Man-in-the-Disk：安卓应用新攻击面分析

angel010 / 2018-08-13 21:22:11 / 浏览数 2258 安全技术 漏洞分析 顶(0) 踩(0)

本文翻译自：
https://blog.checkpoint.com/2018/08/12/man-in-the-disk-a-new-attack-surface-for-android-apps/

更多技术细节请参考：
https://research.checkpoint.com/androids-man-in-the-disk/

研究人员发现安卓应用程序使用存储资源的缺陷。因为对应用使用外部存储没有限制，攻击者利用这一点可能导致未请求的、潜在恶意的程序安装，拒绝合法程序的服务，甚

Man-in-the-Disk攻击是因为没有限制应用程序对外部存储的访问，外部存储是所有应用共享的资源，而且不受到安卓内置沙箱的保护。不能应用安全保护措施所以应用易受

外部存储External Storage

首先介绍一下安卓设备的存储资源。

在安卓系统内部一共有两种类型的存储，分别是内部存储（Internal Storage）和外部存储（External Storage）。内部存储结果安卓沙箱隔离，每个应用使用不同的区域；外部存储一般是SD卡或设备存储的逻辑分区，是所有应用共享的。外部存储主要用于应用与PC之间共

应用开发者选择使用外部存储的原因还包括缺乏足够的内部存储空间、与早期设备的互通、不希望应用使用太多的空间等。

在使用外部存储时，需要注意以下问题：

Google Android文档中，有建议应用开发者如何使用外部存储的内容：

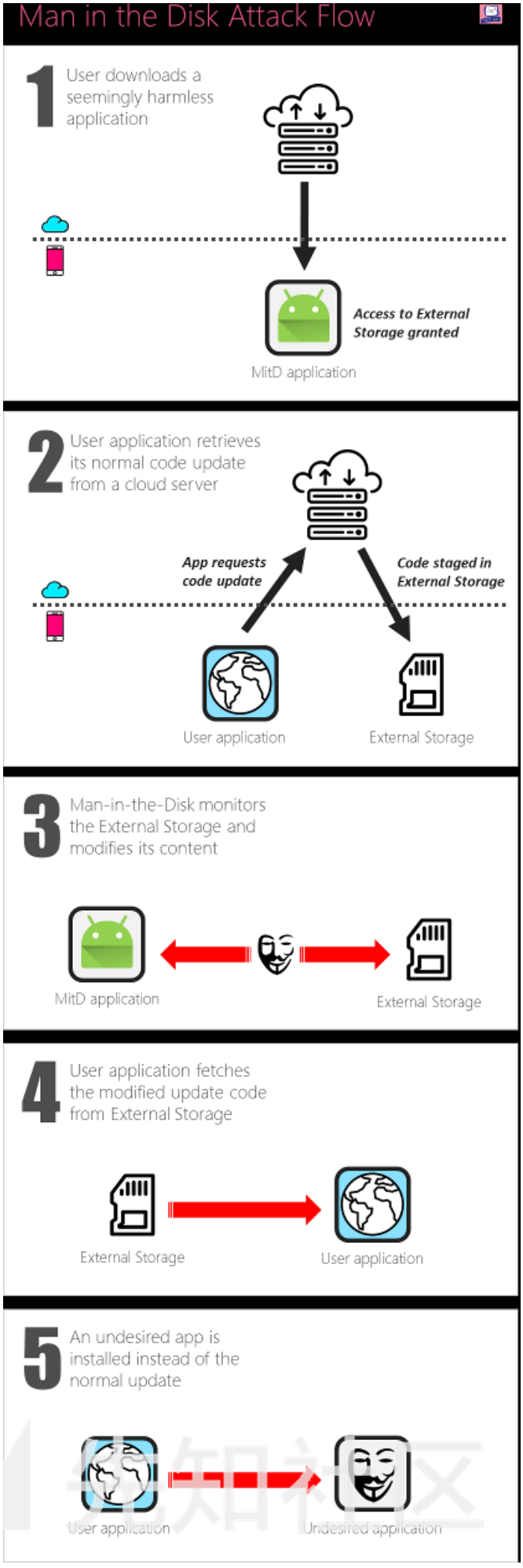
1. 在处理来自外部存储中的数据时要进行输入有效性检查；
2. 不要在外部存储上保存可执行文件或类文件；
3. 外部存储文件在动态加载前，应进行签名和加密。

但实际开发过程中，包括很多来自知名OEM和Google的应用都没有遵守官方指南。这也就催生了利用外部存储上的数据进行攻击的Man-in-the-Disk攻击面的出现。

