Runtime analysis of mobile devices for malware detection.

Research proposal.

Brandon Amos

October 27, 2014

1 Introduction.

Mobile devices and technology are exploding, where the number of mobile devices is expected to exceed the number of people on Earth by 2014[1]. Mobile security has become a serious concern due to the sensitive information mobile devices contain and the critical systems mobile devices control. In *the military*, the GPS locations and identities of deployed military members can be obtained. In *manufacturing*, computer-aided manufacturing tools can be controlled with a mobile device, allowing an attacker to silently alter the manufacturing process, as I have studied [1]. In *healthcare*, patients can rely on glucose monitors on mobile devices, allowing an attacker to send false reports and harm patients. *Low malware detection rates are an* ***open research problem.*** A study of thousands of real Android malware samples in 2011 show that industry antimalware software detect 79.6% of the malware in the best case and 20.2% in the worst case [2].

[1] `http://blogs.cisco.com/sp/the-future-of-monetizing-mobility/`

References

[1] H. Turner, B. Amos, J. White, J. Camelio, C. Williams, and R. Parker. Bad parts: Are our manufacturing systems at risk of silent cyber-attacks? Submitted, 2013.

[2] Y. Zhou and X. Jiang. Dissecting android malware: Characterization and evolution. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 95–109. IEEE, 2012.