**广东南方新媒体股份有限公司2024年终端应用安全加固服务采购需求**

一、 项目背景

近年来，终端应用被破解和感染恶意病毒已经司空见惯，甚至形成了产业链，这些恶意行为都大大损害了用户和开发者的利益。各大运营商针对移动应用的安全扫描也采用新标准，对于安全要求更加精细化和高标准。随着广东南方新媒体股份有限公司业务的不断发展，广东南方新媒体股份有限公司的终端应用越来越多，省内外专网业务，省内手机业务，专网应用商城、互联网电视业务自研应用等，都需要进行安全扫描检查和相关的应用加固服务，来满足各地各运营商的安全扫描要求和运行安全。

因此本项目拟采购第三方加固服务和安全扫描检测平台服务，将更好的对广东南方新媒体股份有限公司移动应用进行安全检查和安全防护，以确保广东南方新媒体股份有限公司终端应用服务安全平稳的发展需要。

二、 业务需求

本项目总体业务需求如下：

(1)对应用商城合作应用进行安全扫描检测，确保进入应用商城的移动应用的安全使用。

(2)对广东南方新媒体股份有限公司自研或合作运营等移动端或者盒子端的终端应用App及办公OA等进行安全加固服务，包括android应用，SDK应用，h5应用等。

(3)所有的服务产品需进行本地化部署，并支持分配相应管理权限。

(4)需根据国家相关安全部门的要求进行实时的策略调整，以满足安全要求。

(5)需根据全国各地各运营商对安全扫描的要求进行实时的策略调整调整，以满足安全要求。

(6)根据国家相关部门相关法律法规的要求，提供对广东南方新媒体股份有限公司移动应用进行隐私合规的评估服务。

三、 技术方案

3.1技术标准要求

投标人必须向招标人提供所投标产品的软件规范、接口、协议等详细技术资料。

3.2功能要求

a按照需求完成对应移动应用的加固服务。

b加固完成之后不能影响移动应用性能。

c加固完成之后不能有兼容性问题，必须通过兼容性测试。

3.3服务内容

3.3.1Android加固服务技术要求

| **序号** | **功能大类** | **技术要求** | **详细描述** |
| --- | --- | --- | --- |
| 1 | 代码防逆向保护 | DEX整体安全加壳保护 | 对DEX文件进行整体加密，防止通过第三方反编译工具获取源码，防止对DEX文件进行Java层动态调试。 |
| DEX代码混淆 | 使用高强度的混淆字典对代码进行混淆 |
| Java2CPP加固 | 将DEX代码中函数转化为C/C++代码，并将代码便以为新的SO库文件，同时对该so库文件进行保护。 |
| DEX动态保护 | 将DEX文件中的方法名和方法体分离加密，防止查看；按需解密，使用到函数时进行解密，内存中的DEX不连续存储，防止通过内存DUMP获取明文。 |
| DEX虚拟化保护（DEX VMP） | 自定义虚拟指令，防止在内存中还原代码；防止内存DUMP获取核心数据和代码；增加黑客反编译代码后对业务逻辑的理解难度。 |
| SO 文件加壳保护 | 对自主研发的SO文件进行加壳处理，隐藏外部函数，自定义elf结构防止SO文件被黑客逆向。 |
| SO文件防盗用 | 支持将SO文件同应用进行绑定，防止SO文件被盗用。对so文件进行授权绑定，可绑定客户端包名及签名信息，防止so文件被非授权应用调用运行。 |
| SO 虚拟化保护（SO VMP） | 采用ELF VMP技术，so文件的源码进行虚拟化保护，实现数据隐藏、防篡改、防Dump，增加逆向分析的难度。 |
