Media Release

For Immediate Release

Total: 5 pages

I²R and SMU strengthen security of iOS platform with mitigating measures on proof-of-concept attacks

I²R, Singapore's largest ICM research institute, and SMU are the first in Singapore to discover three security weaknesses in iOS 7, which Apple Inc. has recognised and rectified

1.   **Singapore, 2 October 2013** - Researchers from the Infocomm Security Department at A*STAR's Institute for Infocomm Research (I²R) and Singapore Management University's (SMU) School of Information Systems have identified three proof-of-concept attacks which can be performed by third-party applications to threaten the security of the iOS platform. The attacks, which include pass-code cracking, interference with or control of telephony functionality and sending tweets without the user's awareness and permission, have been rectified by Apple Inc in its latest operating system, iOS 7.

2.   Apple's iOS operating system is one of the most popular mobile operating systems in terms of the number of users. As of January 2013, 500 million iOS devices have been sold worldwide, and Apple's iTunes App Store has over 800,000 iOS third-party applications with downloads exceeding 40 billion.[1]

3.   Third-party applications are pervasively installed on these iOS devices as they provide various functions that significantly extend the usability of the mobile devices. However, these third-party applications pose potential threats by compromising the personal and business data stored on the devices.

4.   Between June to October 2012, I²R and SMU researchers embarked on a task to unveil a generic attack vector that enables third-party applications to launch attacks on non-jailbroken

---

[1] Source: App Store Tops 40 Billion Downloads with Almost Half in 2012 (January 2013), http://www.apple.com/sg/pr/library/2013/01/07App-Store-Tops-40-Billion-Downloads-with-Almost-Half-in-2012.html

iOS devices. The research team constructed multiple proof-of-concept attacks such as cracking the device PIN, blocking incoming calls and posting unauthorised tweets. To overcome these security breaches, the team proposed several mitigation methods to enhance the vetting process and the iOS application sandbox. Apple Inc. was notified of these security vulnerabilities and rectified them for the launch of iOS 7, acknowledging I^{2}R's and SMU's contributions. *Please see Appendix A for full information on the three security fixes developed by the I^{2}R and SMU research team in iOS 7.*

5.   Dr Tan Geok Leng, Executive Director of the Institute for Infocomm Research (I^{2}R) said, "I^{2}R's expertise in the infocomm security arena has once again been harnessed to benefit the mobile community. We are proud of our researchers' efforts in boosting the security of Apple's latest operating system – the iOS 7. The enhanced data protection, secured telephony functionality and protected Twitter functionality will let iOS end users utilise their mobile devices for leisure or work with a peace of mind."

6.   SMU's Vice Provost of Research and Dean of the School of Information Systems Professor Steven Miller, said "Information security is a core area of research at the SMU School of Information Systems. Our research team not only aims to create impact in the research community, but also in the wider community. I am pleased to note that our researchers have been able to leverage our expertise and technologies to enhance security in cyberspace, and in this case help strengthen the security of the iOS platform to protect the security and privacy of businesses and individuals."

-End-

For more information, please contact:

Ms. Doris Yang   Mr. Teo Chang Ching
Institute for Infocomm Research   Singapore Management University
DID: (65) 6419 6525   DID: 6828 0451
Email: yangscd@scei.a-star.edu.sg   Email: ccteo@smu.edu.sg

About Institute for Infocomm Research (I^{2}R)
Singapore's largest ICM research institute, I^{2}R (pronounced as i-squared-r) is a member of the Agency for Science, Technology and Research (A*STAR) family. Established in 2002, our vision is to power a vibrant and strong infocomm ecosystem in Singapore. I^{2}R focuses on conducting mission oriented research to address key challenges faced locally. At I^{2}R, intelligence,

communications and media (ICM) form our 3 strategic thrusts. Our research capabilities are in information technology, wireless and optical communication networks, interactive and digital media, sensors, signal processing and computing. We perform R&D in ICM technologies to develop holistic solutions across the ICM value chain and we believe that the greatest impact is created when research outcomes are translated into technologies our partners can readily deploy at a competitive advantage. For more information about I^2R, please visit www.i2r.a-star.edu.sg.

