Grant awarded to improve the security of mobile devices and cellular networks

November 10 2009

With a new grant, Georgia Tech computer scientists Jonathon Giffin (left) and Patrick Traynor are developing cell phone remote repair methods, which will allow service providers to assist in cleaning infected devices. Credit: Georgia Tech Photo: Gary Meek

Smart phones -- like BlackBerrys and iPhones -- have become indispensable to today's highly mobile workforce and tech-savvy youngsters. While these devices keep friends and colleagues just a few thumb-taps away, they also pose new security and privacy risks.

"Traditional cell phones have been ignored by attackers because they were specialty devices, but the new phones available today are handheld

computers that are able to send and receive e-mail, surf the Internet, store documents and remotely access data -- all actions that make them vulnerable to a wide range of attacks," said Patrick Traynor, assistant professor in the School of Computer Science at the Georgia Institute of Technology.

Traynor and Jonathon Giffin, also an assistant professor in the School of Computer Science, recently received a three-year $450,000 grant from the National Science Foundation to develop tools that improve the security of mobile devices and the telecommunications networks on which they operate. These Georgia Tech faculty, together with a team of graduate students, are developing methods of identifying and remotely repairing mobile devices that may be infected with viruses or other malware.

Malware can potentially eavesdrop on user input or otherwise steal sensitive information, destroy stored information, or disable a device. Attackers may snoop on passwords for online accounts, electronic documents, e-mails that discuss sensitive topics, calendar and phonebook entries, and audio and video media.

"Since mobile phones typically lack security features found on desktop computers, such as antivirus software, we need to accept that the mobile devices will ultimately be successfully attacked. Therefore our research focus is to develop effective attack recovery strategies," explained Giffin.

The researchers plan to investigate whether cellular service providers -- such as AT&T and Verizon Wireless -- are capable of detecting infected devices on their respective networks. Since infected devices often begin to over-utilize the network by sending a high volume of traffic to a known malicious Internet server or by suddenly generating a high volume of text messages, monitoring traffic patterns on the network

should allow these infected phones to be located, according to the researchers.

"While a single user might realize that a phone is behaving differently, that person probably won't know why. But a cell phone provider may see a thousand devices behaving in the same way and have the ability to do something about it," said Traynor.

Once infected devices are located, those phones will need to be cleared of the malicious code. To accomplish this, the researchers are developing remote repair methods, which will allow service providers to assist in the cleaning of infected devices without requiring that the phones be brought to a service center. The methods will also have to work without much effort on the part of the customer.

This repair may require disabling some functionality on the phone, such as the ability to use downloaded programs, until the malicious program is located and removed. While the repair is underway, phone calling and text messaging functionality would continue to operate.

"Using this remote repair strategy, the service provider no longer has to completely disable a phone. Instead they just put the device into a safe, but reduced, mode until the malware can be removed," said Giffin.

To assess their proposed methods of finding and repairing infected mobile devices, the researchers plan to build a cellular network test bed at Georgia Tech that will simulate how cellular devices communicate over a network.

"We hope that developing these attack recovery strategies will let potential mobile phone and network attackers know that these response mechanisms are in place, ultimately making their attacks far less widespread or successful," said Traynor.

Source: Georgia Institute of Technology