Researchers show new security threat against 'smart phone' users

February 22 2010

Rutgers computer science graduate student Jeffrey Bickford with smart phone used to test malicious "rootkit" software, which attacks the phone's operating system. Researchers showed how rootkits could cause a smart phone to eavesdrop on a meeting, track its owner's travels, or rapidly drain its battery to render the phone useless. Credit: Carl Blesch

Computer scientists at Rutgers University have shown how a familiar type of personal computer security threat can now attack new generations of smart mobile phones, with the potential to cause more serious consequences.

The researchers, who are presenting their findings at a mobile computing workshop this week in Maryland, demonstrated how such a software attack could cause a smart phone to eavesdrop on a meeting, track its owner's travels, or rapidly drain its battery to render the phone useless. These actions could happen without the owner being aware of what happened or what caused them.

"Smart phones are essentially becoming regular computers," said Vinod Ganapathy, assistant professor of computer science in Rutgers' School of Arts and Sciences. "They run the same class of operating systems as desktop and laptop computers, so they are just as vulnerable to attack by malicious software, or 'malware.'"

Smart phones are cellular telephones that also offer Internet accessibility, texting and e-mail capabilities and a variety of programs commonly called "apps," or applications.

Ganapathy and computer science professor Liviu Iftode worked with three students to study a nefarious type of malware known as "rootkits." Unlike viruses, rootkits attack the heart of a computer's software - its operating system. They can only be detected from outside a corrupted operating system with a specialized tool known as a virtual machine monitor, which can examine every system operation and data structure.

Virtual machine monitors exist for desktop computers, but in current form, they demand more processing resources and energy than a portable phone can currently support.

Rootkit attacks on smart phones or upcoming tablet computers could be more devastating because smart phone owners tend to carry their phones with them all the time. This creates opportunities for potential attackers to eavesdrop, extract personal information from phone directories, or just pinpoint a user's whereabouts by querying the phone's Global

Positioning System (GPS) receiver. Smart phones also have new ways for malware to enter the system, such as through a Bluetooth radio channel or via text message.

"What we're doing today is raising a warning flag," Iftode said. "We're showing that people with general computer proficiency can create rootkit malware for smart phones. The next step is to work on defenses."

In one test, the researchers showed how a rootkit could turn on a phone's microphone without the owner knowing it happened. In such a case, an attacker would send an invisible text message to the infected phone telling it to place a call and turn on the microphone, such as when the phone's owner is in a meeting and the attacker wants to eavesdrop.

In another test, they demonstrated a rootkit that responds to a text query for the phone's location as furnished by its GPS receiver. This would enable an attacker to track the owner's whereabouts. Finally, they showed a rootkit turning on power-hungry capabilities, such as the Bluetooth radio and GPS receiver to quickly drain the battery. An owner expecting remaining battery life would instead find the phone dead.

The researchers are careful to note that they did not assess how vulnerable specific types of smart phones are. They did their work on a phone used primarily by software developers versus commercial phone users. Working within a legitimate software development environment, they deliberately inserted rootkit malware into the phone to study its potential effects. They did not find a vulnerability that a real malware attacker would have to exploit.

The research team is presenting its findings at the International Workshop on Mobile Computing Systems and Applications (HotMobile 2010). Working with Ganapathy and Iftode were Jeffrey Bickford and Ryan O'Hare, who worked on the project as undergraduates, and Arati

Baliga, who worked on it as a postdoctoral researcher. The research was supported by the National Science Foundation and the U.S. Army.

Provided by Rutgers University

Citation: Researchers show new security threat against 'smart phone' users (2010, February 22) retrieved 25 April 2024 from https://phys.org/news/2010-02-threat-smart-users.html