About the Agency for Science, Technology and Research (A*STAR)

The Agency for Science, Technology and Research (A*STAR) is the lead agency for fostering world-class scientific research and talent for a vibrant knowledge-based and innovation-driven Singapore. A*STAR oversees 14 biomedical sciences and physical sciences and engineering research institutes, and six consortia & centres, located in Biopolis and Fusionopolis as well as their immediate vicinity. A*STAR supports Singapore's key economic clusters by providing intellectual, human and industrial capital to its partners in industry. It also supports extramural research in the universities, and with other local and international partners. For more information about A*STAR, please visit www.a-star.edu.sg.

About Singapore Management University

Singapore Management University (SMU) is internationally recognised for its world class research and distinguished teaching focused on the world of business and management, and on information systems technology and management. Established in 2000, SMU's mission is to generate leading edge research with global impact and develop broad-based, creative and entrepreneurial leaders for the knowledge-based economy. Home to over 8,500 students, SMU comprises six schools: School of Accountancy, Lee Kong Chian School of Business, School of Economics, School of Information Systems, School of Law and School of Social Sciences, offering undergraduate, postgraduate and executive development programmes. www.smu.edu.sg

About SMU School of Information Systems

The SMU School of Information Systems (SIS) was set up in 2003 to extend SMU's research and education efforts into the areas of Information Systems Technology, Information Systems Management, and problems at the intersection of IS technology and management. SIS is distinct from the other five schools of SMU in that it is the only academic unit within the University which falls under Singapore's Science & Technology cluster of academic units as defined by the Ministry of Education.

The School possesses deep research R&D capability in four strategically-selected areas of IS technology: Information Security & Data Privacy; Data Management & Analytics; Intelligent Systems & Decision Analytics; and Software Systems. The fifth strategic area of the School is Information Systems & Management, where the faculty investigate the managerial aspects and business impact of IT in public and private sector organisations, and across value chains, markets and industries. Since its inception, SIS has established a strategic partnership with Carnegie Mellon. Through SIS, SMU and Carnegie Mellon launched the Living Analytics Research Centre (www.larc.smu.edu.sg) in 2011. More information on SIS can be found at: www.sis.smu.edu.sg

APPENDIX A:

Full information on the three security fixes developed by the I^{2}R and SMU research team:

1.   Data Protection

Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

Impact: Apps could bypass passcode-attempt restrictions

Description: A privilege separation issue existed in Data Protection. An app within the third-party sandbox could repeatedly attempt to determine the user's passcode regardless of the user's "Erase Data" setting. This issue was addressed by requiring additional entitlement checks.

Researchers involved: Jin Han of the Institute for Infocomm Research working with Qiang Yan and Su Mon Kywe of Singapore Management University

2.   Telephony

Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

Impact: Malicious apps could interfere with or control telephony functionality

Description: An access control issue existed in the telephony subsystem. Bypassing supported APIs, sandboxed apps could make requests directly to a system daemon interfering with or controlling telephony functionality. This issue was addressed by enforcing access controls on interfaces exposed by the telephony daemon.

Researchers involved: Jin Han of the Institute for Infocomm Research working with Qiang Yan and Su Mon Kywe of Singapore Management University; Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee from the Georgia Institute of Technology

3.   Twitter

Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

Impact: Sandboxed apps could send tweets without user interaction or permission

Description: An access control issue existed in the Twitter subsystem. Bypassing supported APIs, sandboxed apps could make requests directly to a system daemon interfering with or controlling Twitter functionality. This issue was addressed by enforcing access controls on interfaces exposed by the Twitter daemon.

Researchers involved: Jin Han of the Institute for Infocomm Research working with Qiang Yan and Su Mon Kywe of Singapore Management University; Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee from the Georgia Institute of Technology