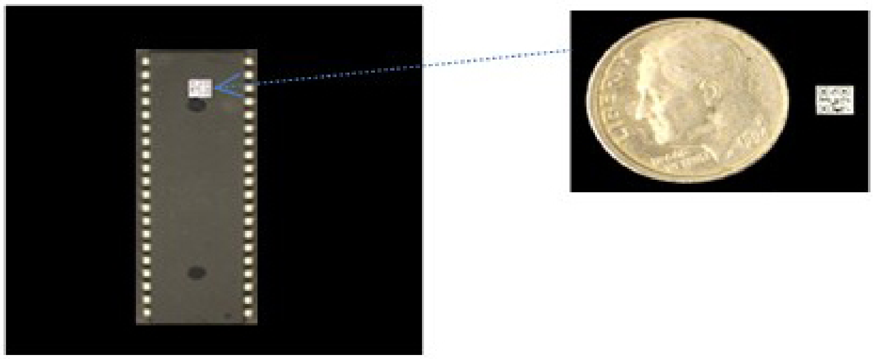
PHYS.ORG

QR codes engineered into cybersecurity protection

February 27 2015, by Colin Poitras



A 3.15 mm QR code storing an encrypted and compressed image shown placed on an integrated circuit and an image of the QR code placed next to a dime. Credit: Adam Markman/Brhram Javidi

QR, or Quick Response, codes – those commonly black and white boxes that people scan with a smartphone to learn more about something – have been used to convey information about everything from cereals to cars and new homes.

But, University of Connecticut (UConn) researchers think the codes have a greater potential: protecting national security.

Using advanced 3-D optical imaging and extremely low light photon counting encryption, Board of Trustees Distinguished Professor Bahram Javidi and his research team have taken the ordinary QR code and transformed it into a high-end cybersecurity application that can be used to protect the integrity of computer microchips. The findings were published in IEEE Photonics Journal.

"An optical code or QR code can be manufactured in such a way that it is very difficult to duplicate," said Javidi, whose team is part of UConn's Center for Hardware Assurance, Security, and Engineering (CHASE) in the School of Engineering. "But if you have the right keys, not only can you authenticate the chip, but you can also learn detailed information about the chip and what its specifications are.

"And, that is important to the person using it."

Corrupted and recycled integrated circuits or microchips posed a significant threat to the international electronics supply chain. Bogus or used computer chips may not matter much when they cause poor cell phone reception or an occasional laptop computer crash in personal use. But the problem becomes exponentially more serious when counterfeit or hacked chips turn up in the U.S. military.

The problem has been exacerbated in recent years by the fact that much of the national production of microcircuits has moved offshore, where prices are lower but ensuring quality control is more difficult.

In 2012, a Senate Armed Services Committee report found that more than 100 cases of suspected counterfeit electronics parts from China had made their way into the Department of Defense supply chain. In one notable example, officials said counterfeit circuits were used in a high-altitude missile meant to destroy incoming missiles. Fixing the problem cost the government $2.675 million, the report said.

Unlike commercial QR codes, Javidi's little black and white boxes can be scaled as small as microns or a few millimeters and would replace the electronic part number that is currently stamped on most microchips.

Javidi says he can compress vital information about a chip – its functionality, capacity, and part number – directly into the QR code so it can be obtained by the reader without accessing the Internet. This is important in cybersecurity circles, because linking to the Internet greatly increases vulnerability to hacking or corruption.

To further protect the information in the QR code, Javidi applies an optical imaging "mask" that scrambles the QR code design into a random mass of black-and-white pixels that look similar to the snowy images one might see on a broken TV. He then adds yet another layer of security through a random phase photon-based encryption that turns the snowy image into a darkened nighttime sky with just a few random stars or dots of pixilated light.

The end result is a self-contained, highly secure, information-laden microscopic design that is nearly impossible to duplicate. Only individuals who have the special corresponding codes could decrypt the QR image.

And that is important to all of us.

Rising awareness about cybersecurity

Given the fact that the most common passwords for computer users are not secure at all – "password" and "12345" – cybersecurity is an issue that should be a concern to even the personal user.

That was the message recently conveyed by a panel of cybersecurity experts hosted by the Center of Excellence for Security Innovation (CSI), a collaboration between UConn School of Engineering and Comcast.

Donna Dodson, chief cybersecurity advisor for the National Institute of Standards and Technology (NIST), told the audience at Wilbur Cross that getting individuals as well as companies to think about cybersecurity is the first step toward a more secure network.

"I may not understand the mechanics of my car, but I know it's my responsibility to keep it safe," said Dodson, the featured speaker at the event.

Toward that end, the NIST wrote a guidebook for the public, titled "Framework for Improving Critical Infrastructure Cybersecurity," which provides a "common language" for people. "It promotes concepts of resiliency and protecting your environment," Dodson said.

UConn's Mark Tehranipoor, director of CSI, said raising awareness about cybersecurity concerns should begin early. "We really have to take it down to the undergraduate level and even bring it down to high school level."

It was a sentiment reiterated by Liam Randall of Critical Stack, an Ohio-based company that specializes in network security. For every person working on preventing attacks, he said, someone else is working on new ways to carry out such attacks.

"When you look at the impact that one person can have, that really keeps me up at night," he said.

Based on the panel discussion, the impact of a single person can apply to the common user as well as the hacker.

Provided by University of Connecticut

Citation: QR codes engineered into cybersecurity protection (2015, February 27) retrieved 20 April 2024 from https://phys.org/news/2015-02-qr-codes-cybersecurity.html