Publication: Phys.org
Date: 5 December 2013
Headline: Researchers bypass Apple security gauntlet

Researchers bypass Apple security gauntlet

December 5, 2013

Hacking programs disguised as games are helping Apple to improve the security of devices operating on its iOS platform.

Software companies work hard to protect their customers' personal data from malicious applications, or 'apps', but even the most secure devices can be vulnerable. Skilled and independent computer scientists, such as Jin Han and co-workers at the A*STAR Institute for Infocomm Research and the Singapore Management University, can greatly assist companies by spotting security weaknesses before they are exploited.

Han and co-workers recently published a detailed comparison of the two very different security models used by the big players in mobile software, Apple's iOS platform and Google's Android. Now, the researchers have developed subtle attack apps that test the secretive model of mobile security used in iOS.

Apple's preferred security model is 'closed source'. This means that the company does not publish details of how apps are vetted before becoming available in their iTunes Store. Apple also refrains from publishing the internal code that decides whether apps can control phone functions such as contacts, calendars or cameras.

Despite this secrecy, the researchers were able to develop generic attack codes that enabled third-party control of iOS devices. They demonstrated seven different attack apps, disguised as games, that performed malicious actions including cracking the device's PIN, taking photographs and sending text messages without the user's awareness.

"We utilized private function calls to gain privileges that are not intended for third-party developers," explains Han. "Furthermore, we found a way to bypass Apple's vetting process so that our apps, embedded with proof-of-concept attacks, could be published on iTunes."

The attack apps worked on both iOS 5 and 6, although the team was careful to include secret triggers to protect any public users. The researchers have shared all of their findings with Apple and published recommendations on how the company should fix these vulnerabilities.

"Apple responded very quickly after we informed them about our findings, and before the release of the new iOS 7 platform," says Han. He expects that the company adopted countermeasures similar to those described in his team's paper, but cannot confirm this since iOS is closed source.

The ongoing debate over open- versus closed-source development will continue to rage among information technology specialists. Nevertheless, Han notes that their attack-app codes could, with some modifications, probably also bypass the permissions-based security model used in Android. "My personal opinion is that closed-source development is not good for security. A cryptosystem should be secure even if everything about the system, except the key, is public knowledge. I think the same principle applies to operating systems."