SMU RESEARCHERS BOOST SECURITY OF GOOGLE'S ANDROID MOBILE SYSTEMS

4 Jul 2016

Security weaknesses discovered in Android 4.4 and Android 5.1, which Google has recognised and rectified

Singapore, 4 July 2016 (Monday) – Ms Su Mon Kywe, a PhD candidate, and Associate Professor Li Yingjiu from SMU's School of Information Systems have discovered several security weaknesses in Google's Android 4.4 and Android 5.1 systems when performing vulnerability analysis on the Android framework as one of their security research projects with Huawei. The weaknesses were reported to Google which has subsequently fixed the vulnerabilities in the newer versions of their Android systems.

The SMU team's purpose of conducting the vulnerability analysis was to discover security loopholes in the Android systems and report them in a timely manner, so that platform providers such as Google and Huawei can fix the vulnerabilities before they are exploited by real hackers.

The team's research involved several static source-code analysis, such as building call-graphs and analysing data-flow, on Android Open Source Project (AOSP) published by Google. The source code of AOSP is also used by other platform vendors, such as Samsung and Huawei, with their own customisations. The result of SMU researchers' analysis revealed that several types of attacks can be launched on mobile users using AOSP versions 4.4 and 5.1.

The researchers found that without requesting for any permission, a malicious third-party application can gain access to the mobile device's identification number, phone service state, SIM card state, Wi-Fi and network information, as well as user setting information, such as airplane, location, Near Field Communication (NFC), Universal Serial Bus (USB) and power modes. A hacker can also interfere with Bluetooth services, and block incoming emails, calendar events, and Google documents. Moreover, a hacker can alter the volumes of mobile devices and trigger alarm tones and ringtones that users had set for their mobile devices.

The SMU research team and Huawei researchers, Dr Li Tieyan and Dr Wu YongZheng reported the findings to Google in November 2015. A Common Vulnerability Exposure number (CVE-2016-0831) was assigned to the case. Google has subsequently fixed the vulnerabilities in the newer versions of their Android systems, and has publicly acknowledged the SMU team's contribution in its Security Bulletin published in March 2016 (https://source.android.com/security/bulletin/2016-03-01.html).

Professor Pang Hwee Hwa, Dean of SMU School of Information Systems said, "We are proud of our researchers' efforts in boosting the security of Google's Android system, which is one of the most popular mobile operating systems in the world. By leveraging our expertise and technologies in cybersecurity, the SMU team has been able to create an impact beyond the academic and research communities, to bring about benefits to businesses and individuals."

For more information, please contact

Teo Chang Ching (Mr)

Senior Assistant Director

Corporate Communications

Singapore Management University

DID: 6828 0451

Email: ccteo@smu.edu.sg (mailto:ccteo@smu.edu.sg)

[Photo: Ms Su Mon Kywe and Associate Professor Li Yingjiu from SMU's School of Information Systems have discovered several security weaknesses in Google's Android 4.4 and Android 5.1 systems when performing vulnerability analysis on the Android framework.. The weaknesses were reported to Google which has subsequently fixed the vulnerabilities in the newer versions of their Android systems.]

Last updated on **7 Jul 2016**.