PCWORLD.COM
TECHNOLOGY ADVICE YOU CAN TRUST

Biometric Security Barely Skin-Deep

Recordings and even gummy bears can hack through biometric devices, security expert tells BlackHat crowd.

Andrew Brandt, PCWorld.com
Thursday, August 01, 2002

LAS VEGAS -- With just $10 in materials and less than an hour to complete his work, a Japanese researcher molded fake fingerprints that could overwhelmingly deceive biometric thumb scanners, a security technology expert reported at the BlackHat Briefings conference here.

It was just one of several failures in biometric technology related by Rick Smith, who has worked in federal research programs on information security and cyberdefense, including a project for the National Security Agency. He addressed a rapt audience of security business professionals, white-hat hackers, and government spy agency representatives gathered for the week-long conference.

Smith described several ways the most common types of biometric identification devices--iris scanners, face and voice recognition systems, and thumbprint readers--could be fooled. Biometrics, the science of identifying a person by reading their unique body features, have been much touted as a way to strengthen domestic security at places ranging from supermarkets to nuclear power stations.

No Panacea

"Biometrics aren't secrets, they're properties of your body that you slough off all day long, when you're eating lunch, or driving your car, or opening the door," Smith said. As a result, each of us leaves a trail of biometric signatures everywhere we go, creating many chances for theft of biometric information.

Part of the problem is people's desire to rely too heavily on biometrics as a security mechanism, while passwords remain too easy to guess, Smith said. Biometrics aren't a replacement for passwords, but an enhancement, he said.

"Any passwords that we can memorize are probably too easy to guess anyway and aren't worth using," Smith said. "That's why I like biometric-enhanced tokens, like those little USB storage keys, where the real authorization is based on a secret embedded in the token, and the biometric serves as a PIN to the token."

Requiring a biometric record, such as a thumbprint, as well as a PIN number at an ATM could improve bank security, for example. But simply changing a PIN to a biometric record does not--and could worsen security, he said.

Each type of existing biometric technology provides myriad low-tech vulnerabilities that can be exploited by people who want to defeat the system, according to Smith.

Busting Biometrics

The most damning criticism came from researchers: one set from Germany, and another at the International Telecommunication Union, a global industry standards group. Tsutomu Matsumoto, researching the security of thumbprint readers for the ITU, demonstrated the relative ease with

which a thumbprint pressed into a soft plastic material could be used to mold fake fingerprints out of a gelatin similar to the composition of gummy bear candies.

Smith also explained how to defeat another kind of thumb scanner, a device that uses capacitive resistance technology to read a fingerprint. It can be thwarted simply by pressing a plastic bag filled with water against the thumb reader after someone else has used it, the German researchers discovered. Simply blowing on the reader generates enough of a pattern from latent oil left on the capacitive surface to trick the sensor into making a false-positive match.

Other kinds of systems are just as easy to defeat, Smith said.

The German team fooled a facial recognition scanner by showing the camera a short video. The same team cracked another by displaying a photograph of the iris of an eye, printed on a high-resolution color laser printer and with a hole cut in the center of the image, to trick an iris scanner into a false identification.

Smith said he casually tried some of the tricks used by the researchers. A voice recognition suite could probably be defeated with a voice recording, he said. On the other hand, sometimes even legitimate access is denied, he noted.

"I tried this one afternoon with the voice login on my Macintosh, but the problem with that was the Mac wouldn't even recognize me when I said it myself," he admitted.