Researchers explore stealthy injections of voice commands

16 October 2015, by Nancy Owano

Credit: Peter Griffin/Public Domain

French researchers want you to listen up about voice-controlled assistants Siri and Google Now. These assistants can also issue orders from a hacker even if the mischief maker issues commands in silence. This was Wednesday news from Andy Greenberg, senior writer for *Wired*.

The findings are from ANSSI (Agence nationale de la sécurité des systèmes d'information, or French Network and Information Security Agency), a government agency focused on information security. ANSSI addresses the challenge of cyberattacks, and is described as an interministerial agency attached to the Prime Minister's office.

How this would work: radio waves silently trigger voice commands on any Android phone or iPhone that has Google Now or Siri enabled, provided that the phone has a pair of headphones with a microphone plugged into its jack (it only works on phones with microphone-enabled headphones or earbuds plugged into them).

SC Magazine said, "Because the signals are coming through the mic, the smartphone considers them voice commands. From there the French spooks can have their way with your phone, sending texts and emails and even opening webpages that contain malware."

The setup involves a laptop running GNU Radio, a USRP software-defined radio, an amplifier, and an antenna, said Greenberg. The phone cord serves as the attacker's antenna "exploiting its wire to convert surreptitious electromagnetic waves into electrical signals that appear to the phone's operating system to be audio coming from the user's microphone."

The wires on that accessory can convert electromagnetic waves into electrical signals that, for iOS and Android, are the equivalent of the user's voice saying "Hey Siri" or "Ok Google."

The hacker could instruct Siri or Google Now to make calls and send texts, dial the hacker's number to turn the phone into an eavesdropping device, send the phone's browser to a malware site, or send spam and phishing messages via email, Facebook, or Twitter, added Greenberg.

How close to the victim must the attacker be? In its smallest form, the range is about six and a half feet. "In a more powerful form that requires larger batteries and could only practically fit inside a car or van, the researchers say they could extend the attack's range to more than 16 feet," Greenberg said.

JC Torres in *SlashGear* thought of a worrying scenario if the attack were to happen in its smallest form: "The contraption can be small enough to fit in a backpack but is limited to 6.5 feet in range. Imagine standing in the midst of a crowd, sending malicious commands to any vulnerable smartphone."

The researchers have a paper on their exploration,

titled "IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones." The authors are José Lopes Esteves and Chaouki Kasmi.

They stated in the abstract that they exploited the principle of front-door coupling on smartphones headphone cables with specific electromagnetic waveforms.

"We present a smart use of intentional electromagnetic interference, resulting in finer impacts on an information system than a classical denial of service effect. As an outcome, we introduce a new silent remote voice command injection technique on modern smartphones."

More information: IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones, *Electromagnetic Compatibility, IEEE Transactions on* , ieeexplore.ieee.org/xpl/abstra … rue&arnumber=7194754

Abstract
Numerous papers dealing with the analysis of electromagnetic attacks against critical electronic devices have been made publicly available. In this paper, we exploit the principle of front-door coupling on smartphones headphone cables with specific electromagnetic waveforms. We present a smart use of intentional electromagnetic interference, resulting in finer impacts on an information system than a classical denial of service effect. As an outcome, we introduce a new silent remote voice command injection technique on modern smartphones.