VIII. CONCLUSION

Android apps specify a target API level and run in a

compatibility mode on devices with higher API levels. The

compatibility mode can disable important security changes in

the Android platform. We call the problem of apps targeting

outdated API levels the target fragmentation problem. In this

study we analyze a dataset of more than one million Android

apps collected over four years and show that the large majority

of collected apps target outdated API levels. We examine

the practical implications of target fragmentation on seven

security changes to the Android platform and show that target

fragmentation hamstrings new security features.

We believe that applying security changes in this optional

manner is a flawed approach that sacrifices security at the

altar of compatibility. Developers become a new obstacle

to securing apps and users have no means of ensuring that

their apps target the most current API levels. The target

fragmentation problem is further compounded by the coupling

of security changes and non-security changes. We hope that by

shedding light on this problem, developers can become more

aware of the consequences of targeting outdated API levels

and this flawed design can be reexamined and changed so that

there is less opportunity for Android apps to operate without

access to important security features.

VIII. 结论

Android 应用程序指定一个目标 API 级别, 并在具有较高 API 级别的设备上的兼容模式运行。兼容模式可以禁用Android 平台重要的安全更改。我们叫这个问题为针对过时API级别的应用程序目标碎片化问题。我们花了四年里研究收集分析了超过 100万 Android 应用，显示大部分收集的应用的目标是过时的 API 级别。我们研究目标碎片化对Android 平台七个安全变化的实际影响 , 并显示目标碎片化对新的安全功能的削弱。我们认为, 应用可选的安全更改方式是一个有缺陷的方法, 牺牲安全性来确保兼容性。开发商为了保证应用程序和用户的安全成为新的障碍，没有办法确保他们的应用程序的目标是最新的 API 级别。目标碎片化问题进一步复杂化加剧安全更改和非安全更改。我们希望通过在这个问题上, 开发者可以变得更意识到以过时的 API 级别为目标的后果，对这种有缺陷设计可以重新审视和改变, 以便Android应用运行时不会产生重要的安全功能。