
倒数	要素 i 与 j 比较的判断为 a_{ij}，则要素 j 与 i 比较的判断为 $a_{ji}=1/a_{ij}$

（3）层次单排序及一致性检验。假设某一层要素的 n 阶判断矩阵 $\boldsymbol{A}$ 的最大特征根为 $\lambda_{\max}$，其对应的特征向量经归一化后记为 $\boldsymbol{W}$。$\boldsymbol{W}$ 的元素为同一层要素对于上一层某要素相对重要性的排序权值，这一过程称为层次单排序。完成层次单排序后，为了避免出现违背常识的判断结果，需要对该次排序进行一致性检验。一致性指标用 CI 计算。CI 越小，说明一致性越大。CI 的定义为：

$$CI=\frac{\lambda_{\max}-n}{n-1}\begin{cases}CI=0, & \text{有完全的一致性}\\ CI\text{接近于}0, & \text{有满意的一致性}\\ CI\text{越大}, & \text{不一致性越严重}\end{cases} \quad (1)$$

为衡量 CI 的大小，引入随机一致性指标 RI，表示矩阵出现一致性随机偏离的可能性。矩阵阶数 n 与 RI 的对应关系如表 2 所示。

表 2 随机一致性指标 RI 对照表

n	RI
1	0
2	0
3	0.58
4	0.90
5	1.12
6	1.24
7	1.32
8	1.41
9	1.45
10	1.49

将 CI 和随机一致性指标 RI 进行比较，得出检验系数 CR，$CR=CI/RI$ 如果 $CR<0.1$，则认为该判断矩阵通过一致性检验。

（4）层次总排序及一致性检验。层次总排序是指从最高层到最低层依次计算某一层所有要素对于最高层相对重要性的权值。假设第一层（A 层）m 个要素对总目标的权重为 $(a_1,a_2,\cdots,a_m)$，第二层（B 层）n 个要素对 A 层中要素 A_j，$j\in(0,m)$ 的权重为 $(b_{1j},b_{2j},\cdots,b_{nj})$，一致性指标为 CI_j，随机一致性指标为 RI_j 则 B 层第 i 个要素对总目标的权重为 $\sum_{j=1}^{m}a_jb_{ij}$。若 B 层中与 A_j 相关的要素的成对比较判断矩阵在层次单排中满足一致性检验，一致性指标为 CI_j，随机一致性指标为 RI_j，则 B 层层次总排序的 CR：

$$CR=\frac{a_1CI_1+a_2CI_2+\cdots+a_mCI_m}{a_1RI_1+a_2RI_2+\cdots+a_mRI_m} \quad (2)$$

当层次总排序的 $CR<0.1$ 时，认为层次总排序通过一致性检验。

3.2 量化评估模型

通过对部门规章、政策文件、标准规范的研究分析可以发现，App 个人信息安全问题包含个人信息主体权益保障和个人信息安全保障两个方面。结合个人信息安全规范中提出的个人信息安全基本原则，本文以明确告知、选择同意、最小必要、确保

安全和主体参与 5 个要素作为 Android 应用个人信息安全的直接评价准则。在此基础上，按照层次分析法的决策思维，结合 Android 应用的特点和检测技术，从隐私政策、权限申请、信息收集、第三方共享以及账号注销等方面对直接评价准则进行逐层分解。对于各层指标，按照该指标不符合时对个人信息主体权益减损多少或可能造成的个人信息安全影响大小进行两两比较。

本文构造的层次模型如图 1 所示。对于第一层的直接评价准则层，根据相关要求与标准文件描述，认为该层各要素对 Android 应用个人信息安全的重要度相同，因此该层要素相对总目标的权重 $\boldsymbol{W}$=(0.2,0.2,0.2,0.2,0.2)。而对于从第二层开始的各要素，根据其对上一层要素的重要程度两两进行比较，确定其相对上一层要素的权重。

