

基金项目论文

移动应用远程诊断与热修复方法

韩康^{1,2} 洪滢³ 孙艳霞⁴ 张啸岳¹ 于佳琳¹ 金小俊^{1,2}

(1.北京大学现代农业研究院, 山东潍坊 261325; 2. 镇江禾硕科技孵化有限公司, 江苏镇江 212400;

3.江苏农林职业技术学院国际教育学院, 江苏镇江 212400; 4.南京交通职业技术学院轨道交通学院, 江苏南京 211188)

摘要: 本文提出了一种移动应用线上问题远程诊断与热修复方法。诊断功能包括, 通过长连接远程下发指令至移动客户端, 并设置触发条件, 若发现线上问题, 采集以下信息: 设备和用户基本信息、堆栈信息、网络请求接口的流水信息、内存中的变量值。其中触发条件为一段返回布尔值的代码字符串, 移动客户端接收到指令后通过轻量级的解释器将字符串解析成可执行的代码, 并嵌入客户端附着执行。代码执行后若条件满足, 即发生了指定的问题, 采集上述调试信息以供诊断使用。热修复功能包括, 当诊断到问题所在后, 下发字符串代码至指定的方法或函数, 并通过解释器解析成可执行的代码后整体或部分替代原方法或函数, 替代的过程通过 AOP 实现。该方法通过下发预置触发条件的指令并结合解释器实现了一套完整的远程诊断和修复功能, 提高了问题诊断以及修复的效率, 且该方法能够顺利通过各移动平台严格的审核。

关键词: 软件开发; 移动应用; 线上问题; 远程诊断; 热修复

中图分类号: TP311.56

文献标识码: A

DOI: 10.3969/j.issn.1003-6970.2023.10.001

本文著录格式: 韩康,洪滢,孙艳霞,等.移动应用远程诊断与热修复方法[J].软件,2023,44(10):001-004+133

Methods for Remote Diagnostics and Hot Fix in Mobile Applications

HAN Kang^{1,2}, HONG Ying³, SUN Yanxia⁴, ZHANG Xiaoyue¹, YU Jialin¹, JIN Xiaojun^{1,2}

(1.Peking University Institute of Advanced Agricultural Sciences, Weifang Shandong 261325;

2.Zhenjiang Heshuo Technology Incubator Co., Ltd., Zhenjiang Jiangsu 212400;

3. School of International Education, Jiangsu Vocational College of Agriculture and Forestry, Zhenjiang Jiangsu 212400;

4. School of Rail Transportation, Nanjing Vocational Institute of Transport Technology, Nanjing Jiangsu 211188)

[Abstract]: This paper presents a method for remote diagnosis and hotfix of online issues in mobile applications. The diagnostic functionality includes remotely sending instructions to the mobile client through a persistent connection and setting trigger conditions. If an online problem is detected, the following information is collected: device and user basic information, stack trace information, sequential information of network request interfaces, and variable values in memory. The trigger condition is a code string that returns a boolean value. Upon receiving the instructions, the mobile client parses the string into executable code using a lightweight interpreter and embeds it for execution. If the condition is satisfied after code execution, indicating the specified problem has occurred, the aforementioned debugging information is collected for diagnostic purposes. The hotfix functionality involves sending code strings to the designated methods or functions once the problem is diagnosed. The code strings are parsed into executable code by the interpreter and used to partially or entirely replace the original methods or functions, which is accomplished through aspect-oriented programming (AOP). This method provided a complete remote diagnosis and repair solution by sending preconfigured trigger condition instructions and utilizing an interpreter. It enhances the efficiency of problem diagnosis and repair while successfully passing strict auditing processes on various mobile platforms.

[Key words]: software development; mobile applications; online issues; remote diagnostics; hot fix

基金项目: 国家自然科学基金项目 (32072498); 泰山学者工程资助项目

作者简介: 韩康 (1990—), 男, 学士, 工程师, 从事软件工程与计算机应用研究工作。

通讯作者: 金小俊 (1987—), 男, 博士生, 副研究员, 从事人工智能技术研究工作。

0 引言

移动应用随着用户量增加后会由于用户使用环境的复杂性和不可知性, 出现一些难以在测试端重现的问题, 这些问题通常会在特定用户群或者特定设备上出现, 在交付测试阶段很难模拟出现问题的环境, 而且用户在描述问题时只是简单的现象描述, 因此排查问题时可用信息甚少, 造成问题诊断困难且周期长^[1,2], 即便侥幸查到问题所在, 修复问题仍然需要依赖发版^[3]。现有技术中, 虽也有热修复功能的开源技术, 比如 JSPatch, 但近年来苹果公司针对运用这些 JavaScript (JS) 脚本相关的热修复技术加强了审核, 大部分使用该技术实现热修复功能的产品都遭遇苹果公司的下架处理^[4,5]。

