Researchers jailbreak iOS 7.1.2

August 1 2014

Security researchers at the Georgia Tech Information Security Center (GTISC) have discovered a way to jailbreak current generation Apple iOS devices (e.g., iPhones and iPads) running the latest iOS software.

The jailbreak, which enables circumvention of Apple's closed platform, was discovered by analyzing previously patched vulnerabilities with incomplete fixes.

It shows that quick workarounds mitigating only a subset of a multi-step attack leave these devices vulnerable to exploitation. Patching all vulnerabilities for a modern, complex software system (i.e., Windows and iOS) is often difficult due to the volume of bugs and response-time requirements.

" Our work shows that software vendors must patch all publicly disclosed threats, as they may be exploited in other, equally disruptive attacks," said Yeongjin Jang, one of the Ph.D. students who led this study.

During Black Hat USA, the GTISC research team will disclose the process for jailbreaking the current version of iOS (7.1.2) on any iOS device, including the iPhone 5s.

"We start by finding new ways to exploit vulnerabilities with incomplete patches," said Tielei Wang, a GTISC faculty member who worked closely with Jang as lead of the project. "Then, we use those vulnerabilities to discover new avenues of attack. We'll detail these vulnerabilities and the exploit techniques that we developed."

A Georgia Tech team that includes Ph.D. students Yeongjin Jang and Byoungyoung Lee, and research scientists Tielei Wang and Billy Lau discovered the jailbreak.

Provided by Georgia Institute of Technology