SpanDex- Secure Password Tracking for Android

DEC 23RD, 2015

论文下载：https://users.cs.duke.edu/~lpcox/spandex.pdf

摘要

- 这篇文章提出的SpanDex，是一个Android DVM的扩展集，用于保证应用程序不会泄露用户的密码。
- SpanDex解决的主要技术问题是准确、完整、有效的处理隐式信息流（如程序控制流传送的信息）。具体方法是借助符号执行技术系来准确地量化一个进程的控制流所揭露的关于一个秘密的信息量。
- 为了运行时应用这些技术系的同时不牺牲性能，SpanDex在一个数据流敏感的沙箱内运行不可信的代码，这个沙箱限制了应用程序可以对敏感数据做的操作的组合（mix of operations）？？
- 文章使用了50个流行的Android应用对SpanDex原型做的实验，以及对于泄露的密码进行的分析表明，对于90%的用户，攻击者需要尝试超过80次登录来猜到用户的密码。今天同样地攻击者只需要对所有用户进行一次尝试。

引论

- 密码连接移动应用和基于云的平台，保护密码不被泄露至关重要
- 污点跟踪是分析密码走向的一个很显然的起始点。目前大多数污点跟踪Monitor只能处理显式流（秘密信息从操作的源操作数传递到目的操作数），但是程序中也包含隐式流（秘密信息通过程序控制流传递给对象）。现有的对隐式流处理的技术容易夸大（overstate）哪些对象包含了秘密信息。如if s!=0 then x=a else y=b。这种静态分析的目标是找出所有受条件影响的对象，会有很高的FPR（False-positive rate）。
- 本文的SpanDex为第三方应用处理密码提供了强的安全保证。集中在要保护数据类型的常见访问模式和语义（common access pattern and semantics of the data type）。对于隐式流的处理是借助符号执行技术来准确量化控制流揭露的秘密信息的信息量.

信任和攻击模型

- SpanDex是在Dalvik虚拟机接口之下实现的，因此虚拟机提供的保护提供了SpanDex的信任模型基础。SpanDex无法对使用第三方native code的应用进行密码保护
    - 被taint的对象在应用执行native code前要被清理
    - 进程调用第三方native code后，就不被允许接收密码数据（SpanDex依赖内核维护进程调用native code的信息）

    - 应用不能把tainted数据写到永久存储去，或者通过IPC发送给其他应用
- SpanDex关注密码数据在应用内的流向
    - 用户将密码和对应的域打标签
- 确保密码数据只跟域内的服务器共享，但是在数据离开设备后，不提供任何保证。
    - 例如SpanDex无法阻止攻击者将用户的facebook密码作为一条消息发送给攻击者控制的Facebook账户
- 攻击模型
    - 攻击者知道用户的用户名，并且假定用户的密码是一个很大的list中的一个，攻击的目标就是使用应用中获得的信息，从密码list中找到用户的密码。一旦攻击者计算出一个用户名可能的密码集，找出真正密码的方法就是在线查询。

Evaluation

- Spandex假设攻击者能够访问到一个大的明文密码列表，可以通过应用中没有被标记的信息来缩小可能的用户密码集合