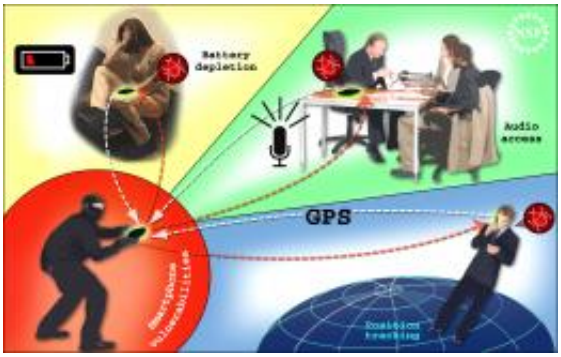
Can Clever Hackers Target Smart Phones?

April 2 2010



Smart phones are becoming a common part of everyday life, but the same capabilities that make them so useful offer opportunities for hackers. Credit: Zina Deretsky, National Science Foundation

(PhysOrg.com) -- Smart phones are becoming a common part of everyday life. Millions of Americans are using these powerful devices whose impressive capabilities and features rival that of desktop computers from just a few years ago, including new tools that can help simplify everyday tasks such as finding a parking garage or the nearest drycleaner.

But suppose you're a criminal who wants to surreptitiously monitor someone's every move and even eavesdrop wherever they take their phone? Yes, as it turns out, there's an ap for that, too.

Few smart phone users realize that the same characteristics that make these devices so useful can be can be hijacked and used against them.

Recently, two researchers from Rutgers University, Vinod Ganapathy and Liviu Iftode, with support from the National Science Foundation tasked a group of graduate students with an intriguing challenge. Starting with the assumption that they had found a way to hack into a smart phone, the grad students were asked to take a smart phone platform commonly used by software developers and develop malicious applications that a user may not even notice.

Vinod Ganapathy and Liviu Iftode, two researchers from Rutgers University, described the results of their attempts to hack and hijack smart phones in this online media briefing. Credit: National Science Foundation/Rutgers University

The team decided to inject software components known as rootkits into the phone's operating system. Rootkits are a particularly devious threat to a computer, because they attack the operating system itself. Traditional antivirus software, therefore, may not be able to detect them because they don't appear to be stand alone applications or viruses. Most desktop computers are protected from rootkits by something known as virtual machine monitor, but because of their limited size and limited energy resources, smart phones don't deploy these monitors, making it very difficult to know a rootkit attack has taken place.

Once the rootkits were in place, the researchers were able to hijack a smart phone by simply sending it a text message. This allowed them to do things like quietly turn on the device's microphone, enabling them to hear what was going on in the room where the phone had been placed. Another attack trained the phone to use its GPS capabilities to report the phone's exact location without the user's knowledge. By turning on various high-energy functions, the team was even able to rapidly drain the phone's batteries, rendering it useless. The Rutgers team presented the results of their attempts to hack and hijack smart phones at the International Workshop on Mobile Computing Systems and Applications

(HotMobile 2010).

Ganapathy and Liviu say they haven't been approached by the makers of popular smart phone devices, but hopefully their research will help keep these new devices safe and sound.

Provided by National Science Foundation