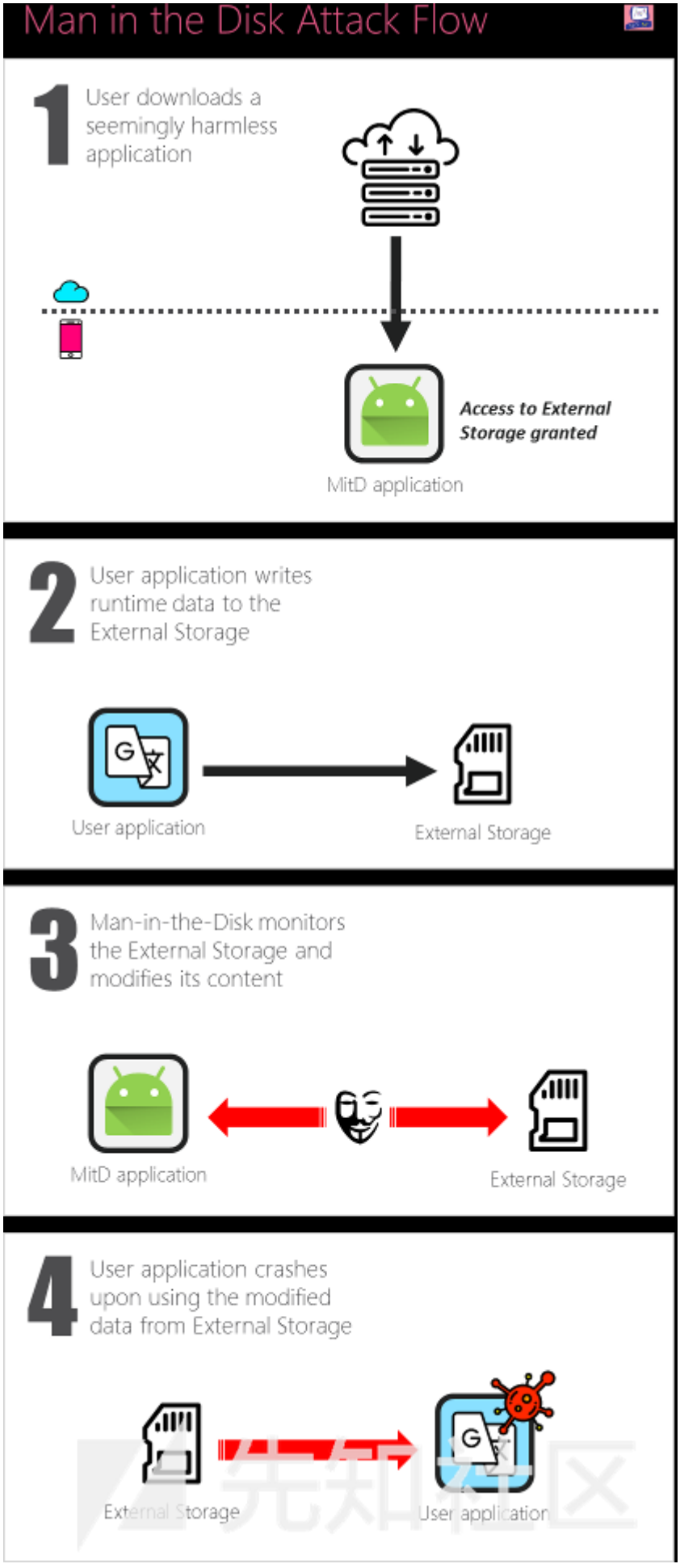
Man-in-the-Disk攻击

攻击者利用Man-in-the-Disk攻击可以修改和处理位于外部存储上的数据。

研究人员分析发现，从app提供上的服务器上下载、更新和接收的数据，在抵达app前都是通过外部存储传输的，下图所示。这就是一种攻击机会，在应用读取数据之前，可



