Researchers exploit cellular tech flaws to intercept phone calls

By jvijayan

Published: 2013-08-01 · Archived: 2026-04-06 02:10:07 UTC

LAS VEGAS — Researchers showed a Black Hat audience how femotcell technology, used by phone companies to boost cell phone coverage, can be hacked to intercept cell phone calls, text messages and other data.

Tom Ritter and Doug DePerry , researchers from iSec Partners, used an femtocell from Verizon to demonstrate how hackers can eavesdrop on phone conversations and see text messages and photos sent or received by nearby cell phone users.

The femtocells used by other phone carriers can be exploited as well, the researchers noted at the hacker conference here this week.

Femtocells are small, low-power base stations provided by phone companies to extend cellular coverage, especially inside buildings and facilities with spotty coverage. The devices use cable or DSL services to connect to a service providers' network.

Nearby mobile phones automatically connect to femtocells if both are from the same service provider. The phone sends all traffic through the femtocell.

Ritter and DePerry gained root access to the Linux operating system used in Verizon's femotcell by interfacing with he device via an HDMI port at the base of the system. Then they used the root access to tweak the femtocell to intercept voice and text messages from cell phones connected to the device.

As part of the demonstration, the researchers intercepted text messages sent by some of those at the presentation and replayed audio of a phone call made by one of the researchers during the demo. They also showed how root access on a femotcell can be used to clone cell phones connected to the device.

The researchers noted that Verizon patched the flaw in its femtocells after it was notified. But they added that femtocells from other vendors are vulnerable to the same kind of exploits.

Alex Watson, director of security research at Websense Inc said the research by Ritter and DePerry shows how cellular networks are as susceptible to security vulnerabilities as WiFi networks. He noted that service providers are deploying femtocells in growing numbers to expand their coverage, exposing a lot of users to potential hacks.

"They showed that cellular networks are not bullet proof. They showed that cellular technologies do have flaws and cannot be taken as perfect," he said.

IT security managers should pay attention to such risks and ensure that cell phones that connect to the corporate network have multiple layers of protection, including encryption of data at rest and in transmission.

Jaikumar Vijayan *covers data security and privacy issues, financial services security and e-voting for* Computerworld. *Follow Jaikumar on Twitter at @jaivijayan, or subscribe to Jaikumar's RSS feed . His email address is jvijayan@computerworld.com.*
