iOS Mobile Application Security (iMAS) Provides Additional Defense for iOS

Problem

Originally known as the Apple iPhone Operating System, iOS and its security features have evolved considerably since the unveiling of the iPhone in 2007. The latest iPhones are running iOS 7.x, which makes it difficult to craft and proliferate malware.

Does iOS meet all enterprise security needs today? Granted, iOS 7.x has considerable security in place and its attack surface has been reduced considerably. Many developers are convinced that Apple's Data Protection (DP) framework is secure enough for sensitive application data.

However, other experts in the field have described iOS security attacks and work-arounds that have exposed and allowed app data exfiltration. One problem is that many users do not set their device passcode, rendering DP security useless. Or users rely on the default four-digit passcode, which can be easily brute-forced and cracked. Many organizations that have an MDM solution in place do not enforce complex system passcodes. Malware can be an issue with the increased use of custom applications downloaded from enterprise app stores as malware could be included unbeknownst to the developer via open source code integration. Lastly, iPads and iPhones are easily lost, increasing the chances of physical attacks. All this leaves iOS devices, especially applications containing enterprise data, vulnerable to attack.

Solution

MITRE researchers have developed a framework of security controls that significantly enhance an application security profile and reduce its task surface. We call this framework "iMAS" for iOS Mobile Application Security. The research team focused on the application data as the target—including, for example, enterprise data, tactical operational data, and patient health info.

The framework currently consists of nine security controls, providing capabilities to:

- Protect iOS applications and data beyond the Apple provided security model, for example, protecting against malware and physical access attacks with secure static and dynamic application controls.
- Reduce an adversary's ability and efficiency to perform recon, exploitation, control and execution on iOS mobile applications.
- Transform the effectiveness of the existing iOS security model across major vulnerability areas, including the No Passcode or four-digit System Passcode, jailbreak, debugger/run-time, flash storage, and keychain.

Results/Impact

Over the past several years, the iMAS team has researched many different possible security controls to bolster the iOS application security model. We are providing the results in an open source application framework. The controls—which include access protection, data at rest, data in use, and anti-tampering techniques—are available on gituhub.com (http://project-imas.github.io/). The iMAS library provides developers with a set of tools to accomplish various security tasks in their apps.

The site has been active for 10 months and has considerable traffic and use including 39,000 page views, 24,000 unique visitors across 115 countries. The github statistics consist of 65 forks (developers making their own copy of the code to make use of) and over 340 stars (which indicates 340 developers are tracking iMAS activity).

Additionally, iMAS is featured on the OWASP mobile security site as its number one endorsed mobile security tool.

The iMAS team will continue to explore technical security controls and share its findings. And we will continue to actively open source iMAS and leverage the community of developers to enhance our research and maintain relevance and currency.

For more information, please send inquiries to CEMinnovation@mitre.org.

Approved for Public Release; Distribution Unlimited. 14-0598