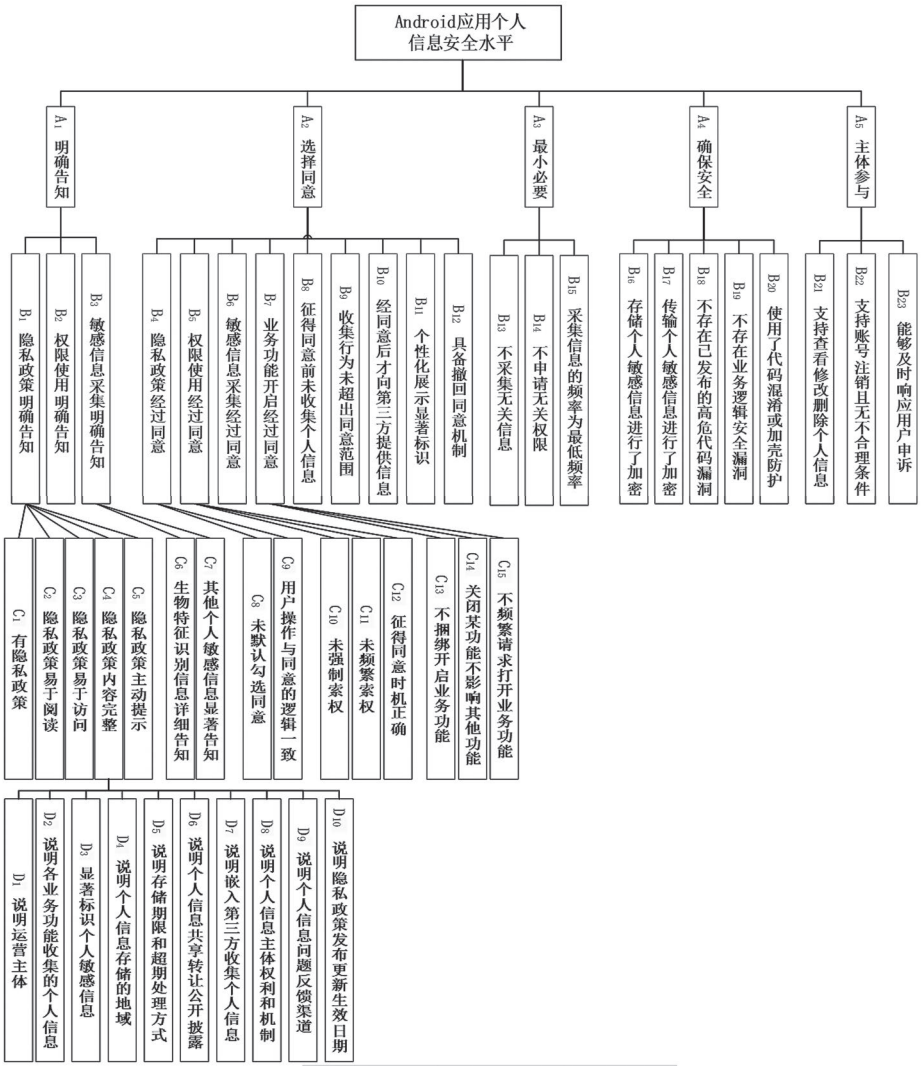

图 1　Android 应用个人信息安全评估指标层次结构模型

以 C_1 ~ C_5 为例，其相对 B_1 的权重确定过程如下。

首先根据 B_1 的重要度，两两比较 C_1 ~ C_5 的要素，构造判断矩阵 $\boldsymbol{A}_c$。

$$\boldsymbol{A}_c=\begin{bmatrix} C & C_1 & C_2 & C_3 & C_4 & C_5 \\ C_1 & 1 & 7 & 5 & 2 & 6 \\ C_2 & 1/7 & 1 & 1/4 & 1/6 & 1/3 \\ C_3 & 1/5 & 4 & 1 & 1/4 & 3 \\ C_4 & 1/2 & 6 & 4 & 1 & 5 \\ C_5 & 1/6 & 3 & 1/3 & 1/5 & 1 \end{bmatrix} \quad (3)$$

计算判断矩阵 $\boldsymbol{A}_c$ 的最大特征根 λ_{max}=5.278 7、一致性指标 CI=0.069 7 和检验系数 CR=0.062 2。由 CR<0.1 可知，该判断矩阵通过一致性检验，各项权重无逻辑错误。由判断矩阵的特征值向量归一化，可得 C_1 ~ C_5 要素对 B_1 的重要度权重为 $\boldsymbol{W}$=(0.455 2, 0.040 0,0.125 9,0.308 9,0.070 0)。