修改外部存储的数据可以使用一些看起来无害的应用，比如假的手电筒app，其中含有攻击者的漏洞利用脚本。攻击者会诱使用户下载看起来无害的APP，这些app在安装时

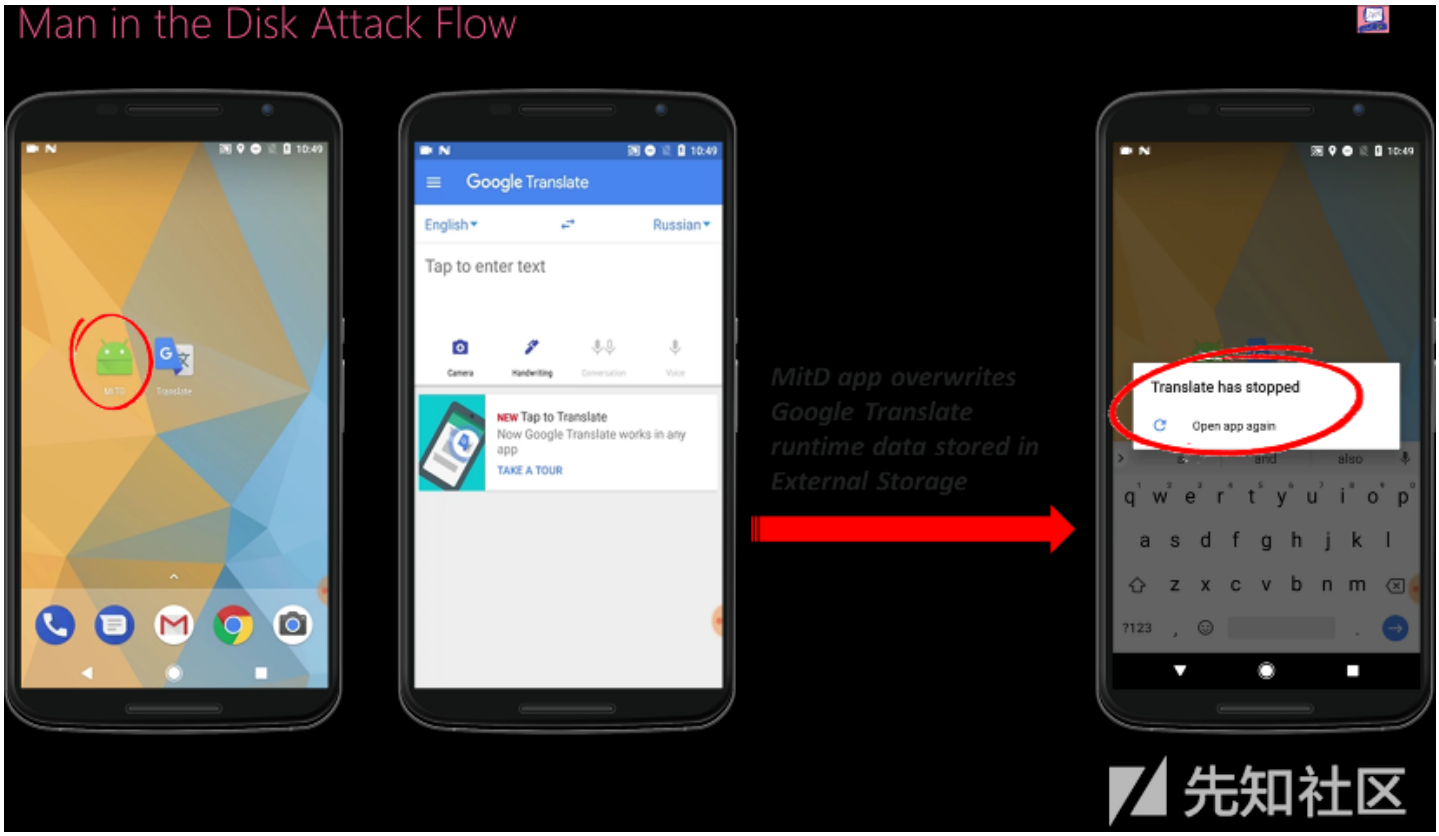


也就是说，攻击者利用Man-in-the-Disk攻击可以拦截和修改已安装的app与外部存储之间的数据交换。根据攻击者目的的不同，攻击效果也不同。本研究证明了可以在不没

