Researchers find vulnerabilities in iPhone, iPad operating system

August 25 2016

An international team of computer science researchers has identified serious security vulnerabilities in the iOS - the operating system used in Apple's iPhone and iPad devices. The vulnerabilities make a variety of attacks possible.

"There's been a lot of research done on Android's operating systems, so

we wanted to take a closer look at Apple's iOS," says William Enck, an associate professor of computer science at North Carolina State University and co-author of a paper describing the work. "Our goal was to identify any potential problems before they became real-world problems."

The researchers focused on the iOS's "sandbox," which serves as the interface between applications and the iOS. The iOS sandbox uses a set "profile" for every third-party app. This profile controls the information that the app has access to and governs which actions the app can execute.

To see whether the sandbox profile contained any vulnerabilities that could be exploited by third-party apps, the researchers first extracted the compiled binary code of the sandbox profile. They then decompiled the code, so that it could be read by humans. Next, they used the decompiled code to make a model of the profile, and ran series of automated tests in that model to identify potential vulnerabilities.

Ultimately, the researchers identified vulnerabilities that would allow them to launch different types of attacks via third-party apps. Those attacks include:

- Methods of bypassing the iOS's privacy settings for contacts;
- Methods of learning a user's location search history;
- Methods of inferring sensitive information (such as when photos were taken) by accessing metadata of system files;
- Methods of obtaining the user's name and media library;
- Methods of consuming disk storage space that cannot be recovered by uninstalling the malicious app;
- Methods of preventing access to system resources, such as the address book; and
- Methods that allow apps to share information with each other without permission.

"We are already discussing these vulnerabilities with Apple," Enck says. "They're working on fixing the security flaws, and on policing any apps that might try to take advantage of them."

The international collaboration led to the paper "SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles" which will be presented end of October at the renowned ACM Conference on Computer and Communications Security (CCS) in Vienna.

More information: "SandScout: Automatic Detection of Flaws in iOS Sandbox Profiles" Authors: Luke Deshotels and William Enck, North Carolina State University; Mihai Chiroiu and Răzvan Deaconescu, University Politehnica of Bucharest; Lucas Davi and Ahmad-Reza Sadeghi, Technische Universität Darmstadt. Presented: Oct. 24-28, ACM Conference on Computer and Communications Security, Vienna Austria

Abstract
Recent literature on iOS security has focused on the malicious potential of third-party applications, demonstrating how developers can bypass application vetting and code-level protections. In addition to these protections, iOS uses a generic sandbox profile, called "container," to confine malicious or exploited third-party applications. In this paper, we present the first systematic analysis of the iOS container sandbox profile. We propose the SandScout framework to extract, decompile, formally model, and analyze iOS sandbox profiles as logic-based programs. We use our Prolog-based queries to evaluate file-based security properties of the container sandbox profile for iOS 9.0.2 and discover seven classes of exploitable vulnerabilities. These attacks affect nonjailbroken devices running later versions of iOS. We are working with Apple to resolve these attacks, and we hope SandScout will play a significant role in the development of sandbox profiles for future versions of iOS.

Provided by North Carolina State University