Critique on
You, W., Liang, B., Shi, W., Zhu, S., Wang, P., Xie, S., & Zhang, X. (2016, May) "Reference hijacking: Patching, protecting and analyzing on unmodified and non-rooted android devices."

Astha Sharma
asharma6@uno.edu

SUMMARY

According to the paper presented, the then practiced deployment techniques like root access and source tree were not the best solution in terms of security and that they didn't provide the best security measurement. So the authors of the paper came up with a better solution to this problem - Reference Hijacking Prototype. It is a kind of a special reset procedure targeting the underlying system libraries or files go through redirected security enhanced alternatives without flashing or root Android devices. The authors also discuss about the developed three prototype systems, wiz. Patchman, Controlman and Taintman, that are based on reference hijacking. The Patchman patches the vulnerable underlying system libraries, Controlman enforces a flexible access control policy on inter component communication and finally the Taintman increases security by preventing malicious users from executing command on devices.

STRENGTHS

1. Reference hijacking is a two-edged sword - does both the task of securing Android devices and works against the possible attacks.

2. The reference hijacking technique has been shown to be applicable to both the Dalvik and ART runtime environments in almost all mainstream Android versions (2.x to 5.x).

3. A proper case study and the test results demonstrating the significance of the technique.

4. It is claimed that combining reference hijacking with some of the existing technique such as Boxify can significantly address the security problems in the android system.

WEAKNESSES

1. The research seems to be outdated for the fast pacing technology as it was based on version 2.x to 5.x, whereas, now we have a android version 9 (PIE).

2. Additional efforts is required in order to bypass the validation of the package integrity by adjusting the validation logic.

3. It can increase burden over a device in terms of space required for running the security application environment.

4. The reference hijacking technique can also be used by the attackers to generate security related risks.