为解决现有技术存在的不足, 本文首先对已经发布上线的版本出现的在测试端难以模拟和重现的问题, 提供了一种远程诊断的方法, 通过下发指令至目标设备, 抓取排查问题所需的环境和调试信息用于研发人员调查问题出现的原因; 然后本文提供了一种轻量级的热修复方案, 通过代码解释器解决了热修复的规则限制, 使具有热修复功能的产品能顺利通过各移动平台严格的审核。

1 系统组成与方法流程

移动应用远程诊断与热修复系统组成包括监控告警模块、信息组合模块、信息上传模块和热修复模块。其中监控告警模块分为应用状态管理 (Application Performance Management APM) 监控和异常预警, 异常发生时将自动上传预置的埋点日志。信息组合模块为诊断信息所需的必要构成, 包括设备基本信息、设备运行信息、用户信息、调试日志等。上传组成 (下发埋点触发规则) 则是在发生问题时用于从用户端获取特定

的诊断信息。热修复模块则是通过解释器将下发字符串转成代码以实现动态修复。

远程诊断与热修复方案总体流程为预先在 App 埋点日志, 当发生 APM 预警或者异常状态时触发日志上传。另外, 当用户反馈问题时, 可通过静默推送下发埋点并在指定规则满足的状态下触发获取用户设备环境下的各类诊断日志信息。除此之外, 在分析定位到问题后, 也可下发代码通过解释器实现热修复。如图 1 所示为系统组成与方案流程示意图。

2 远程诊断

诊断指令格式为 JavaScript Object Notation (JSON) 文本, 通过长连接下发至移动应用客户端。如图 2 所示为远程诊断系统总体方案流程示意图。诊断指令包含 9 类信息, 用于完整描述所需诊断的版本信息、设备信息以及环境信息。具体指令内容如下所示:

- (1) 当前诊断指令所针对的客户端版本号;
- (2) 当前诊断指令的 ID;
- (3) 当前诊断指令所针对的客户端 bundleId;
- (4) 当前诊断指令是单次生效或是持久生效;
- (5) 当前诊断指令所嵌入的代码块类名;
- (6) 当前诊断指令所嵌入的代码块方法或函数;
- (7) 当前诊断指令嵌入方法或函数中的执行时机 (原方法或函数执行前 / 后执行或替代执行);
- (8) 当前诊断指令的触发条件;
- (9) 当前诊断指令所需采集的信息。