按照同样的方法，计算各层要素对上一层要素的重要度权重，再根据 3.1 节描述的层次总排序计

算方法计算各层要素对总目标的重要度权重，最终计算结果如图 2 所示。经检验，该层次结构模型的层次总排序 $CR<0.1$，满足一致性指标。评估中使用该层次结构模型作为 Android 应用的量化评估模型。

设 Android 应用个人信息安全水平的满分为 100，各指标项的权重值乘以 100 为该项的分值，对 App 满足的指标项的分值求和，即为该 App 个人信息安全水平的量化评分。

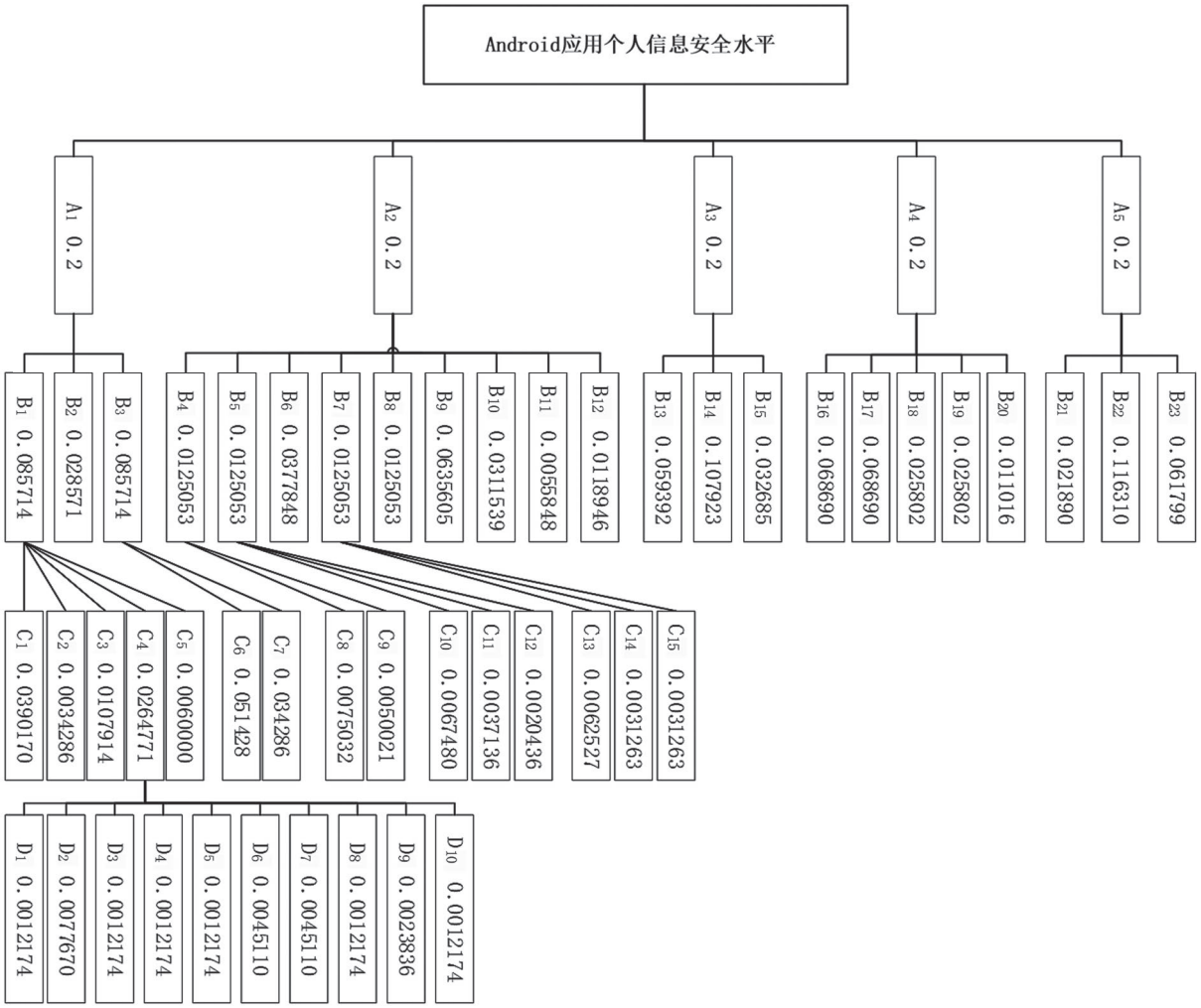

图 2　评估指标层次结构权重

4　评估实例分析

按照上述评估模型，本文选择了 12 款不同服务类型的 Android 应用进行对比评估。表 3 显示了每款 App 对应的主要个人信息安全问题及其对应的量化评分。可以看出，通过提出的量化评估模型，量化评分结果可以较好地反映 App 的个人信息安全保护水平。对于存在无隐私政策、无法注销账号、申请无关权限等较严重个人信息安全问题的 App，本文所提方法会打出较低的评分。而对于打开权限时未同步明示目的、频繁提示缺少的权限等问题，这些问题虽然在一定程度上造成用户知情权和用户体验的下降，但实际对用户个人信息安全的影响低于无隐私政策等问题。对于仅存在这些问题的 App，本文所提方法给出了较高的评分。利用本文所提出的量化评估模型，通过量化评分结果的对比，一方面可以促进当前评分较低的 App 改进自身存在的严重个人信息安全问题，快速提升自身评分；另一方面可以鼓励当前评分较高的 App 进一步提升自身的个人信息保护水平，从而取得更高的分数。因此，本文所提评估模型具有较好的实用意义。

表 3　12 款 Android 应用的对比评分

序号	App 所属服务类型	主要个人信息安全问题	量化评分
App1	即时通信	打开权限时未同步明示目的；频繁索取地理位置权限；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；隐私政策内容不完整；未使用加壳防护	91.98
App2	网络社区	收集个人敏感信息时未同步告知目的；强制索取存储权限；部分个人信息无法修改；隐私政策内容不完整；未使用加壳防护	91.34
App3	网络约车	打开权限时未同步明示目的；征得用户同意前收集个人信息；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；App 在后台运行时读取地理位置信息；未使用加壳防护	87.96
