Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

The paper shows that, android user security can be compromised by using two highly underestimated and security sensitive permissions - `SYSTEM_ALERT_WINDOW` and `BIND_ACCESSIBILITY_SERVICE`. Paper claims that using these two permissions, it is possible to take total control of victim's device. Using `SYSTEM_ALERT_WINDOW` permission confusion attack, the attacker can modify what user sees and using `BIND_ACCESSIBILITY_SERVICE` (this service is designed for users with disabilities, but attacker takes advantage of that) permission confusion attack, the attacker can insert fake user inputs. Combination of these two permission confusion attacks, leads to more powerful attack 'cloak and dagger' (authors named it). On Google play store, `SYSTEM_ALERT_WINDOW` is granted automatically and `BIND_ACCESSIBILITY_SERVICE` can be obtained by performing clickjacking(using overlays), etc. to trick the user to enable this permission. Authors claimed that, the design shortcomings in these permissions and android system, makes it difficult to defend against these attacks. Using techniques (by enabling only two above mentioned permissions) such as clickjacking, keystore reconrding, device unlocking, enabling permissions, ad hijacking, etc., it is possible to get complete access of the device. To show this attack practically, authors did a user study, and none of the 20 participants were able to suspect the attack. Finally authors propose a defense mechanism, "that can block any attempt to confuse the use and limit the attack"[1].

2 Contribution

Authors highlighted that there are major deign flaws in the permissions `SYSTEM_ALERT_WINDOW` and `BIND_ACCESSIBILITY_SERVICE`, and the android system itself. To show these shortcomings, authors mount 'Cloak and Dagger' attack, which they claim was able to bluff 20 participants (in their user study). They also suggest defense mechanisms which can possibly limit the attack.

3 Strengths

I would say the major strength is that none of the participants were able to detects the attack and hence, that successfully proves that these attacks can be severe and thus that proves author's point. I liked the detailed explanation of attacks. As their proposals need system modifications, I liked that they also proposed short term recommendations.

4 Limitations

Their proposal does not prevent malicious app to use the `BIND_ACCESSIBILITY_SERVICE` permission as a side channel to infer which app the user is interacting with. They left the responsibility of choosing security sensitive widgets on developers. Also, as their major recommendations require system modifications, it will take a long time to include majority of the users (and to aware developers).

5 Future Work

As authors suggested, to automatically determine which widgets should be considered as security-sensitive, would be an important research direction. Also, Google must inspect apps which uses the combination of above two permissions and remove the ones, which are used to compromise user security.

References

[1] Y. Fratantonio and C. Qian and S. P. Chung and W. Lee *Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop*, IEEE, (2017)