Femtocell hackers from iSEC hear, see smartphone content

July 16 2013, by Nancy Owano

(Phys.org) —While all thoughts are on how government agencies can abuse surveillance technologies to ruin people's lives, an unassuming group of backyard neighbors in summer clogs and shorts can leisurely lean back in their chairs and snoop to read an SMS that a victim has just sent from her smartphone, listen in on her phone calls, and see all the pictures she is sending off by intercepting the data connection. Better still, they can plant themselves in the financial district and snoop on people talking about accounts, business mergers, or anything else ripe for exploit. Welcome to iSEC's kind of exploit, the talk of the security

crowd this week and no doubt the talk of companies that depend on red flags for potential security holes. The security consultants, iSEC Partners Tom Ritter and Doug DePerry, managed to hack a Verizon Wireless device and turn it into a mobile spy. "This is not about how the NSA would attack ordinary people. This is about how ordinary people would attack ordinary people," said Tom Ritter, a senior consultant with the security firm iSEC Partners.

At play are small cellphone tower used by carriers as network extenders to boost wireless signals indoors, called femtocells, which are available commercially at prices ranging from about $200-250.These are small base stations that can substantially improve indoor voice coverage and data performance. Ritter and DePerry intend to go into detail about the exploit at the upcoming hacking conferences, Black Hat, starting July 27, and Def Con, scheduled for August, in Las Vegas. They intend to use femtocells from Samsung and a $50 antenna from Wilson Electronics for their proof of concept.

These researchers were able to use the femtocell from Verizon to spy on Verizon customers. Whether the smartphone in use was Android or an iPhone made no difference. Text messages and pictures in the message were seen. This was not just any Verizon femtocell; it was a device that they had previously, deliberately, hacked.

Verizon Wireless in its response said, in essence, they fixed it. They updated the software on their signal-boosting devices to prevent hackers from copying the iSEC pair's technique. Verizon Wireless back in March released the Linux software update , in order to thwart any attempts such as Ritter and DePerry had made to compromise the network extenders. They also said there were no reports of any customer impact.

Ritter is not optimistic that this sort of spying technique using femtocells as a potential point of attack cannot happen again. Hackers might find other ways to abuse femtocells, to modify the device and circumvent updates, whether from Verizon or any other carrier offering them to their customers.

More information: via Reuters