Lane Gramling
EECS 700
Reading 9

Summary - Cloak and Dagger

This paper brings to attention a glaring security flaw existent in the android permission system, specifically focusing on a pair of permissions provided by Android. The first is the SYSTEM_ALERT_WINDOW permission, which allows an app with this permission to draw arbitrary overlays over other apps. The second is the BIND_ACCESSIBILITY_SERVICE permission, which allows an app to capture accessibility events (which can be exploited to gain privileged information) as well as providing full access to the view model tree displayed on the screen of the device. This paper paints a picture of how these two freedoms, if allowed in concert, can be exploited to gain full 'god-mode' control of an Android phone, even stretching beyond the typical capabilities of an app granted full administrative permissions.

Contributions

The first major contribution of this paper is its description of how these permissions can be used to gain complete control of the UI feedback loop. As explained by the authors, access to the complete view model tree afforded by the BIND_ACCESSIBILITY_SERVICE can be used by a malicious actor to gain knowledge of what is on the screen at any given time. One particularly interesting observation of the authors regarding this issue was how number presses on the PIN lock screen in Android send accessibility events to the device, from which the contents of each event can be extracted and reconstructed to find the PIN of the user. Furthermore, by leveraging the SYSTEM_ALERT_WINDOW permission, which is automatically granted to apps installed from the Play Store, targeted clickjacking attacks can be far enhanced using knowledge of the view model tree. The authors provide a number of examples of how this can be used, from feigning login screens to steal passwords or 2FA codes, to browsing the internet and clicking ads to farm revenue while the device seems unassumingly asleep, without giving the user any reason for suspicion. The next notable contribution is a number of observations of the design shortcomings of Android enabling this exploit, and attempts are made to give suggestions on how to combat this. However, the authors note that this exploitation potential is possible chiefly due to the inherent design of Android, and note that there are no true easy fixes to prevent this exploit entirely.

Limitations

While the paper is effective at bringing to light the danger of this combination of permissions, it felt apparent that the authors spent far more time daydreaming about what kind of ways this vulnerability can be used maliciously than they spent trying to come up with meaningful solutions (or at least suggestions) for how to combat the efficacy of this exploit. In my opinion, the vast majority of the many capabilities of this exploit enumerated by the authors should have been obvious simply by pointing out that full control of the UI feedback loop is possible, leaving a wide range of potential for exploitation to be assumed as possible. Thus, a more succinct exploration of potential malware cases would have been satisfactory, and more focus could have been placed on solving the problems they pointed out.

Future Work

This paper did well in explaining the massive potential for exploitation provided by the combined capabilities of the SYSTEM_ALERT_WINDOW and BIND_ACCESSIBILITY_SERVICE permissions, but certainly left a space for plenty more work to be done investigating the issue. The elaboration on potential countermeasures was not satisfactory, which leaves plenty of room for discussion regarding the design flaws of android that enable this issue, how to make adjustments to correct for those flaws, or how to take measures decreasing its effectiveness by other means.