Apple pitches gadget security to hacker crowd (Update)

July 26 2012, by Glenn Chapman

Apple pitched security measures in its mobile gadgets on Thursday during its first presentation at a premier gathering of hackers and those intent on thwarting cyber attacks.

Apple pitched security measures in its mobile gadgets on Thursday during its first presentation at a premier gathering of hackers and those intent on thwarting cyber attacks.

The unprecedented talk by Apple head of software platform security Dallas De Atley at the 15th annual Black Hat conference in Las Vegas came as hackers increasingly target smartphones at the heart of Internet Age lifestyles.

"We are really excited to be here," De Atley said before launching into

his presentation at a packed Caesars Palace ballroom.

"When we were developing the iPhone we realized there were aspects that make it different from computers," he continued.

"Security is architecture; you have to build it in from the very beginning. It is not something you can sprinkle over your code when it is done."

De Atley spent an hour providing insights into encryption, software keys and other security features built into the iOS operating system for iPhones, iPads and iPod touch devices.

Hacking attacks on mobile devices, especially Apple gadgets or those powered by Google-backed Android software, were hot topics at Black Hat, where developers voiced doubt that device makers are devoted to security.

Unlike other speakers at the weeklong gathering, De Atley did not field questions from the audience. Instead, he brushed aside queries as he was ushered quickly out a side door after his talk.

His brusque departure underscored a complaint by developers, and those who craft security for Apple gadgets, that they are often left guessing answers to questions when dealing with the revered gadget maker.

"IOS is pretty secret," said Accuvent Labs principal research consultant Charlie Miller, who is credited with the first remote hacker exploit of an iPhone.

"How do they test their software before they ship it?" he continued, rattling off a litany of questions he'd like Apple to answer. "How do they determine an application is malicious and how many times has it happened?"

In the room where De Atley made his presentation, a team from security firm FishNet later announced that in the days ahead it will release a tool designed to expose security problems in applications tailored for Apple gadgets.

"I feel like Apple's security is reactive and not proactive," said Seth Law of FishNet.

"They picked a great base to start from but continually get burned," Law continued. "The fact you can jailbreak an iPhone points to the fact that it is not rock solid."

With Apple boasting of more than 650,000 applications in its online App Store and the addition of more than a thousand a day, an automated way to check third-party software security is needed, according to the FishNet team.

Concerns in applications include whether they intrude on privacy by mining contact lists or other data on devices.

"The process for approving applications (for the App Store) is more about the business decisions than the security aspects," Law said. "Apple's testing in this case is the big unknown."

The list of rules Apple provides developers calls for software to work smoothly on devices but makes no mention of security issues, according to FishNet.

"Developers out there learn to game the system to push their apps through the registration process as fast as possible," Law said. "Apple is looking at how to best enforce their rules and make their money; they want their 30 percent cut."

Cupertino, California-based Apple gets 30 percent of the money from sales of virtual goods or subscriptions in applications on its globally popular devices.

(c) 2012 AFP