A Picture is Worth a Thousand Locksmiths, Computer Scientists Say

October 29 2008

Scenes from one of the proof-of-concept telephoto experiments using a new software program from UC San Diego that can perform key duplication without having the key. Instead, the computer scientists only need a photograph of the key. Credit: UC San Diego Jacobs School of Engineering

(PhysOrg.com) -- UC San Diego computer scientists have built a software program that can perform key duplication without having the key. Instead, the computer scientists only need a photograph of the key.

"We built our key duplication software system to show people that their keys are not inherently secret," said Stefan Savage, the computer science professor from UC San Diego's Jacobs School of Engineering who led the student-run project. "Perhaps this was once a reasonable assumption, but advances in digital imaging and optics have made it easy to duplicate someone's keys from a distance without them even noticing."

Professor Savage presents this work on October 30 at ACM's Conference on Communications and Computer Security (CCS) 2008, one of the premier academic computer security conferences.

The bumps and valleys on your house or office keys represent a numeric code that completely describes how to open your particular lock. If a key doesn't encode this precise "bitting code," then it won't open your door.

In one demonstration of the new software system, the computer scientists took pictures of common residential house keys with a cell phone camera, fed the image into their software which then produced the information needed to create identical copies. In another example, they used a five inch telephoto lens to capture images from the roof of a campus building and duplicate keys sitting on a café table more than 200 feet away.

"This idea should come as little surprise to locksmiths or lock vendors," said Savage. "There are experts who have been able to copy keys by hand from high-resolution photographs for some time. However, we argue that the threat has turned a corner—cheap image sensors have made digital cameras pervasive and basic computer vision techniques can automatically extract a key's information without requiring any expertise."

Professor Savage notes, however, that the idea that one's keys are sensitive visual information is not widely appreciated in the general public.

"If you go onto a photo-sharing site such as Flickr, you will find many photos of people's keys that can be used to easily make duplicates. While people generally blur out the numbers on their credit cards and driver's licenses before putting those photos on-line, they don't realize that they should take the same precautions with their keys" said Savage.

As for what to do about the key duplication threat, Savage says that companies are actively developing and marketing new locking systems that encode electromagnetic secrets as well as a physical code. "Many car keys, for example, have RFID immobilizer chips that prevent duplicated keys from turning the car on." he says. In the meantime, he suggests that you treat your keys like you treat your credit card, "Keep it in your pocket unless you need to use it."

How it works

The keys used in the most common residential locks in the United States have a series of 5 or 6 cuts, spaced out at regular intervals. The computer scientists created a program in MatLab that can process photos of keys from nearly any angle and measure the depth of each cut. String together the depth of each cut and you have a key's bitting code, which together with basic information on the brand and type of key you have, is what you need to make a duplicate key.

The chief challenge for the software system, called "Sneakey," is to adjust for a wide range of different angles and distances between the camera and the key being captured. To do so, the researchers relied on a classic computer vision technique for normalizing an object's orientation and size in three dimensions by matching control points from a reference image to equivalent points in the target image.

"The program is simple. You have to click on the photo to tell it where the top of the key is, and a few other control points. From here, it normalizes the key's size and position. Since each pixel then corresponds to a set distance, it can accurately guess the height of each of the key cuts," explained Benjamin Laxton, the first author on the paper who recently earned his Master's degree in computer science from UC San Diego.

The researchers have not released their code to the public, but they acknowledge that it would not be terribly difficult for someone with basic knowledge of MatLab and computer vision techniques to build a similar system.

"Technology trends in computer vision are at a point where we need to consider new risks for physical security systems," said Kai Wang, a UC San Diego computer science graduate student and author on the new paper. Wang is a computer vision researcher working on the creating systems capable of reading text on product packaging. This is part of a larger project on creating a computerized personal shopping assistant for the visually impaired from the lab of computer science professor Serge Belongie.

As a computer security expert, Savage said he particularly enjoyed working on a project with computer vision students.

"UC San Diego is very supportive of interdisciplinary work. There are many opportunities for students and faculty to get their hands dirty in fields they may not know much about a lot at first," said Savage.

Provided by University of California - San Diego