



From: www.csoonline.com

3 Simple Steps to Hack a Smartphone (Includes Video)

Security firm Trust Digital demonstrates how easy it is to steal data and push nasty stuff to a mobile device with nothing more than a phone number

by Joan Goodchild, Senior Editor, CSO

April 29, 2009

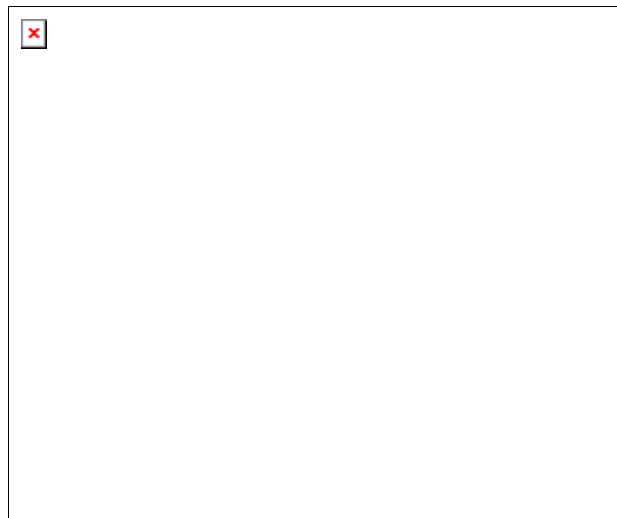
What kind of information do you have on your business card? Company name? Check. Your name and title? Check. Business address? Check. Mobile work phone number? Wait a minute.

CSO recently sat down with Trust Digital, a firm that specializes in mobile security, for a demonstration on how to hack a smartphone with no more information than a phone number.

"All I need is a business card," said Meir Machlin, director of product architecture with Trust Digital, who performed the demonstration (You can check out the demonstrations in the video).

How to Hack a Smartphone

Meir Machlin of Trust Digital demonstrates how to hack a smartphone using SMS.



Machlin walked us through two hacks using basic tools available to anyone. Machlin's 'hacker tool kit' included a laptop with WiFi connectivity, and two phones. One phone acts as a GSM modem for the laptop, the other phone is Machlin's personal phone, which he used to receive information. A third phone served as our target device, the phone that was 'under attack' in the demonstration.

The first attack we watched is known as a 'Midnight Raid,' because it is often pulled off during the night when the phone's user is asleep and the device is still turned on as it is charged, or simply left on the nightstand.

Machlin sent a simple SMS which invoked Internet Explorer on the attack device. First, Machlin sent a graphic to the target phone that said "You have been hacked" to show just how quick and easy it is to get into another user's phone with SMS. In the second push, Machlin ran an application on the attacked phone that could retrieve data. The SMS came back to Machlin's phone with the attack phone's INSI number; the phone's unique ID. However, Machlin noted the application could have just as easily have stolen a contact list, either personal or corporate. He said it was also possible in this scenario to push viruses to the device or even initiate a denial of service attack.

How to Hack a Smartphone, Part 2

Meir Machlin of Trust Digital continues his demonstration of how to hack a smartphone.



In the second demonstration (which you can view in "How to Hack a Smartphone, Part 2"), Machlin ran through a control message attack. In this kind of hack, a criminal can change the control settings of a device without the user having any knowledge. He showed us how he could easily uncheck SSL, leaving the device vulnerable with no encryption. As a finale, he pushed a wipe command, which removed all stored information from the device. The wipe, said Machlin, could also be pushed to all devices contained in a hacked phone's contact list.

The attacks, according to Machlin, prove that texts can no longer be considered safe. And these kinds of hacks are unique to smartphones because PCs don't have SMS capabilities, he said.

Which smartphones are vulnerable to these kinds of attacks? That varies widely depending on the security settings and practices in place for use of the device. Some contend that mobile devices still pose little security threat to an organization. In fact, in a recent [hacking "contest" that took place in March](#), none of the smartphones slated for attack were compromised. However, a [report from Gartner analyst John Girard](#) predicts as wireless devices become more pervasive in the enterprise, the potential for security problems will increase.

Machlin advised all smartphones that are under an organization's control be tightly monitored, patched and updated regularly to avoid users taking matters in their own hands (See also: [The Top 5 Stupid Things That People Do with Mobile Phones](#)).

"The IT guys need to control the phones and secure them. They need to always be ahead (of the threats) and push the right patches to the population."

© CXO Media Inc.