Analysis of Apple's iOS and Google's Android Platform

Symantec announced the publication of “A Window Into Mobile Device Security: Examining the security approaches employed in Apple’s iOS and Google’s Android” (PDF). This whitepaper conducts an in-depth, technical evaluation of the two predominant mobile platforms, Apple’s iOS and Google’s Android, in an effort to help corporations understand the security risks of deploying these devices in the enterprise.

Chief among the findings is that while the most popular mobile platforms in use today were designed with security in mind, these provisions are not always sufficient to protect sensitive enterprise assets that regularly find their way onto devices. Complicating matters, today’s mobile devices are increasingly being connected to and synchronized with an entire ecosystem of 3rd-party cloud and desktop-based services outside the enterprise’s control, potentially exposing key enterprise assets to increased risk.

Click to Tweet: Symantec analysis finds iOS and Android security better than that of PCs, but major gaps remain: http://bit.ly/jYflt3

The paper offers a detailed analysis of the security models employed by Apple’s iOS and Google’s Android platforms, evaluating each platform’s effectiveness against today’s major threats, including:

• Web-based and network-based attacks
• Malware
• Social engineering attacks
• Resource and service availability abuse
• Malicious and unintentional data loss
• Attacks on the integrity of the device’s data

This analysis has led to some important conclusions:

• While offering improved security over traditional desktop-based operating systems, both iOS and Android are still vulnerable to many existing categories of attacks.
• iOS’s security model offers strong protection against traditional malware, primarily due to Apple’s rigorous app certification process and their developer certification process, which vets the identity of each software author and weeds out attackers.
• Google has opted for a less rigorous certification model, permitting any software developer to create and release apps anonymously, without inspection. This lack of certification has arguably led to today’s increasing volume of Android-specific malware.

• Users of both Android and iOS devices regularly synchronize their devices with 3rd-party cloud services (e.g., web-based calendars) and with their home desktop computers. This can potentially expose sensitive enterprise data stored on these devices to systems outside the governance of the enterprise..
• So-called “jailbroken” devices, or devices whose security has been disabled, offer attractive targets for attackers since these devices are every bit as vulnerable as traditional PCs.

“Today’s mobile devices are a mixed bag when it comes to security,” said Carey Nachenberg, Symantec Fellow and Chief Architect, Symantec Security Technology and Response. “While more secure than traditional PCs, these platforms are still vulnerable to many traditional attacks. Moreover, enterprise employees are increasingly using unmanaged, personal devices to access sensitive enterprise resources, and then connecting these devices to 3rd-party services outside of the governance of the enterprise, potentially exposing key assets to attackers.”

Related
• White Paper: A Window Into Mobile Device Security: Examining the security approaches employed in Apple’s iOS and Google’s Android (PDF)
• Blog Post: New Symantec Research: The Current State of Mobile Device Security
• Podcast: A Window Into Mobile Device Security
• Infographic: Top Threats Targeting Mobile Devices
• SlideShare Presentation: Mobile Device Security
• Expert Biography: Carey Nachenberg
• Symantec Mobile Solutions

Connect with Symantec
• Follow Symantec ThreatIntel on Twitter
• Follow Symantec on Twitter
• Join Symantec on Facebook
• Join Norton on Facebook
• Read Industry Trends on Delicious
• View Symantec’s SlideShare Channel
• Subscribe to Symantec News RSS Feed
• Visit Symantec Connect Business Community

About Security Technology and Response
The Security Technology and Response (STAR) organization, which includes Security Response, is a worldwide team of security engineers, threat analysts and researchers that provides the underlying functionality, content and support for all Symantec corporate and consumer security products. With Response centers located throughout the world, STAR monitors malicious code reports from more than 130 million systems across the Internet, receives data from 240,000 network sensors in more than 200 countries and tracks more than 25,000 vulnerabilities affecting more than 55,000 technologies from more than 8,000 vendors. The team uses this vast intelligence to develop and deliver the world’s most comprehensive security protection.

More information is available at www.symantec.com [1].

Links:
[1] http://www.symantec.com