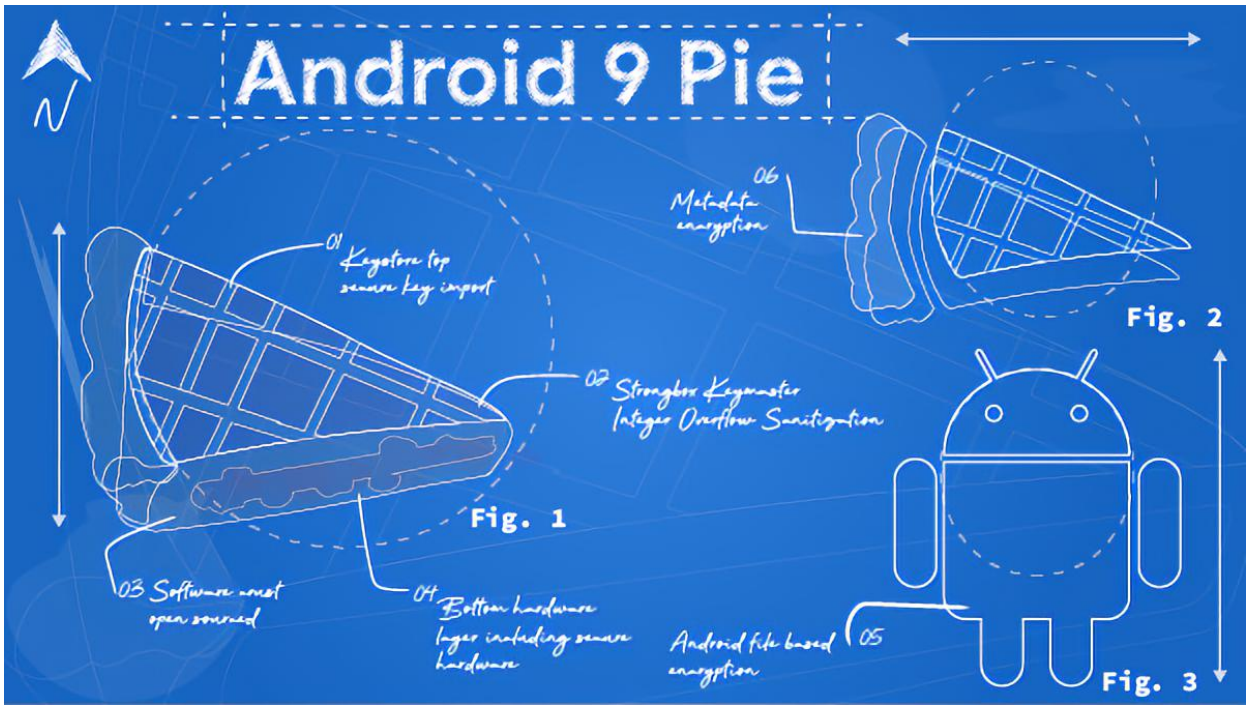
现代化 Android Pie：安全与隐私

原创： Android



作者：Vikrant Nanda 和 René Mayrhofer，Android 安全与隐私团队

没有什么时候比节假日更适合聊 Android 甜点系统了，毕竟，有谁不喜欢在放假的时候来上一两口甜点呢？那么，大家最喜欢的节日甜点又有些什么呢？我相信派（Pie）肯定是不少小伙伴的心上之选。

说真的，"派"这个比喻确实很恰当，各种材料细细烘焙，化为层层美味：精致的馅料（软件）配上酥脆的底子（硬件），简直完美！感兴趣的读者不妨耐心阅读下文，了解一下 Android Pie 新添加了哪些安全及隐私特性吧。

更新 Android

我们需要在加强平台建设的同时改进反漏洞技术，双管齐下才能打造更加安全的 Android。

强化平台建设

我们为 Android Pie 更新了文件级加密（FBE）功能，使其支持外部存储媒介（如可扩展存储卡），并添加了带有硬件支持的元数据加密技术。通过文件系统元数据加密，设备启动时生成的单个密钥会加密所有未经过 FBE 加密的内容（例如目录布局、文件大小、权限和创建 / 修改时间）。

- 文件级加密

https://source.android.google.cn/security/encryption/file-based

- 元数据加密

https://source.android.google.cn/security/encryption/metadata

应用可以通过调用 Android Pie 中的 BiometricPrompt API，在设备上显示身份验证对话框（例如提示用户进行指纹识别），而且该方法与形态无关（modality-agnostic），生成的对话框具备统一的样式、使用感和屏幕位置。这种标准化的体验有助于增加用户信心，让他们感觉正在授权一个可信赖的身份验证请求。

- BiometricPrompt API

https://android-developers.googleblog.com/2018/06/better-biometrics-in-android-p.html

应用沙盒引入了新保护机制和测试用例，这有助于确保所有针对 Android Pie（以及所有未来版本系统）开发的非特权应用都可以在更强大的 SELinux 沙盒中运行。通过向沙盒提供针对各个应用的加密认证，该保护机制可以提升应用隔离效果，防止替换安全默认设置，并且（同时也是最重要的一点）防止应用数据被所有人访问。

- 应用沙盒

https://source.android.google.cn/security/app-sandbox

- SELinux

https://source.android.google.cn/security/selinux

反漏洞技术升级

我们在 Android Pie 中进一步扩展了编译器级别的安全措施，以便在运行时捕获会触发未定义行为的操作，并让这些操作安全地失效。

控制流程完整性（CFI） 是一种安全机制，它不允许更改已编译代码的原始控制流图。在 Android Pie 中，CFI 在媒体框架和其它关键安全组件中默认启用，如近场通信（NFC）和蓝牙协议。此外，为了继续加强旧版本系统的内核，我们在 Android 通用内核中也实现了CFI 支持。