其中, 当前诊断指令所需采集的信息又包含三方面的内容: 1) 所需采集的程序执行中的变量值或方法 / 函数的返回值。数组格式, 元素为代码字符串; 2) 需

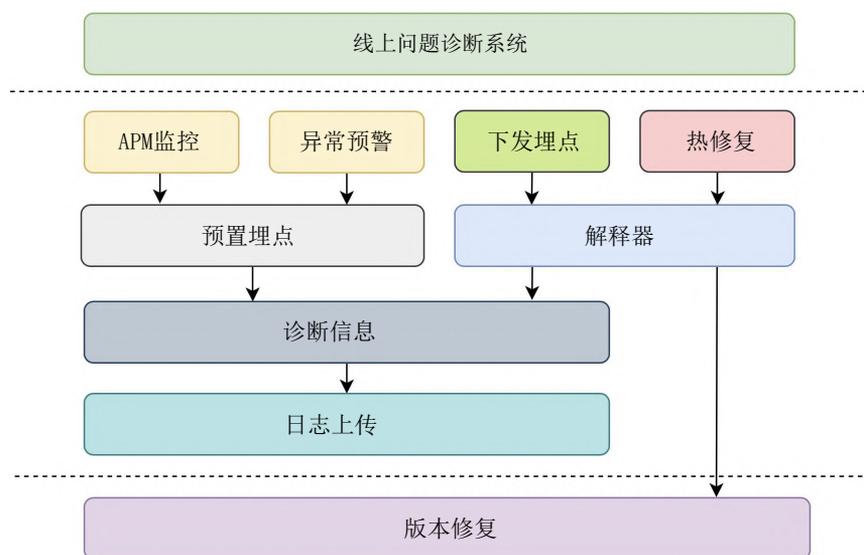


图 1 系统组成与方案流程示意图

Fig.1 Schematic diagram of system composition and scheme flow

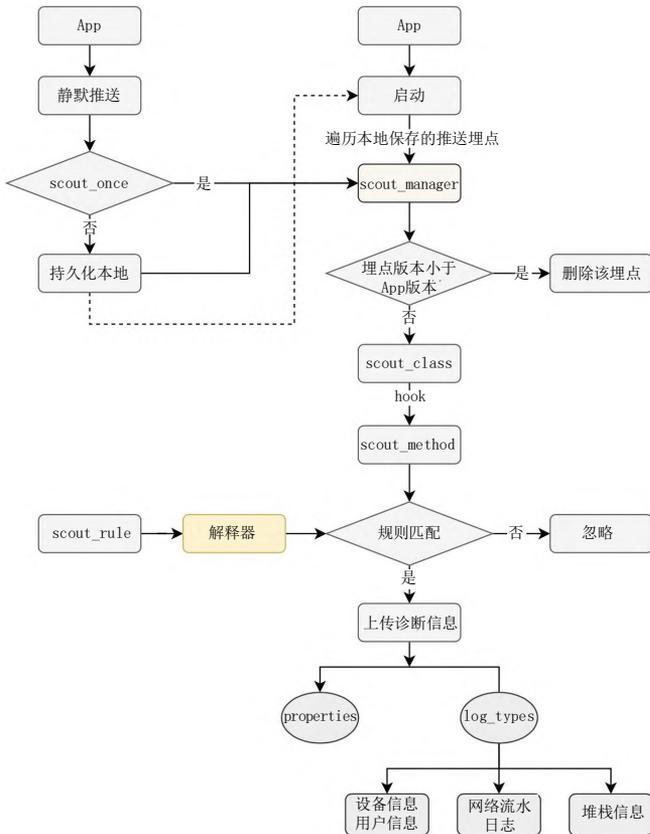


图 2 远程诊断系统总体方案流程示意图

Fig.2 Flowchart of the overall scheme of remote diagnosis system

要上传的调试信息。数组格式，元素为调试信息的枚举值，包括设备和用户基本信息、堆栈信息、用户网络请求接口的流水信息；3) 网关名。数组格式，元素为网关接口名，设置后只采集指定网关请求接口的流水。

移动客户端接收到诊断指令后，其执行步骤为：判断诊断指令所针对的客户端 bundleId 和版本号，只有在这两个都匹配上的情况下才会执行诊断指令；判断诊断指令是单次生效或是持久生效，若是持久生效则将指令保存到本地，在应用每次运行时诊断指令都会执行；获取诊断指令的触发条件，若是多个条件，则遍历执行。指令的触发条件为返回布尔值的表达式，字符串格式，通过解释器解析成可执行的表达式代码；获取诊断指令条件代码所需嵌入的类和方法名，并使用 AOP 的方式 Hook 住该类中的方法（比如可使用开源库 Aspects），当该方法执行时附着执行诊断条件代码；诊断指令条件代码嵌入的方法或函数执行时，根据诊断指令中的执行时机 / 方式执行诊断触发的条件代码，若条件满足，则触发诊断信息的采集。

诊断信息采集的条件触发后，获取诊断指令中所需采集的内容。若需要采集程序执行中的变量值，则读取

该变量值的变量名，并通过 runtime（安卓平台为反射）的方式获取该变量值；若需要采集具有返回值的单个步骤或多个步骤的方法或函数，则通过解释器将字符串解析成代码并执行获取返回值。获取所需采集的调试信息，包括：(1) 设备和用户基本信息，如设备名称、系统版本号、设备类型、UUID、应用版本号、内存 / CPU / 磁盘使用率、用户信息、登录名、用户 ID、账号状态；(2) 堆栈信息；(3) 获取诊断指令中指定的网关名，上传网关名对应接口的请求参数和返回内容的记录。对于网络请求的流水，其实施流程如下：

客户端接收诊断指令后，读取需要记录的网关名，每次网络请求时，遍历需要记录的网关列表，若该次网络请求的网关在列表中，则将网络请求数据记录到本地，同一个网关最多记录 3 条，超过 3 条，先进先出。当诊断采集信息的条件触发后，读取本地保存的网关数据请求记录并上传。对于诊断指令下发的目标和范围，通常情况下，用户遇到的问题不会是孤立情况，某一个用户遇到的问题，其他用户也可能会遇到，因此下发的规则不仅仅可以下发给反馈问题的用户，还需要能够下发给其他用户（灰度下发），一旦有用户遇到相同的问题即触发诊断日志的上传。

