Biometric expert shows an easy way to spoof fingerprint scanning devices

December 11 2005

Eyeballs, a severed hand or fingers carried in ziplock bags. Back alley eye replacement surgery. These are scenarios used in recent blockbuster movies like Steven Spielberg's "Minority Report" and "Tomorrow Never Dies" to illustrate how unsavory characters in high-tech worlds beat sophisticated security and identification systems.

Photo: Clarkson University Associate Professor of Electrical and Computer Engineering Stephanie C. Schuckers, with imitation fingers. Simple casts made from a mold and material such as Play-doh, clay or gelatin can be used to fool most fingerprint recognition devices. Schuckers, an expert in biometrics, the science of using biological properties, such as

fingerprints or voice recognition, to identify individuals, is a partner in a $3.1 million interdisciplinary biometrics research project funded by the NSF with support from the Department of Homeland Security.

Sounds fantastic? Maybe not. Biometrics is the science of using biological properties, such as fingerprints, an iris scan, or voice recognition, to identify individuals. And in a world of growing terrorism concerns and increasing security measures, the field of biometrics is rapidly expanding.

“Biometric systems automatically measure the unique physiological or behavioral 'signature’ of an individual, from which a decision can be made to either authenticate or determine that individual’s identity, ” explained Stephanie C. Schuckers, an associate professor of electrical and computer engineering at Clarkson University. “Today, biometric systems are popping up everywhere – in places like hospitals, banks, even college residence halls – to authorize or deny access to medical files, financial accounts, or restricted or private areas.”

“And as with any identification or security system, ” Schuckers adds, “biometric devices are prone to 'spoofing’ or attacks designed to defeat them.”

Spoofing is the process by which individuals overcome a system through an introduction of a fake sample. “Digits from cadavers and fake fingers molded from plastic, or even something as simple as Play-Doh or gelatin, can potentially be misread as authentic, ” she explains. “My research addresses these deficiencies and investigates ways to design effective safeguards and vulnerability countermeasures. The goal is to make the authentication process as accurate and reliable as possible.”

Schuckers’ biometric research is funded by the National Science Foundation (NSF), the Office of Homeland Security and the Department

of Defense. She is currently assessing spoofing vulnerability in fingerprint scanners and designing methods to correct for these as part of a $3.1 million interdisciplinary research project funded through the NSF. The project, “ITR: Biometrics: Performance, Security and Societal Impact, ” investigates the technical, legal and privacy issues raised from broader applications of biometric system technology in airport security, computer access, or immigration. It is a joint initiative among researchers from Clarkson, West Virginia University, Michigan State University, St. Lawrence University, and the University of Pittsburgh.

Fingerprint scanning devices often use basic technology, such as an optical camera that take pictures of fingerprints which are then “read” by a computer. In order to assess how vulnerable the scanners are to spoofing, Schuckers and her research team made casts from live fingers using dental materials and used Play-Doh to create molds. They also assembled a collection of cadaver fingers.

In the laboratory, the researchers then systematically tested more than 60 of the faked samples. The results were a 90 percent false verification rate.

“The machines could not distinguish between a live sample and a fake one, ” Schuckers explained. “Since liveness detection is based on the recognition of physiological activities as signs of life, we hypothesized that fingerprint images from live fingers would show a specific changing moisture pattern due to perspiration but cadaver and spoof fingerprint images would not.”

In live fingers, perspiration starts around the pore, and spreads along the ridges, creating a distinct signature of the process. Schuckers and her research team designed a computer algorithm that would detect this pattern when reading a fingerprint image. With the new detection system integrated into the device, less than 10 percent of the spoofed samples

were able to fool the machine.

Addressing potential problems before they can occur is one of the goals of Schuckers' biometrics research. "As security systems based on biometrics continue to develop, it is important that people are reassured that their privacy is protected, " she said. "How confident will someone feel giving his/her fingerprint over a public communication channel, such as the Internet? The technology needs to be solid and reliable and offer adequate privacy protection before biometric security systems will be accepted by the public."

Schuckers is also a member of the Center for Identification Technology, a cooperative research center headquartered at West Virginia University that brings together the NSF, industry and government agencies, and university researchers. She is director of the Biomedical Signal Analysis Laboratory at Clarkson. Schuckers joined the faculty of Clarkson in 2002. She received her doctoral degree in electrical engineering from the University of Michigan in 1997.

Source: Clarkson University