整数溢出排错程序可以缓解由整数溢出导致的内存损坏和信息泄露问题。在 Android Pie 中，我们将排错程序的使用范围扩展至以下两类库：(1) 需要处理复杂且不受信任的输入；(2) 曾收到过安全漏洞报告。

- 编译器级别的安全措施

https://android-developers.googleblog.com/2018/06/compiler-based-security-mitigations-in.html

- 控制流程完整性 (CFI)

https://source.android.google.cn/devices/tech/debug/cfi

- 在 Android 通用内核中也实现了 CFI 支持

https://android-developers.googleblog.com/2018/10/control-flow-integrity-in-android-kernel.html

对基于硬件安全技术的持续投入

Android 高可信度用户确认（Android Protected Confirmation）是 Android Pie 的亮点功能之一。它是第一个可以在移动设备上通过可信 UI 保障交易安全的系统级 API，主要作用是利用受硬件保护的用户界面（即可信 UI ），确保关键交易在主操作系统外完成。开发者调用该 API 后，设备便会向用户显示一个可信 UI 提示， 请他们通过物理输入（如设备按键）进行授权。授权成功后，依赖方便会收到一个带有加密签名的声明，然后再次确认用户确实想在应用内完成一笔敏感交易。

我们还为一种新密钥库类型添加了支持，它可以利用搭载独立 CPU、RAM 和闪存的防篡改硬件，为私钥提供更强大的安全防护。StrongBox Keymaster 是一种位于硬件模块中的 Keymaster HAL 实现。该模块拥有自己的 CPU、安全储存空间、真实随机数生成器，以及用于抵御软件包篡改和侧通道攻击的保护机制。

其它密钥库特性（属于 Keymaster 4 的一部分）包括键盘锁定密钥、安全密钥导入、3DES 支持和版本绑定 。键盘锁定密钥可以限制密钥的使用，从而达到保护敏感讯息的目的；安全密钥导入让密钥的使用更加方面，防止应用和操作系统提取密钥材料。更多内容，请参阅《 Keystore 新特性让 Android Pie 更安全》以及 Android Pie 版本说明内的相关部分。

- Android 高可信度用户确认

https://android-developers.googleblog.com/2018/10/android-protected-confirmation.html

- StrongBox Keymaster

https://developer.android.google.cn/training/articles/keystore#HardwareSecurityModule

- Keystore 新特性让 Android Pie 更安全

https://android-developers.googleblog.com/2018/12/new-keystore-features-keep-your-slice.html

- Android Pie 版本说明

https://source.android.google.cn/setup/start/p-release-notes#keystore

加强用户隐私保护

为了增强用户隐私，Android Pie 引入了若干行为变更，如限制后台应用访问摄像头，麦克风和设备传感器。系统为通话、手机状态和 Wi-Fi 扫描设立了新的权限规则和权限组，并限制应用通过 Wi-Fi 扫描获取敏感信息。 此外，我们还添加了另一个和 WiFi 安全相关的新功能—— MAC 地址随机化。此功能启用后，每当设备连接到 WiFi 网络时便会使用不同的网络地址。

另外，Android Pie 还支持使用用户锁屏密码（即 PIN, 图案或者字符组合）来加密备份数据，即是说，攻击者不知道具体的锁屏密码时便无法访问用户备份的应用数据。应用的自动备份功能也有所优化，开发者可以指定在哪些条件下，应用数据被排除在自动备份计划外。比如说，Android Pie 新添加的一款标签就可用于判定用户备份是否为客户端加密。

为了将所有网络流量从明文（未加密的 HTTP）逐步迁移至 TLS（HTTPS），我们修改了网络安全配置的默认设置，以屏蔽所有明文流量。除非您明确允许特定域名使用明文传输，Android Pie 默认启用 TLS 来保护用户。系统同时也为 DNS-over-TLS 提

供了内置支持：当网络的 DNS 服务器支持时，设备会自动将 DNS 查询升级为 TLS。该方法能从网络层面防止 IP 地址信息被监听或拦截。

我们认为本文描述的特性很好地总结了 Android 在安全与隐私方面的工作进展。亲爱的读者们，您可能觉得这只是我们的一面之词，不过事实表明，这几年来，我们对安全话题的持续投入确实显著提高了系统的安全防护能力，不断增加的漏洞利用难度和独立移动安全评级都很好地证明了这一点。赶快上手体验 Android Pie 吧！我们正在快马加鞭准备下个版本的系统发布，敬请期待！

- 行为变更

https://developer.android.google.cn/about/versions/pie/android-9.0-changes-all#privacy-changes-all

- MAC 地址随机化

https://source.android.google.cn/devices/tech/connect/wifi-mac-randomization

- 攻击者不知道具体的锁屏密码时便无法访问用户备份的应用数据

https://developer.android.google.cn/about/versions/pie/security/ckv-whitepaper

- 默认启用 TLS

https://android-developers.googleblog.com/2018/04/protecting-users-with-tls-by-default-in.html

- 不断增加的漏洞利用难度

https://www.thezdi.com/blog/2018/9/04/announcing-pwn2own-tokyo-for-2018

- 独立移动安全评级

https://www.blog.google/products/android-enterprise/gartners-analysis-progress-android-security/

推荐阅读

- 高效管理 Android 前台服务
- **即刻注册 SDK，获取实时动态及相关更新**
- **和 Twitter 开发者们一起学习通知管理技巧**

阅读原文