Your smartphone's next trick? Fighting cybercrime.

www.buffalo.edu/news/releases/2017/12/013.html

Each device, regardless of the manufacturer or make, can be identified through a pattern of microscopic imaging flaws that are present in every picture they take. Credit: Douglas Levere.

Like bullets fired from a gun, photos can be traced to individual smartphones, opening up new ways to prevent identity theft

BUFFALO, N.Y. — Not comfortable with Face ID and other biometrics? This cybersecurity advancement may be for you.

A University at Buffalo-led team of researchers has discovered how to identify smartphones by examining just one photo taken by the device. The advancement opens the possibility of using smartphones — instead of body parts — as a form of identification to deter cybercrime.

"Like snowflakes, no two smartphones are the same. Each device, regardless of the manufacturer or make, can be identified through a pattern of microscopic imaging flaws that are present in every picture they take," says Kui Ren, the study's lead author. "It's kind of like matching bullets to a gun, only we're matching photos to a smartphone camera."

The new technology, to be presented in February at the 2018 Network and Distributed Systems Security Conference in California, is not yet available to the public. However, it could become part of the authentication process — like PIN numbers and passwords — that customers complete at cash registers, ATMs and during online transactions.

For people who've had their personal identification stolen, it could also help prevent cybercriminals from using that information to make purchases in their name, says Ren, PhD, SUNY Empire Innovation Professor in the Department of Computer Science and Engineering in UB's School of Engineering and Applied Sciences.

How each camera is unique

The study — "ABC: Enabling Smartphone Authentication with Built-in Camera" — centers on an obscure flaw in digital imaging called photo-response non-uniformity (PRNU).

Digital cameras are built to be identical. However, manufacturing imperfections create tiny variations in each camera's sensors. These variations can cause some of sensors' millions of pixels to project colors that are slightly brighter or darker than they should be.

Not visible to the naked eye, this lack of uniformity forms a systemic distortion in the photo called pattern noise. Extracted by special filters, the pattern is unique for each camera.

First observed in conventional digital cameras, PRNU analysis is common in digital forensic science. For example, it can help settle copyright lawsuits involving photographs.

But it hasn't been applied to cybersecurity — despite the ubiquity of smartphones — because extracting it had required analyzing 50 photos taken by a camera, and experts though that customers wouldn't be willing to supply that many photos. Plus, savvy cybercriminals can fake the pattern by analyzing images taken with a smartphone that victims post on unsecured websites.

Applying the technique to cybersecurity

The study addresses how each of these challenges can be overcome.

Compared to a conventional digital camera, the image sensor of a smartphone is much smaller. The reduction amplifies the pixels' dimensional non-uniformity and generates a much stronger PRNU. As a result, it's possible to match a photo to a smartphone camera using one photo instead of the 50 normally required for digital forensics.

"I think most people assumed you would need 50 images to identify a smartphone camera. But our research shows that's not the case," says Ren, an IEEE (Institute of Electrical and Electronics Engineers) Fellow and an ACM (Association for Computing Machinery) Distinguished Scientist.

To prevent forgeries, Ren designed a protocol — it is part of the authentication process described below — which detects and stops two types of attacks.

How the new security protocol works

The study discusses how such a system might work. First, a customer registers with a business — such as a bank or retailer — and provides that business with a photo that serves as a reference.

When a customer initiates a transaction, the retailer asks the customer (likely through an app) to photograph two QR codes (a type of barcode that contains information about the transaction) presented on an ATM, cash register or other screen.

Using the app, the customer then sends the photograph back to the retailer, which scans the picture to measure the smartphone's PRNU. The retailer can detect a forgery because the PRNU of the attacker's camera will alter the PRNU component of the photograph.

More savvy cybercriminals could potentially remove the PRNU from their device. But Ren's protocol can spot this because the QR codes include an embedded probe signal that will be weakened by the removal process.

The transaction is either approved or denied based upon these tests.

Results and what's next

The protocol defeats three of the most common tactics used by cybercriminals: fingerprint forgery attacks, man-in-the-middle attacks and replay attacks. It was 99.5 percent accurate in tests involving 16,000 images and 30 different iPhone 6s smartphones and 10 different

Galaxy Note 5s smartphones.

Ren plans to lead future experiments on smartphones that include two cameras, which he said could be used to make the forgery attacks more difficult.

In addition to Ren, co-authors include Zhongjie Ba (UB), Sixu Piao (UB), Dimitrios Koutsonikolas (UB), Aziz Mohaisen (formerly of UB, and now of the University of Central Florida), and Xinwen Fu (University of Central Florida).