German Researchers Discover a Flaw That Could Let Anyone Listen To Your Cell Calls

By Craig Timberg
December 18, 2014
REUTERS/Kacper Pempel

German researchers have discovered security flaws that could let hackers, spies and criminals listen to private phone calls and intercept text messages on a potentially massive scale – even when cellular networks are using the most advanced encryption now available.

The flaws, to be reported at a hacker conference in Hamburg this month, are the latest evidence of widespread insecurity on SS7, the global network that allows the world's cellular carriers to route calls, texts and other services to each other. Experts say it's increasingly clear that SS7, first designed in the 1980s, is riddled with serious vulnerabilities that undermine the privacy of the world's billions of cellular customers.

The flaws discovered by the German researchers are actually functions built into SS7 for other purposes – such as keeping calls connected as users speed down highways, switching from cell tower to cell tower – that hackers can repurpose for surveillance because of the lax security on the network.

Those skilled at the myriad functions built into SS7 can locate callers anywhere in the world, listen to calls as they happen or record hundreds of encrypted calls and texts at a time for later decryption. There also is potential to defraud users and cellular carriers by using SS7 functions, the researchers say.

These vulnerabilities continue to exist even as cellular carriers invest billions of dollars to upgrade to advanced 3G technology aimed, in part, at securing communications against unauthorized eavesdropping. But even as individual carriers harden their systems, they still must communicate with each other over SS7, leaving them open to any of thousands of companies worldwide with access to the network. That means that a single carrier in Congo or Kazakhstan, for example, could be used to hack into cellular networks in the United States, Europe or anywhere else.

"It's like you secure the front door of the house, but the back door is wide open," said Tobias Engel, one of the German researchers.

Engel, founder of Sternraute, and Karsten Nohl, chief scientist for Security Research Labs, separately discovered these security weaknesses as they studied SS7 networks in recent months, after The Washington Post reported the widespread marketing of surveillance systems that use SS7 networks to locate callers anywhere in the world. The Post reported that dozens of nations had bought such systems to track surveillance targets and that skilled hackers or criminals could do the same using functions built into SS7. (The term is short for Signaling System 7 and replaced previous networks called SS6, SS5, etc.)

The researchers did not find evidence that their latest discoveries, which allow for the interception of calls and texts, have been marketed to governments on a widespread basis. But vulnerabilities publicly reported by security researchers often turn out to be tools long used by secretive intelligence services, such as …

To read this article in its entirety, go to:
http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/