PHYS.ORG

New framework would facilitate use of new Android security modules

August 20 2014, by Matt Shipman

Computer security researchers from North Carolina State University and Technische Universität Darmstadt/CASED in Germany have developed a modification to the core Android operating system that allows developers and users to plug in new security enhancements. The new Android Security Modules (ASM) framework aims to eliminate the bottleneck that prevents developers and users from taking advantage of new security tools.

"In the ongoing arms race between white hats and black hats, researchers and developers are constantly coming up with new security extensions," says Dr. William Enck, an assistant professor of computer science at NC State and a senior author of a paper describing the new framework. "But these new tools aren't getting into the hands of users because every new extension requires users to change their device's firmware, or operating system (OS).

"The ASM framework allows users to implement these new extensions without overhauling their firmware," Enck says. "The framework is available now for security enthusiasts. But for widespread adoption, either Google or one of the Android phone manufacturers will need to adopt the framework and incorporate it into the OS."

The ASM framework allows the creation of custom security control modules that better protect phones owned by consumers and businesses. The custom security modules receive "callbacks" for every security-sensitive operation in the Android OS. In this context, a callback means that Android is contacting the security module to determine whether an operation should proceed.

"Our ASM framework can be used in various personal and enterprise scenarios. For instance, security modules can implement dual persona: i.e., enable users to securely use their smartphones and tablets at home and at work while strictly separating private and enterprise data," says Enck.

"Security modules can also enhance consumer privacy. The framework provides callbacks that can filter, modify, or anonymize data before it is shared with third-party apps, in order to protect personal information," Enck says. "For instance consider an app like Whatsapp, which usually copies all your contacts to its server – which is not needed for it to function." With ASM, the user can make sure Whatsapp only gets the information it really needs.

"In addition, we designed the framework to allow apps to create their own hooks, which could be enforced by the security module," Enck says. "This increases flexibility for app developers and allows them to benefit from the security protections provided by the module."

The researchers also went to great lengths to ensure that the ASM framework complies with the security guarantees Google and others make with app developers. For example, the framework can only make data access more restrictive.

The researchers will present a paper on the ASM framework Aug. 22 at the USENIX Security Symposium in San Diego, California. The researchers are now reaching out to Google and Android phone manufacturers to demonstrate the effectiveness of the ASM framework. More information on the ASM framework, including sourcecode, is available at http://www.androidsecuritymodules.org.

More information: Paper: "ASM: A Programmable Interface for Extending Android Security": www.enck.org/pubs/heuser-sec14.pdf

Authors: Stephan Heuser and Ahmad-Reza Sadeghi, Technische Universität Darmstadt; Adwait Nadkarni and William Enck, North Carolina State University

Presented: Aug. 22, 2014, at USENIX Security Symposium in San Diego, California

Abstract: Android, iOS, and Windows 8 are changing the application architecture of consumer operating systems. These new architectures required OS designers to rethink security and access control. While the new security architectures improve on traditional desktop and server OS designs, they lack sufficient protection semantics for different classes of OS customers (e.g., consumer, enterprise, and government). The Android OS in particular has seen over a dozen research proposals for security enhancements. This paper seeks to promote OS security extensibility in the Android OS. We propose the Android Security Modules (ASM) framework, which provides a programmable interface for defining new reference monitors for Android. We drive the ASM design by studying the authorization hook requirements of recent security enhancement proposals and identify that new OSes such as Android require new types of authorization hooks (e.g., replacing data). We describe the design and implementation of ASM and demonstrate its utility by developing reference monitors called ASM apps. Finally, ASM is not only beneficial for security researchers. If adopted by Google, we envision ASM enabling in-the-field security enhancement of Android devices without requiring root access, a significant limitation of existing bring-your-own-device solutions.

Provided by North Carolina State University

Citation: New framework would facilitate use of new Android security modules (2014, August 20) retrieved 25 April 2024 from https://phys.org/news/2014-08-framework-android-modules.html