

# Hacking experts find new ways to attack Android phones

Jim Finkle, Reuters

(Reuters) - Hacking experts on Wednesday demonstrated ways to attack Android smartphones using methods they said work on virtually all such devices in use today, despite recent efforts by search engine giant Google to boost protection.

Experts showed off their prowess at the Black Hat hacking conference in Las Vegas, where some 6,500 corporate and government security technology workers gathered to learn about emerging threats to their networks.

"Google is making progress, but the authors of malicious software are moving forward," said Sean Schulte of Trustwave's SpiderLabs.

Google spokeswoman Gina Scigliano declined to comment on the security concerns or the new research.

Accuvant researcher Charlie Miller demonstrated a method for delivering malicious code to Android phones using a new Android feature known as near field communications.

"I can take over your phone," Miller said.

Near field communications allow users to share photos with friends, make payments or exchange other data by bringing Android phones within a few centimeters of similarly equipped devices such as another phone or a payment terminal.

Miller said he figured out how to create a device the size of a postage stamp that could be stuck in an inconspicuous place such as near a cash register at a restaurant. When an Android user walks by, the phone would get infected, said Miller.

He spent five years as a global network exploit analyst at the U.S. National Security Agency, where his tasks included breaking into foreign computer systems.

"WILD WEST"

Miller and another hacking expert, Georg Wicherski of CrowdStrike, have also infected an Android phone with a piece of malicious code that Wicherski unveiled in February.

That piece of software exploits a security flaw in the Android browser that was publicly disclosed by Google's Chrome browser development team, according to Wicherski.

## Hacking experts find new ways to attack Android phones

Published on Electronic Component News (<http://www.ecnmag.com>)

---

Google has fixed the flaw in Chrome, which is frequently updated, so that most users are now protected, he said.

But Wicherski said Android users are still vulnerable because carriers and device manufacturers have not pushed those fixes or patches out to users.

Marc Maiffret, chief technology officer of the security firm BeyondTrust, said: "Google has added some great security features, but nobody has them."

Experts say iPhones and iPads don't face the same problem because Apple has been able to get carriers to push out security updates fairly quickly after they are released.

Two Trustwave researchers told attendees about a technique they discovered for evading Google's "Bouncer" technology for identifying malicious programs in its Google Play Store.

They created a text-message blocking application that uses a legitimate programming tool known as java script bridge. Java script bridge lets developers remotely add new features to a program without using the normal Android update process.

Companies including Facebook and LinkedIn use java script bridge for legitimate purposes, according to Trustwave, but it could also be exploited maliciously.

To prove their point, they loaded malicious code onto one of their phones and remotely gained control of the browser. Once they did that, they could force it to download more code and grant them total control.

"Hopefully Google can solve the problem quickly," said Nicholas Percoco, senior vice president of Trustwave's SpiderLabs. "For now, Android is the Wild West."

(Editing by Paul Tait)

**Source URL (retrieved on 08/31/2014 - 6:30am):**

<http://www.ecnmag.com/news/2012/07/hacking-experts-find-new-ways-attack-android-phones>