FreeMarket: Shopping for free in Android applications*

Daniel Reynaud, Eui Chul Richard Shin, Thomas R. Magrino, Edward X. Wu, Dawn Song
University of California, Berkeley

Google recently launched Android Market In-app Billing (IAB), a service that allows developers to sell digital content in their Android applications by delegating the billing responsibilities to Google. This feature has already gained immense popularity with developers—16 of the top 20 grossing apps in the Android Market rely on IAB for generating revenue. However, despite Google's recommendations for preventing attacks on IAB applications,[1] the majority of applications do not use adequate security measures to authenticate IAB purchases.

In this work we present the *FreeMarket attack*, which automatically identifies and exploits such insecure IAB coding practices. Our attack produces a rewritten application for which all in-app purchases succeed without any payment. The rewritten application retains the full functionality of the original and can be executed on unmodified Android devices. We show that at least 174 applications in the Android Market (more than 50% of the applications we tested) are vulnerable to this attack.

As part of this work, we develop a translation tool named Deja, which converts the proprietary Dalvik bytecode used by Android applications to standard Java bytecode, enabling the use of the ASM bytecode rewriting library.[2] Deja uses SSA-based dataflow analysis to infer the operand types, which must be explicitly specified in Java bytecode, and correctly reasons about important differences between the two formats (e.g., the bytecode verification process).[3]

In the IAB protocol, Google digitally signs the message notifying an application of a successful purchase. Although Google advises developers to verify this signature on a remote server before acknowledging the purchase, many applications either do not perform any verification or perform the verification on the device using the `java.security.Signature.verify` API.

The FreeMarket attack exploits this behavior by rewriting all calls to `java.security.Signature.verify` with a method that always returns true. To enable this rewriting, it first translates the application to Java bytecode using Deja, then invokes the ASM rewriting library on the Java bytecode. The rewritten application is translated back to Dalvik bytecode, then repackaged and signed so that it can be installed and executed on unmodified Android devices.

To evaluate the effectiveness of the FreeMarket attack, we perform the attack on 295 IAB applications from the Android Market: 126 applications on Android Market's top-2000 grossing list and 169 additional randomly-selected applications. We manually exercise the IAB functionality of each rewritten application to check whether the attack succeeded.

Our results indicate that 58.98% (174 applications) are vulnerable to the attack, and 22.03% (65 applications) are not vulnerable (i.e., the rewritten applications correctly refused to acknowledge the purchases). We were unable to evaluate the remaining 18.98% (56 applications), which were inoperable after the rewriting. Applications with greater revenue were less likely to be vulnerable to our attack, which is not surprising given the greater incentives for developers of higher-revenue applications to implement IAB securely despite the increased development costs.

Upon manual inspection, we find that most of the applications unaffected by this attack perform server-side verification, in accordance with Google's recommendations. Several applications perform validation in native code (which our rewriting tool does not handle) or use third-party cryptographic libraries to verify the signature locally.

Given the increasing popularity of IAB, we expect it will become an increasingly attractive target for attackers. We strongly recommend that developers use tamper-resistant mechanisms and server-side verification of cryptographic signatures in order to prevent automated attacks such as FreeMarket.

Acknowledgements. This material is based upon work supported by the MURI program under Air Force Office of Scientific Research Grant Nos. FA9550-08-1-0352 and FA9550-09-1-0539, and the National Science Foundation under Grant No. 0842695.

*The full version of this paper is available at `http://droidblaze.cs.berkeley.edu/freemarket.pdf`.

[1] `http://developer.android.com/guide/market/billing/billing_best_practices.html`

[2] `http://asm.ow2.org`

[3] Existing tools for this translation do not properly reason about some of these differences and consequently produce output that cannot be translated back to Dalvik bytecode.