App4	新闻资讯	未完整说明各业务功能收集的个人信息；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；未主动提醒用户阅读并同意隐私政策；打开权限时未同步明示目的；收集个人生物特征信息时未显著告知目的和使用规则；未使用加壳防护	85.96
App5	安全管理	隐私政策内容不完整；诱导用户略过隐私政策；后台运行时收集用户个人信息；用户注销账号机制无效；未使用加壳防护	82.26
App6	拍照美化	未完整说明各业务功能收集的个人信息；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；打开权限时未同步明示目的；申请与业务功能无关的位置权限；读取 IMEI 和地理位置信息的频率超出实际需要的范围	78.74
App7	网络借贷	隐私政策内容不完整；诱导用户略过隐私政策；未充分明示个人敏感信息收集目的；频繁索取地理位置权限；打开权限时未同步明示目的；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；App 在后台运行时收集用户的个人信息；设置不合理注销条件	73.13
App8	在线视频	隐私政策内容不完整；隐私政策不易访问；诱导用户略过隐私政策；强制索取地理位置权限；打开权限时未同步明示目的；征得用户同意前收集使用个人信息；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；申请与业务功能无关的权限；App 在后台运行时收集用户的个人信息；未使用加壳防护	72.44
App9	日常工具	隐私政策内容不完整；强制索取电话权限；打开权限时未同步明示目的；征得用户同意前收集个人信息；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；收集个人信息的频率超出实际需要的范围；无法注销账号；申诉渠道不可用；未使用加壳防护	68.57
App10	主题壁纸	隐私政策内容不完整；强制索取地理位置权限；未说明 App 中嵌入的第三方 SDK 收集个人信息的行为；申请与业务功能无关的权限；收集个人信息的频率超出业务功能实际需要的范围；设置不合理注销条件；未使用加壳防护	68.19
App11	手机游戏	无隐私政策；打开权限时未同步明示目的；申请权限的时机不正确；无法注销账号；未使用加壳防护	63.66
App12	快递配送	无隐私政策；强制索取权限；强制捆绑其他业务功能；打开权限时未同步明示目的；无法注销账号；申诉渠道不可用	57.28

