Research identifies Android security weaknesses caused by performance design

June 19 2014

Georgia Tech researchers have identified a weakness in one of Android's security features and will present their work at Black Hat USA 2014, which will be held August 6-7 in Las Vegas.

The research, titled Abusing Performance Optimization Weaknesses to

Bypass ASLR, identifies an Android performance feature that weakens a software protection called Address Space Layout Randomization (ASLR), leaving software components vulnerable to attacks that bypass the protection. The work is aimed at helping security practitioners identify and understand the future direction of such attacks.

The work was conducted at the Georgia Tech Information Security Center (GTISC) by Ph.D. students Byoungyoung Lee and Yeongjin Jang and research scientist Tielei Wang, and reveals that the introduction of performance optimization features can inadvertently harm the security guarantees of an otherwise vetted system. In addition to describing how vulnerabilities originate from such designs, they demonstrate real attacks that exploit them.

"To optimize object tracking for some programming languages, interpreters for the languages may leak address information," said Lee, lead researcher for the effort. "As a concrete example, we'll demonstrate how address information can be leaked in the Safari web browser by simply running some JavaScript."

Bypassing ASLR using hash table leaks was previously believed to be obsolete due to its complexity. By exhaustively investigating various language implementations and presenting concrete attacks, the research aims to show that the concern is still valid.

"As part of our talk, we'll present an analysis of the Android Zygote process creation model," Lee said. "The results show that Zygote weakens ASLR as all applications are created with largely identical memory layouts. To highlight the issue, we'll show two different ASLR bypass attacks using real applications – Google Chrome and VLC Media Player."

The Black Hat Briefings were created about 16 years ago to provide

computer security professionals a place to learn the very latest in information security risks, research and trends. Presented by the brightest in the industry, the briefings cover everything from critical information infrastructure to widely used enterprise computer systems to the latest InfoSec research and development. These briefings are vendor-neutral, allowing the presenters to speak candidly about the real problems and potential solutions across both the public and private sectors.

Provided by Georgia Institute of Technology