Introduction to HICSS-47 Software Security for Mobile Platforms Minitrack

Daniel Plakosh  
CERT  
Software Engineering Institute  
Carnegie Mellon University  
dplakosh@cert.org

Robert Seacord  
CERT  
Software Engineering Institute  
Carnegie Mellon University  
rcs@cert.org

This minitrack focuses on the research and automation techniques that can be applied to mobile platforms to ensure that software developed for these devices is secure without compromising other system properties such as performance or reliability. In both the personal computer and mobile platform arena, current security engineering methods are demonstrably inadequate at identifying software vulnerabilities. These vulnerabilities are caused by software designs and implementations that do not adequately protect systems and by development practices that do not focus sufficiently on eliminating implementation defects that result in security flaws. This been especially true in the area of mobile platforms where one study found that, from 2010 to 2011, the number of new vulnerabilities in mobile operating systems jumped 93 percent. Additionally, according to Symantec Corp, 2011 was the also first year that mobile malware presented a tangible threat.

Android is the most widely used mobile platform, capturing a slight majority of the US and world smartphone markets. Android offers strong isolation for apps to prevent a potentially malicious app from accessing the protected data of other apps. However, there are two major weaknesses. First, Android lacks a fine-grained permission-granting mechanism. When a user installs an app, the app must request all potentially needed permissions upfront, and the user must either grant all requested permissions or cancel installing the app. The user cannot selectively grant only some permissions. So, users often grant potentially malicious apps more permissions than desired.

A second major weakness in Android lies in its complex inter-app communication system. Although this system is very powerful, it is hard for app developers to get security right. Since the same system is used for both inter-app and intra-app communication, it is easy for developers to inadvertently subvert Android's isolation protection and leave their apps vulnerable malicious apps.

Recent work at CERT includes the development of the Mobile SCALe—an extension of CERT’s Secure Coding Standards and source code analysis laboratory [1] to mobile platforms. In particular, CERT and CERT-affiliated authors have recently published a book on Java Coding Guidelines [2] that includes a listing of guidelines applicable to Android as well as applicable guidelines from The CERT Oracle Secure Coding Standard for Java [3]. These documents identify general Java secure coding rules that can be applied to the development and analysis of Android source code. Android-specific rules are also being developed in CERT’s secure coding wiki.

References


1 Mobile vulnerabilities increased by 93% in 2011 http://www.symantec.com/about/news/release/article.jsp?prid=20120429_01
3 https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=111509535