PHYS.ORG

U r pwned: text messaging paves way for hacking

July 30 2009, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Getting a text message is akin to someone sliding a piece of mail under your door: You may not have asked for it, you can't stop its delivery and you have to deal with it whether you want to or not.

The fact that text messages appear on mobile phones without any interaction from the user, and sometimes with limited interference from the cellular network operators, can give criminals an opening to break into those devices, as three teams of researchers showed Thursday at the Black Hat security conference here.

Their targets ran the gamut.

Apple Inc.'s iPhones and phones running Microsoft Corp.'s Windows Mobile and Google Inc.'s Android operating systems were all shown to be vulnerable. In some cases, the problems weren't with software, but the way cellular networks process messages.

The findings are troubling as people increasingly use their phones for handling sensitive data, like e-mail and online banking.

Phones are morphing into mini-computers, which means they're going to start getting attacked like PCs.

In some respects, phones are relatively safer. Cellular carriers control their networks more tightly than anyone controls the Internet, so they're in a better position to stop new types of attacks that crop up.

Telling the difference between harmful and legitimate traffic can be tricky, though. And anonymity still is possible given the proliferation of prepaid plans that don't require long-term contracts; a carrier can trace an attack to a particular phone but not necessarily to a particular person.

The techniques demonstrated Thursday show that even disciplined and safety-conscious users could have their phones hacked because they can't totally control what's coming into them.

Innocent people could have their smart phones knocked offline, commanded to visit sites hosting pornography or viruses, or even turned into remote-controlled subordinates of a criminal gang behind an attack.

Take this example about the iPhone, from Charlie Miller, a well-known hacker of Apple Inc. and other products, and his co-presenter Collin Mulliner, a Ph.D. student in telecommunications security at the Technical University of Berlin.

They showed how they can disconnect an iPhone from the cellular network by sending it a single, maliciously crafted text message - a message the victim never sees. The messages exploit bugs in the way iPhones handle certain messages and are used to crash parts of the software.

They even said it's possible to remotely control an iPhone by sending 500 messages to a single victim's phone. Those messages contain the necessary commands for the attack and would get executed automatically by exploiting a weakness in the way the iPhone's memory responds to that volume of traffic.

Miller said messaging attacks are so attractive, and are going to become more common, because the underlying technology is a core phone feature that can't be turned off.

"It's such a powerful attack vector," Miller said. "All I need to know is your phone number. As long as their phone's on, I can send this and their phone's going to do something with this. ... It's always on, it's always there, the user doesn't have to do anything - it's the perfect attack vector."

Miller and Mulliner also found problems in phones running Android (that problem has been fixed) and Windows Mobile (they say that problem hasn't been fixed yet).

Apple said it couldn't immediately comment. Microsoft said it is investigating the matter. Google confirmed that its vulnerability was fixed.

Sometimes the culprit isn't a software flaw but the way the phones were configured at the factory to handle messaging traffic. Hackers can break in if the phones are too permissive in what types of traffic they accept.

John Hering and Kevin Mahaffey, co-founders of Flexilis Inc., and Anthony Lineberry, a senior software engineer with the Los Angeles-based mobile security firm, made browser screens pop up and direct victims to any page of their choosing by sending specially crafted messages to phones made by Taiwan-based HTC Corp. and sold under major carriers' brand names.

The user never sees a text message pop up; the mobile Web browser suddenly springs to life and navigates to a page the user didn't ask for.

The researchers said spammers have latched onto this type of attack in Europe and Asia.

They said the problem they found wasn't in the Windows Mobile software on the devices, but rather in the way the manufacturer configured software settings on some phones, allowing anyone to send certain messaging commands to them.

A call to HTC's North American headquarters wasn't returned Thursday.

The carriers play a critical role in stopping these types of attacks.

Because they have a stranglehold on what comes in and out of their networks, they can stop malicious traffic from ever hitting a user's cell phone by filtering out types of traffic that attackers shouldn't be able to send. Hackers are able to game the system when they're allowed to push commands that only the carrier should be allowed to send.

That was the theme of a talk by Zane Lackey, senior security consultant with San Francisco-based iSEC Partners Inc., and Luis Miras, an independent security researcher.

They showed how they can trick a cell phone into pulling in content from a computer under their control. The content never passes through the cellular carrier's security gauntlet as it's supposed to.

The hack works because Lackey and Miras figured out how to attach a "notification" alert - something they said only the carrier should be allowed to send - to administrative messages they sent through an unidentified carrier's network.

The alert tells victims they have a message, such as one instructing them to update settings. To the recipient's phone, it looks the same as a notice sent by the carrier.

If the user chooses to update the device, the phone then reaches out for the content - on computers under a hacker's control.

"The way carriers built their networks, there were a lot of security assumptions based on the idea that only the carrier would be able to send certain messages," Lackey said. "Those assumptions are invalid."

The flip side to the dangers the researchers have uncovered in mobile devices is that they're often able to write programs to help companies and individual users look for vulnerabilities in their devices. That could protect against future attacks.

Citation: U r pwned: text messaging paves way for hacking (2009, July 30) retrieved 11 May 2024 from https://phys.org/news/2009-07-pwned-text-messaging-paves-hacking.html