另外一方面，客户端可以同时接收并记录多个诊断指令，当这些诊断信息采集的条件满足的时候分别触发所需采集的调试信息并上传。诊断信息采集后，由客户端调用接口上传至服务器，服务器接收到采集的信息后通过 MIS 系统进行展示。当发现某次下发的诊断指令存在问题时，系统需要能够通过下发撤销诊断的指令用于删除之前下发的诊断指令。撤销诊断的指令内容为所需撤销的诊断指令的 ID，为数组格式，可一次性撤销多个诊断指令。

3 热修复

热修复指令同诊断指令，格式为 JSON 文本，通过长连接下发至移动应用客户端。指令包含 7 类信息，用于描述热修复的环境和执行信息。具体指令内容如下所示：

- (1) 当前热修复指令所针对的客户端版本号；
- (2) 当前热修复指令的 ID；
- (3) 当前热修复指令所针对的客户端 bundleId；
- (4) 当前热修复指令是单次生效或是持久生效；
- (5) 当前热修复指令所嵌入的代码块类名；
- (6) 当前热修复指令所嵌入的代码块方法或函数；
- (7) 当前热修复指令需要执行的代码字符串。

移动客户端接收到热修复指令后，其执行步骤为：判断热修复指令所针对的客户端 bundleId 和版本号，只有

在全部匹配的情况下才会执行热修复指令；判断热修复指令是单次生效或是持久生效，若是持久生效则将指令保存至本地，在应用每次运行时热修复指令均会执行；获取热修复指令执行代码的字符串，通过解释器将字符串转换成可执行的代码，解释器的原理为匹配代码关键字，如点符号为 setter 或 getter 方法、if 字符为条件判断、[] 为执行方法，可直接转换成 performSelector 方法执行（安卓平台类似机理）；获取热修复指令代码所需嵌入的类和方法名，使用 AOP 的方式 Hook 该类中的方法，当该方法执行时附着执行热修复代码；和诊断指令相同的，热修复指令也支持撤销操作。

4 应用实例

在实际应用中，根据问题出现的类和方法所在位置，指定诊断条件与修复内容。如用户在使用 App 过程中发现页面布局错乱，其指令内容可根据指定的类名

和方法名，通过 Method Swizzling 技术 Hook 相应执行方法，并将修复的代码通过推送下发，再结合解释器解析成代码插入原先方法体中。执行方式可在方法执行前 / 后插入，或者整体替换原方法。推送下发的远程诊断指令内容及释义如表 1 所示。

表 2 为修复该问题的热修复指令。修复方法为将布局变量 current_y 的值增加 44。具体为通过 Method Swizzling 技术 Hook 类 MainOrderInfoHeaderView 中的 drawRect: 方法，并在其中添加代码执行内容 self.current_y += 44;。热修复指令内容与释义如表 2 所示。

5 结语

本文提出了一种移动应用线上问题远程诊断和热修复的方法。远程诊断方案流程为首先通过长连接下发指令至移动客户端，设置触发条件，若发现线上问题，则

表 1 远程诊断指令示例

Tab.1 Examples of remote diagnostic instructions

指令	释义
<pre>"saic_scout": [{ "scout_version": "1.0.0", "scout_id": "scout_1001", "scout_needstore": 0, "scout_class": "MainOrderInfoHeaderView", "scout_method": "drawRect:", "scout_option": 2, "scout_rule": ["self.current_y < 44;"], "scout_report": { "properties": ["self.current_y;"], "log_types": [1, 2, 4], } }, "predicate": ["/biznet/login", "/biznet/user"] }]</pre>	<p>指令针对的客户端版本号为 1.0.0； 指令 id 为 scout_001； 该指令单次有效，无需存储； 需要 hook 的类为 MainOrderInfoHeaderView，方法名为 drawRect:； hook 方法的执行时机为方法执行前； 指令的触发条件为类中的 current_y 变量值小于 44； 上报信息包括 current_y 变量值、设备信息、网络日志和当前堆栈信息，上报的网络日志接口为 /biznet/login 和 /biznet/user 两个接口。</p>

表 2 热修复指令示例

Tab.2 Examples of hot repair instructions

指令	释义
<pre>"saic_scout": [{ "scout_version": "1.0.0", "scout_id": "scout_fix_1001", "scout_needstore": 1, "scout_class": "MainOrderInfoHeaderView", "scout_method": "drawRect:", "scout_option": 2, "scout_fix": "self.current_y += 44;" }]</pre>	<p>指令针对的客户端版本号为 1.0.0； 指令 id 为 scout_fix_1001； 该指令需持久化并持续生效； 需要 hook 的类为 MainOrderInfoHeaderView，方法名为 drawRect:； hook 方法的执行时机为方法执行前； 指令的代码执行内容为将类中的 current_y 变量值加上 44；</p>

