Publication: Phys Org
Date: 6 November 2013
Headline: Enhancing security in Apple devices

Enhancing security in Apple devices

12 hours ago

Boosting security for mobile devices is a top priority for service providers and consumers. Credit: Geber86/iStockphoto.com

A*STAR's Institute for Infocomm Research has helped to fix three security weaknesses in Apple's iOS mobile operating system.

A Singapore-based team of researchers has been acknowledged by Apple Inc. for helping to strengthen the security of the company's latest mobile operating system, iOS 7, which runs on its popular smartphones and tablets. The team identified three security weaknesses related to data protection, telephony and Twitter use, which Apple then rectified prior to the much-anticipated global launch of iOS 7 in September 2013.

With each successive update to the iOS operating system, Apple strives to offer a host of new features aimed at broadening and improving the user experience. New functionalities and the rise of third-party applications, however, risk compromising the security of the iOS platform. "While Apple has made significant efforts to secure iOS and provide a secure mobile platform for its users, we wanted to test just how secure the operating system was and how to improve security further if any vulnerabilities were identified," says Jianying

Zhou of the A*STAR Institute for Infocomm Research (I2R). "Platform security, user privacy and availability of services are some of the top security and privacy concerns of mobile users."

Working in collaboration with researchers from the School of Information Systems at Singapore Management University, the A*STAR team uncovered security flaws that would enable hackers to access a user's passcode, interfere with incoming calls and post unauthorised content on Twitter.

The researchers developed multiple proof-of-concept studies—designed to test whether iOS would work as intended—to investigate three theoretical attack scenarios for the iPhone 4 and newer models, the fifth-generation iPod touch onwards, and the iPad 2 and later versions. In each case, the researchers proposed solutions that could reinforce security through additional entitlement checks, as well as ways to improve Apple's vetting process for third-party applications.

The motivation behind the research, Zhou explains, was "to protect the security and privacy of businesses and individuals." Apple's iOS and Google's Android are two of the most popular mobile operating systems in terms of the number of users worldwide. "A lot of research had been conducted on the security of the Android platform but relatively few efforts focusing on the security of the iOS platform when we embarked on this research in 2012," says Zhou. The team notified Apple of their findings in October 2012 and the weaknesses were fixed before the release of iOS 7 in September 2013. "It took almost a year because the issues were quite complicated to address," explains Zhou.

With over 100 PhD-level researchers active in the fields of analytics, cyber security and human language and speech technologies, the I2R is Singapore's largest intelligence, communications and media research institute. The I2R partners with leading universities and companies through joint laboratories and feasibility studies to develop innovative solutions for a wide spectrum of consumer products.

"We are encouraged to perform mission-oriented research that could help to address real-world problems and make an impact," says Zhou. "We aim for a balance between basic science and industry development. By collecting input from industry on their requirements, we can predict future trends that guide our research; this strategy means that our findings have a better chance of being translated into useful technologies."