Collaborative Verification of Information Flow for a High-Assurance App Store

René Just, Michael D. Ernst, and Suzanne Millstein

Computer Science & Engineering
University of Washington
Seattle, WA, USA
{rjust, mernst, smillst}@cs.washington.edu

Abstract:

Current app stores distribute some malware to unsuspecting users, even though the app approval process may be costly and time-consuming. High-integrity app stores must provide stronger guarantees that their apps are not malicious. This talk presents a verification model for use in such app stores to guarantee that the apps are free of malicious information flows. In this model, the software vendor and the app store auditor collaborate—each does tasks that are easy for her/him, reducing overall verification cost. The software vendor provides a behavioral specification of information flow and source code annotated with information-flow type qualifiers. This talk also presents our flow-sensitive, context-sensitive information-flow type system that checks those information flow type qualifiers and proves that only information flows in the specification can occur at run time. We have implemented the information-flow type system for Android apps written in Java, and we evaluated both its effectiveness and usability in practice. In an adversarial Red Team evaluation, we analyzed 72 apps (576,000 lines of code) for malware. Our information-flow type system was effective: it detected 96% of malware whose malicious behavior was related to information flow. Besides, the programmer annotation burden was low: only 6 annotations per 100 LOC were required in our evaluation.

Acknowledgment We would like to thank our collaborators Werner Dietl, Stuart Pernsteiner, Franziska Roesner, Karl Koscher, Paulo Barros, Ravi Bhoraskar, Seungyeop Han, Paul Vines, and Edward X. Wu.

References

[EJM+14] Michael D. Ernst, René Just, Suzanne Millstein, Werner M. Dietl, Stuart Pernsteiner, Franziska Roesner, Karl Koscher, Paulo Barros, Ravi Bhoraskar, Seungyeop Han, Paul Vines, and Edward X. Wu. Collaborative Verification of Information Flow for a High-Assurance App Store. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 1092–1104, Scottsdale, AZ, USA, November 4–6 2014.