..... 下转第133页

《信息安全技术个人信息安全规范》《信息安全技术健康医疗数据安全指南》GB_T 39725-2020 等对医疗机构的数据隐私和安全提出了严格的要求。

此外，医院还需要密切关注网络安全领域的新兴技术和攻击方式，并不断更新和完善网络安全技术体系。例如，加强对无线网络的安全管理，采用强密码和加密技术，防止未经授权的访问。另外，对新兴技术如区块链、边缘计算和虚拟化等的安全应用和防护也是未来的发展方向。

6 总结

医院网络安全是当前亟待解决的重要问题。本论文通过研究医院网络安全运营体系，提出了一系列建议和策略，旨在构建健全的网络安全保障体系。

首先，建立网络安全管理机构是确保医院网络安全的关键。该机构应由专业的安全团队组成，负责制定安全策略和规范，并监测和应对安全威胁。其职责还包括与相关机构和专家进行合作和交流，不断更新和完善网络安全防护手段。

其次，加强员工的安全意识培训是保障医院网络安全的重要环节。通过定期的培训和教育活动，提高员工对网络安全风险和安全操作的认识，减少人为失误和安全漏洞的发生。此外，建立严格的权限管理制度，限制员工的网络访问权限，也是提高网络安全的有效手段。

在技术层面上，采取一系列安全技术措施能够有效提升医院网络的安全性和稳定性。其中包括部署网络防火墙、对网络通信进行加密、采用身份认证机制控制访问权限、安装网络入侵检测系统和安全信息及事件管理系统等。

此外，定期进行安全性评估和渗透测试，建立监控

系统和日志审计机制，有助于发现安全漏洞和弱点，并及时采取措施进行修复。通过持续监测和审计网络活动，可以追踪安全事件的发生和传播，从而更好地保护医院网络的安全。

总而言之，医院网络安全是一项重要而复杂的任务，需要综合运用管理、培训和技术手段来构建健全的安全保障体系。只有这样，医疗机构才能对患者隐私进行有效保护，并保障医疗数据的安全性、完整性和可用性，以及维护机构的声誉和信任。

参考文献

- [1] 冯东建.疫情下的医院网络安全运营思考[J].中国质量万里行,2022,354(10):66-69.
- [2] 张红彬.医院网络安全体系构建与实现探析[J].网络安全技术与应用,2018,212(8):95+112.
- [3] 汤斌,黄玉成.三级等保下医院信息系统安全优化方案实践[J].中国医疗设备,2018,33(9):136-140.
- [4] 张红霞,周麒,吴奇,等.一院多区场景下的数字化医院网络安全体系构建[J].数字通信世界,2023,220(4):89-91.
- [5] 赖建华,张可同,陈雨婕.基于医院等级保护2.0的实践思考[J].软件,2020,41(3):114-117.
- [6] 胡立.如何构建网络安全策略[J].计算机与网络,2019,45(15):50-51.
- [7] 梁晴.基于自适应安全3.0架构的网络安全运营方案研究[J].网络安全技术与应用,2023,267(3):1-2.
- [8] 王晟,赵建福,李超峰,等.持续化网络安全运营体系研究[J].电信工程技术与标准化,2020,33(12):37-41.

..... 上接第4页

分别采集设备、环境和堆栈信息，用于问题的诊断与排查。其中触发条件为代码字符串，移动客户端接收到指令后通过轻量级的解释器将字符串解析成可执行的代码，并嵌入客户端附着执行。代码执行后若条件满足，即发生了指定的问题，采集上述调试信息以供诊断使用。另一方面，当诊断到问题所在后，进一步通过热修复功能对问题进行修复，通过解释器解析热修复代码，整体或部分替代原方法或函数，替代的过程通过 AOP 实现。实践表明，本文提出的移动应用远程诊断与热修复方法灵活、高效、扩展性强，具有较高实际应用价值。

参考文献

- [1] 宓云翀,孙轶康,钱虹.移动医疗应用程序产品安全性评价研究进展[J].中国医学装备,2021,18(2):162-165.
- [2] 季莹莹,王月领,虞成磊,等.移动应用程序安全监测检测平台研究[J].中国新通信,2023,25(7):110-112.
- [3] 任远,丁玲,戚伟.Uni-App移动应用开发技术分析[J].电子技术与软件工程,2023(3):41-44.
- [4] 杜帅,鄂海红,许可.混合移动应用开发模式的新策略[J].软件,2015,36(6):12-17.
- [5] 熊建芳.Android App功能插件化机制的研究与实现[J].智能计算机与应用,2019,9(1):235-238.