Georgia Tech trio to reveal iOS test exploit at Black Hat

June 4 2013, by Nancy Owano

(Phys.org) —Apple's iOS devices such as smartphones are considered relatively secure, so when an Apple customer pays more for an Apple device with iOS there is that reassuring feeling of confidence that the investment is worth it for security sake. Next month at the Black Hat

conference, however, three security researchers from Georgia Tech will show that using chargers to power up iOS devices may be a direct path to insecurity. The three, Billy Lau, Yeongjin Jang, and Chengyu Song, will discuss how their proof of concept charger can hack Apple devices easily, in under a minute—and, we might add, hack devices running the latest version of Apple iOS.

They pushed software onto an iOS device using a charger. They will provide more detail at the Black Hat event conference which takes place in Las Vegas from July 27 to August 1.

Technology-watching sites have already, though, posted the Black Hat web site's overview description of the upcoming talk. The one word that stands out in the summary is "alarming." They wrote that "Apple iOS devices are considered by many to be more secure than other mobile offerings. In evaluating this belief, we investigated the extent to which security threats were considered when performing everyday activities such as charging a device."

That is when the "A" word came in. They said, "The results were alarming: despite the plethora of defense mechanisms in iOS, we successfully injected arbitrary software into current-generation Apple devices running the latest operating system (OS) software."

Their investigation did not need a jailbroken device and it did not need any user interaction.

The charger was built around a single-board computer, the open source BeagleBoard. "We built a proof of concept malicious charger, called Mactans, using a BeagleBoard," they wrote. They chose BeagleBoard to show how easy it was to construct "malicious" USB chargers. BeagleBoard in a single small package can work with the functionality of a laptop. Its roots are in a group of people including several employees

of Texas Instruments who provided a low-cost, fan-less single-board computers based on low-power Texas Instruments processors featuring the ARM Cortex-A series core.

The three pose the question that if they were able to build Mactans in a limited amount of time and with a small budget, what could motivated, better-funded people with bad intentions accomplish?

The authors said they can recommend ways in which users can protect themselves and can suggest security features that Apple can put in place to make attacks by way of chargers more difficult to accomplish.

Andy Greenberg of *Forbes* spoke to one of the Georgia Tech team, Yeongjin Jang, who said that Apple had been contacted about the exploit.

More information: www.forbes.com/sites/andygreen … a-malicious-charger/