| so融合 | 将多个so文件融合成一个so文件，防止so文件被查看、篡改。 |
| SO linker | 对整个so文件进行加密压缩，包括代码段、符号表和字符串等，运行时再解密解压缩到内存，从而有效的防止so数据的泄露 |
| 2 | 应用防篡改保护及防二次打包 | DEX文件防篡改 | 对DEX文件进行完整性校验，防止篡改 |
| so文件防篡改 | 对so文件进行完整性校验，防止篡改 |
| H5文件防篡改 | 安全加固后APP本地的资源文件具备加密能力，对服务端下发的H5代码做加密混淆，防止被读取和篡改 |
| Aesset资源文件防篡改 | 对Aesset资源文件进行完整性校验，防止篡改；防止盗版应用 |
| Res资源文件防查看及篡改 | 对Res资源文件进行完整性校验，防止篡改；防止盗版应用 |
| 资源文件加密 | 安全加固后APP本地的资源文件具备加密能力，对所有资源文件下的所有内容进行加密保护，如图片、证书、html、xml等 |
| APK签名校验 | 支持在APK运行时对其签名的合法性进行校验，防止二次打包和盗版。防止APK被其他签名证书签名； 防止APK组件篡改；防止APK资源文件篡改；防止APK二次打包 |
| APK完整性验证 | 支持对APK内的文件进行完整性校验，防止篡改 |
| AndroidMainfest文件防反编译 | 对AndroidMainfest文件进行保护，防止被反编译，防止查看、修改AndroidMainfest文件中的配置信息 |
| 3 | 防调试保护 | 内存防调试保护 | 防止利用调试技术或工具对应用进行内存动态调试，防止GDB、IDA Pro等动态调试工具调试APK，保护内存数据不被读取，保护内存数据不被篡改。 |
| 防止内存代码注入 | 防止利用内存注入技术对应用进行恶意代码注入，实时检测APK运行环境，监控内存和进程状态。 |
| 防trace分析 | 防止通过android trace跟踪函数之间的调用关系。 |
| 防HOOK 保护 | 防止利用xposed、Cydia Substrate、Frida等框架或工具进行Hook攻击。 |
| 4 | 数据据防泄露 | 防内存数据读取、修改 | 实时检测APK运行环境，监控内存和进程状态，防内存数据读取和修改 |
| 本地sharepreference数据加密 | 对SharedPreferences数据文件进行透明加密保护式，无需集成SDK即可实现。 |
| 本地SQLite数据加密 | APK写入数据库文件的时候，进行透明加密；APK写入数据库文件的时候，进行透明加密；加密so库进行加固，混淆保护，防止算法本身被破解 |
| 5 | 运行环境保护 | 防截屏、录屏保护 | 安全加固后APK具备防截屏能力，防止数据泄露，采用纯净加密方式，无需集成SDK即可实现。 |
| 防界面劫持保护 | 安全加固后APK具备防劫持能力，防止恶意应用劫持、防止关键页面的敏感信息泄露、防止应用钓鱼攻击、防止应用界面仿冒欺诈，采用纯净加密方式，无需集成SDK即可实现。 |
| 防日志泄漏保护 | 防止黑客通过日志调试的方式分析客户端代码。 |
| 防模拟器检测及保护 | 对应用运行环境进行检测，判断是否运行在模拟器上，确认后阻止应用运行。 |
| 6 | 加固性能 | 运行时间 | 首次启动时间增量＜1s |
| 加固大小 | 标准加固增量≤2MB |
| 内存变化 | 内存占用率增量（%） ≤15% |
| CPU 变化 | CPU 占用率增量（%） ≤5% |