存在Man-in-the-Disk攻击的应用

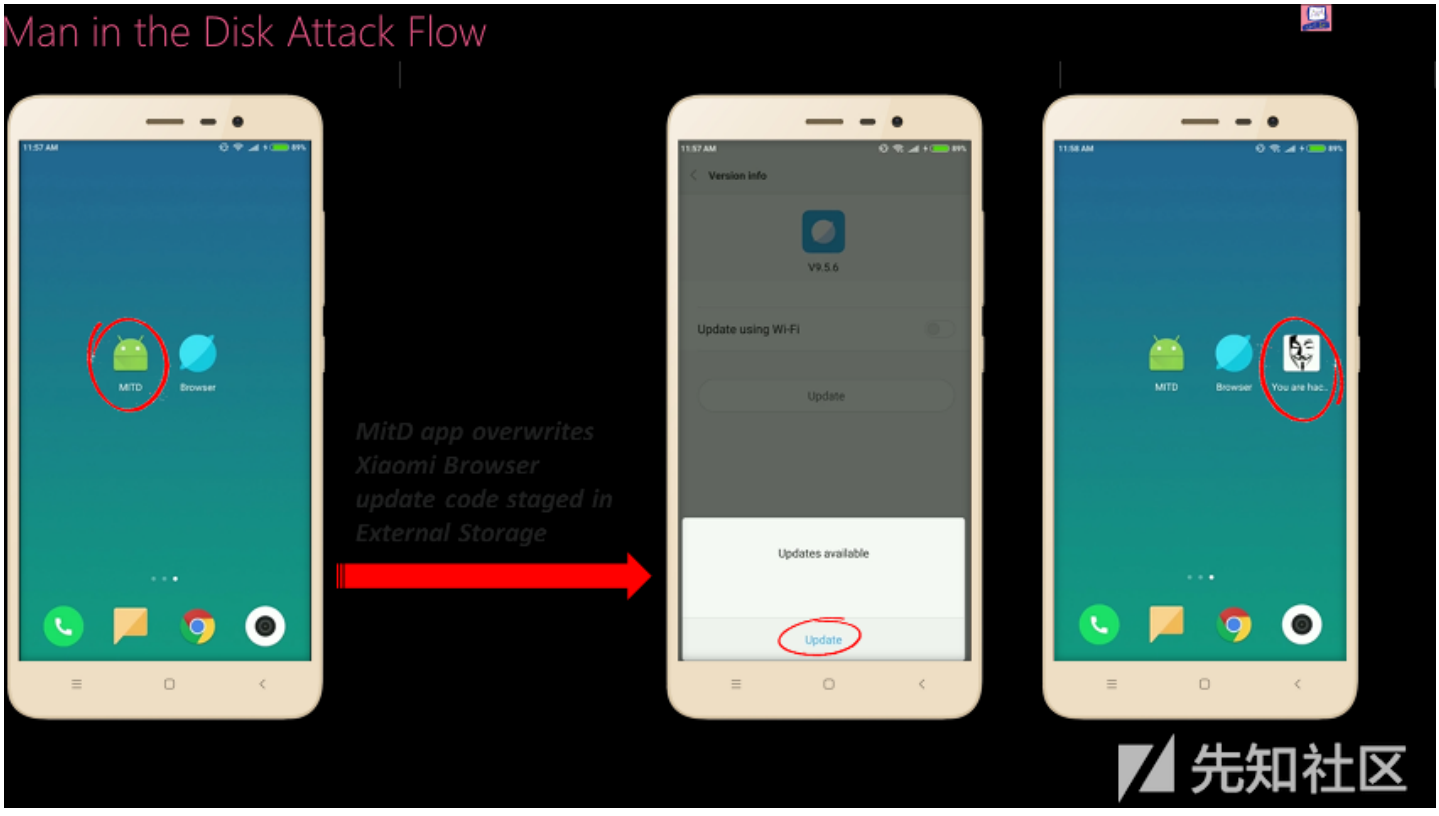
研究人员通过测试发现， Google翻译, Yandex翻译, Google语音输入, Google文本转语音, Xiaomi浏览器等应用都存在Man-in-the-Disk攻击。

研究人员对比Google的开发者指南进行了比较分析：
研究人员发现Google翻译,
Yandex翻译和Google语音输入应用中，开发者没有验证来自外部存储的数据的完整性。因此研究人员黑掉了这些应用需要的特定文件，导致这些应用程序奔溃。



Man-in-the-Disk攻击实例：Google翻译应用奔溃

研究人员发现Xiaomi浏览器在应用升级时会把外部存储作为资源中转站。因此，研究人员替换了应用的升级代码，导致安装了其他的应用。



Man-in-the-Disk攻击实例：xiaomi浏览器升级代码被替换

漏洞修复情况

研究人员将发现的漏洞情况通报给了Google、Xiaomi和其他相关厂商。Google已经修复了存在的漏洞，其他应用漏洞会在补丁发布后公布，xiaomi选择目前不解决该漏洞

研究人员只检查了一小部分的应用样本，但相信这种漏洞广泛存在各种应用之中。而且应用程序请求的权限越多，越容易被攻击者盯上。对有权限的应用的代码注入会使攻击

因果

攻击细节看起来比较复杂， 但安卓系统也存在一定的缺陷：

安卓设备的外部存储是公共区域，设备上的任何应用都可以查看和修改；

安卓对外部存储上的数据没有内置的保护措施，只对开发者合理使用资源给出指南和参考；

开发者既没有意识到潜在的安全风险，也没有遵照开发者指南的建议；

一些预装的应用和主流的应用也没有遵照开发者指南的建议，在未受保护的外部存储中保存敏感信息；

这会导致Man-in-the-Disk攻击，导致未受保护的敏感数据的修改或滥用。

如何应对Man-in-the-Disk攻击

通过上面的分析，很清楚攻击的来源在于安卓系统的设计缺陷以及应用开发者没有遵守开发者指南中的建议。那么首先开发者在开发过程中要考虑应用开发的安全性，而不仅

研究人员认为确保底层系统的安全性是应对这一新攻击面的长期解决措施。

上一篇：Sulley fuzzer lea... 下一篇：XML外部实体注入小结

1. 0 条回复
   - 动动手指，沙发就是你的了！