Fooling biometrics
Seamus Phan
NETWORK COMPUTING ASIAN EDITION, September 01, 2002

We have been led to believe that biometrics will solve our identification and verification woes. Nothing could be further from the truth.

Im tired. There seems no end to how hackers can invent new ways to evade detection, to intrude upon networks, to bring down connectivity, to steal information, or wreck havoc on hardware and software systems.

At the height of the post September 11 period, biometrics vendors were quick to suggest that biometric identification systems will be the answer to identifying and authenticating people. The movie industry also did its part to create this grand delusion that biometric systems can be a guarantee towards flawless identification of any individual.

The fact is that biometric systems are not flawless, and can fail at the simplest means to thwart them.

Fooling biometric systems

The journalists at ct magazine in Germany have proven, at the cursory level, that consumer-oriented biometric products simply dont cut it.

For example, they demonstrated that facial feature recognition devices can be fooled by simply showing a video footage of a registered user moving his head from side to side. The same system also could not reliably detect legitimate users when its security setting was set at a higher level.

Fingerprinting systems were also proven to be inadequate in detecting trusted and untrusted parties. Some fingerprint sensors (and theyre not cheap ones) could be defeated by simply breathing on the sensor where previous fingerprints left oily deposits. Even a thin plastic bag filled with water could force the sensor to reactivate the previous legitimate users fingerprint all over again.

The most reliable way to trick some of these sensors is to use a commercial graphite powder known as Ravenol, dust it onto a previous legitimate fingerprint, and lifted off with an adhesive film. Then place the adhesive film over the sensor with some pressure. Bingo! Youre in!

Professor Tsutomu Matsumoto, a Japanese cryptographer and teacher at Yokohama National University, has also developed a technique where he used gelatin to recreate fingerprints. He claimed that with this technique, he could foil commercial fingerprint readers about 80% of the time.

In the movie "Demolition Man", Wesley Snipes extracted the eyeball of a prison guard using a fountain pen and foiled the iris scanner. Actually, you dont even need to do that. You simply have to get a high resolution photograph of a legitimate users iris and cut a hole in the middle, and you may be able to fool some iris scanners.

What does this mean?

It means that there is still no available security system or method that can guarantee 100% effectiveness.

Vendors touting their systems can sing praises and evangelise their virtues, but the truth is that simple gelatin and a warm breath can easily foil most well-intended biometric sensors.

This compounds the lack of a security mindset among most people in general, as well as the failings of the username and password combination. For more serious security implementations, such as at airports, even x-ray machines can be foiled sometimes by breaking down dangerous items into components, and packing them strategically.

As the Chinese saying goes, "the demon is always miles ahead of the monk." Until crime becomes unfashionable and unprofitable, we will always have to stay vigilant and play catch up.

Are biometrics that bad? talkback@ncasia.com.

World Reporter

Dialog® File Number 20 Accession Number 24758082