5　结　语

本文针对 Android 应用个人信息安全的量化评估问题，研究了 App 个人信息安全的要求与标准，结合 Android 应用个人信息安全的检测技术，提出了层次结构的 Android 应用个人信息安全评估指标项。按照某项指标不符合时对个人信息主体权益减损多少或可能造成的个人信息安全影响大小，采用层次分析法计算了各项指标的权重。最后，通过在 12 款 App 上的对比使用，验证了方法的有效性。本文所提指标虽然针对 Android 应用，但其中大部分指标和方法同样适用于 iOS 应用个人信息安全的量化评估。在未来工作中，计划更深入地研究评估指标的分层拆解，进一步减小同一层次不同指标间的关联性，并通过多位专家共同决策的方式提高指标间比较结果的客观性，从而提高整个评估模型的准确性。

参考文献：

[1] 中国互联网络信息中心 . 第 45 次中国互联网络发展状况统计报告 [EB/OL].(2020–04–28)[2020–04–30]. http://www.cac.gov.cn/2020–04/27/c_1589535470378587.htm.

China Internet Network Information Center.The 45th China Statistical Report on Internet Development[EB/OL].(2020-04-28)[2020-04-30].http://www.cac.gov.cn/2020-04/27/c_1589535470378587.htm.

[2] 中国网信网 .2019 年我国移动应用程序 (APP) 数量增长情况 [EB/OL].(2020-02-17)[2020-04-30].http://www.cac.gov.cn/2020-02/17/c_1583491211996616.htm.
Cyberspace Administration of China.2019 China Mobile App (APP) number growth[EB/OL].(2020-02-17)[2020-04-30].http://www.cac.gov.cn/2020-02/17/c_1583491211996616.htm.

[3] 极光 .2020 年 Q1 移动互联网行业数据研究报告 [EB/OL].(2020-05-01)[2020-05-04].https://www.jiguang.cn/reports/483.
Aurora Mobile.2020 Q1 Mobile Internet Industry Data Research Report[EB/OL].(2020-05-01)[2020-05-04].https://www.jiguang.cn/reports/483.

[4] 新华网 . 中消协：八成多受访者遭 APP 个人信息泄露 [EB/OL].(2018-08-30)[2020-04-30].http://www.xinhuanet.com/fortune/2018-08/30/c_1123350774.htm.
Xinhua News.China Consumers Association: More than 80% of respondents suffered APP personal information leakage[EB/OL].(2018-08-30)[2020-04-30].http://www.xinhuanet.com/fortune/2018-08/30/c_1123350774.htm.

[5] 全国信息安全标准化技术委员会秘书处 . 网络安全标准实践指南—移动互联网应用程序 (App) 个人信息安全防范指引 (征求意见稿)[EB/OL].(2020-03-30)[2020-04-30].https://www.tc260.org.cn/front/postDetail.html?id=20200330091643.
Secretariat of National Information Security Standardization Technical Committee.Cyber Security Standard Practice Guide-Mobile Internet Application (App) Personal Information Security Prevention Guidelines (Draft for Comment)[EB/OL].(2020-03-30)[2020-04-30].https://www.tc260.org.cn/front/postDetail.html?id=20200330091643.

[6] MBA 智库 · 百科 . 层次分析法 [EB/OL].[2020-04-30].https://wiki.mbalib.com/wiki/ 层次分析法 .
MBA Think Tank · Encyclopedia.Analytic Hierarchy Process[EB/OL].[2020-04-30].https://wiki.mbalib.com/wiki/ 层次分析法 .

作者简介：

赵　波（1967—），男，硕士，高级工程师，主要研究方向为信息安全、人工智能、计算机、软件；

刘贤刚（1980—），男，博士，高级工程师，主要研究方向为数据安全和个人信息保护、人工智能、生物特征识别；

刘　行（1989—），男，博士，工程师，主要研究方向为个人信息保护；

胡　影（1980—），女，博士，工程师，主要研究方向为数据安全和个人信息保护、人工智能安全。