3.3.2应用安全测评平台技术要求

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **技术要求** | | **详细描述** |
| 1 | Android APP安全检测能力 | 检测项及检测 类别要求 | 支持对 Android APP 的检测不少于 140 个检测项， 且必须覆盖APP基本信息、程序源文件安全、数据存储风险、内部数据交互风险、通信传输风险、身份认证风险、组件风险、HTML5风险、安全防护能力、第三方SDK风险、服务端数据泄露风险、通用WEB风险等检测类型。 |
| 2 | 静态检测 | 支持静态检测分析能力，能够全面扫描应用的静态代码特征，准确识别和定位风险漏洞，提供问题代码位置信息。 |
| 3 | 动态检测 | 支持动态检测分析能力，能够提供至少包含篡改和二次打包攻击风险、应用签名未检验风险、数据 库注入漏洞、动态调试攻击风险、HTTP 报文信 息泄漏风险、界面劫持风险、Content Provider 数 据泄露漏洞、本地端口开放越权漏洞、拒绝服务 攻击漏洞、Root 设备运行风险等 10 个以上的动态安全检测内容。 |
| 4 | 行为检测 | 支持应用行为检测，能够对应用程序进行指令码的行为分析，检测移动应用的行为信息，并提供每个行为的位置信息。 |
| 5 | 权限检测 | 支持权限检测，能够检测移动应用申请了哪些权限，以及识别出哪些权限是移动应用使用的。 |
| 6 | 程序源文件安全检测 | 支持对移动应用程序源文件可能面临的源代码被破解，代码信息泄露，篡改和二次打包等安全风险的检测。 |
| 7 | 数据存储风险检测 | 支持本地数据存储安全的检测，能够提供至少包 含WebView明文存储密码风险、数据库注入漏洞、SharedUserId属性设置风险、StrandHogg漏洞、证书文件明文存储风险、AES/DES加密算法不安全使用风险、RSA加密算法不安全使用风险、全局可读写的内部文件风险、Internal Storage数据全局可读写风险、数据库文件任意读写风险、SharedPreferences数据全局可读写风险、getDir数据全局可读写风险、数据越权备份风险、剪切板敏感信息泄露风险、日志数据泄露风险、URL硬编码风险、密钥硬编码风险、测试信息泄露风险、残留账号密码信息、残留手机号码信息、残留Email信息、SD卡数据泄露风险、明文泄露风险、私有IP地址暴露风险、字节数组与字符串转换风险等 25 个以上的安全检测内容，以排查可能导致移动应用本地数据存储的安全隐患。 |
| 8 | 通信传输风险检测 | 支持通信数据传输安全的检测，能够提供至少包 含HTTPS未校验服务器主机名漏洞、HTTPS允许任意服务器主机名漏洞、HTTP传输通道风险、SSL证书有效性风险、中间人攻击风险、联网环境检测、启用VPN服务检测、访问境外服务器风险、HTTP 报文信息泄漏风险、SSL不安全组件使用风险、通信套接字安全、未配置网络安全属性风险等12个以上安全检测内容。 |
| 9 | Android SDK安全检测能力 | 安全防护能力评测 | 支持恶意攻击防范能力评测，能够提供至少包含ZipperDown风险、下载任意APK风险、从SD卡加载SO风险、“寄生推 ”云控风险、从SD卡加载DEX风险、Java层代码动态调试风险、启动隐藏服务风险、未使用编译器堆栈保护技术风险、未使用地址空间随机化技术风险、随机数不安全使用风险、私有函数调用风险、不安全的浏览器调用风险、动态链接库中包含执行命令函数等 13个以上的安全检测内容，以分析移动应用安全防护能力。 |
| 10 | 安全检测能力 | 支持对 Android SDK 实现自动化识别和安全检测，检测范围涵盖基本信息和安全风险两个层面的检测类别。  应用基本信息的检测内容至少应该包括权限信息、 行为信息、第三方 SDK 检测、开放端口检测等 4 个以上检测内容。  2）安全风险检测内容至少应该包括数据库注入漏洞、SD卡数据泄露风险检测、应用测试模式发布风险、本地端口开放越权风险检测、中间人攻击风险、恶意可执行程序感染漏洞、Provider文件目录遍历风险检测、发送广播信息泄漏风险检测、Activity绑定browserable与自定义协议检测、HTTP报文信息泄漏风险检测、libupnp栈溢出漏洞、敏感文本检测、敏感图片检测等13个以上安全检测内容。 |
| 11 | 检测报告要求 | 结果查看模式 | 检测结果必须支持在线查看和报告下载两种阅读模式，且必须支持 WORD 和 PDF 两种报告格式。 |
| 12 | 报告构成要求 | 检测报告必须包括封面、目录、检测结果统计、检测项情况汇总、检测结果分析等关键构成元素。 |
| 13 | 报告详情要求 | 检测详情必须包含测评目的、风险等级、威胁描述、 检测结果、结果描述、检测详情、解决方案等关键要素，同时解决方案中需具备修复代码示例等内容。 |
| 14 | 批量检测要求 | 可在界面上一次性提交多个 Apk 文件，实现批量检测以及批量下载报告。 |
| 15 | 管理功能要求 | Android 检测 结果源数据可导出 | Android检测结果源数据可导出，可针对APP的某一次检测，导出相应的检测结果源数据excel，便于对数据进行二次加工分析。 |
| 16 | 应用安全数据的统计分析 | 支持平台上应用安全数据的统计分析，通过多样化的图表展示分析结果，呈现发生最多的安全漏洞等安全趋势。 |
| 17 | Android SDK 管理 | 提供第三方SDK 的管理功能，可自主添加或删除第三方 SDK |
| 18 | 报告封面自定义 | 支持通过管理员对报告的名称、LOGO、封面、水印等进行自主设置。 |
| 19 | 产品信息自定义 | 支持通过管理员后台对平台的厂商信息和logo信息等内容进行自主设置和编辑，实现重置。 |

3.4保密性要求

投标方未经需求方书面许可，不得将本文件的任何内容透露给除招标方以外的第三方。由应答方提供业务或内容的，应答方应与需求方签订信息安全承诺保证书，明确应答方的信息安全责任。

3.5第三方软件要求

平台所涉及的第三方软件必须要求正版授权，涉及任何盗版或者侵权行为责任由投标方承担。

四、 采购内容

采购移动应用加固服务、安全扫面检测服务及相关伴随服务（含终验后一年维保服务），本期需求一共12款应用。