PHYS ORG

# Study shows side-channel phone risk via microphone and camera

November 12 2013, by Nancy Owano

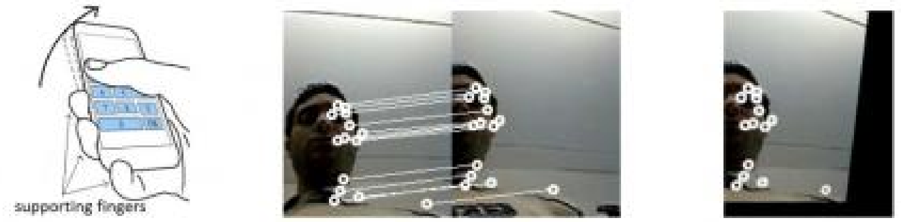

Figure 7: Supporting fingers push the phone upwards to touch a digit. Figure 8: Key points of OK-button frame (left) and digit #1 frame (right). Figure 9: Image of OK-button frame by Homography.

Credit: 'PIN Skimmer: Inferring PINs Through The Camera and Microphone' by Laurent Simon, Ross Anderson

(Phys.org) —Researchers exploring smartphone security vulnerabilities are increasingly turning to information about smartphone sensors as pathways to security breach. Earlier this year, a Stanford University team warned that sensors such as accelerometers could identify a device and track it. In 2012, a paper titled "Practicality of Accelerometer Side Channels on Smartphones" by researchers from the University of Pennsylvania reported that by analyzing data gathered by accelerometers they were able to get a good idea of the PIN or pattern used to protect a phone. Now a study by two researchers at Cambridge University set out to show that a smartphone PIN can be identified via the smartphone camera and microphone. Smartphone rsearchers Ross Anderson, Professor of Security Engineering at the Computer Laboratory at the University of Cambridge and Laurent Simon, also of the Computer

Laboratory, demonstrated an attack that can reveal the PIN codes for sensitive apps, such as those for banking, by tapping into the microphone and camera.. They wrote about their finding in the paper, "PIN Skimmer: Inferring PINs Through the Camera and Microphone." Their study was presented at a recent workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) in Berlin.

"In this paper," they wrote, "we aim to raise awareness of side-channel attacks even when strong isolation protects sensitive applications. Previous works have studied the use of the phone accelerometer and gyroscope as side channel data to infer PINs. Here, we describe a new side-channel attack that makes use of the video camera and microphone to infer PINs entered on a number-only soft key-board on a smartphone."

Their attack was achieved through a program called PIN Skimmer. They found that codes entered on a number-only soft keypad could be identified. Their feat involves software that watches the smartphone user's face by means of the camera and listens to clicks through the microphone as the victim types. The microphone can detect touch as a user enters the PIN, taking in the clicks made by the smartphone from the user pressing on the virtual number keys. The camera estimates the orientation of the phone as the user is doing this and correlates it to the position of the user-tapped digit.

Writing about their work in the security weblog "Light Blue Touchpaper," Ross Anderson said, "We found that software on your smartphone can work out what PIN you're entering by watching your face through the camera and listening for the clicks as you type. Previous researchers had shown how to work out PINs using the gyro and accelerometer; we found that the camera works about as well. We watch how your face appears to move as you jiggle your phone by typing."

The paper reported these results: When selecting from a test set of 50 four-digit PINs, PIN Skimmer correctly infers more than 30 percent of PINs after two attempts, and more than 50 percent of PINs after five attempts on Android-powered phones. When selecting from a set of 200 eight-digit PINs, PIN Skimmer correctly infers about 45 percent of the PINs after five attempts and 60 percent after 10 attempts.

The authors reserved a special section in the paper where they presented possible countermeasures to mitigate side-channel attacks on PIN input. Blogged Anderson: "Meanwhile, if you're developing payment apps, you'd better be aware that these risks exist."

© 2013 Phys.org

Citation: Study shows side-channel phone risk via microphone and camera (2013, November 12) retrieved 25 April 2024 from
https://phys.org/news/2013-11-side-channel-microphone-camera.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.