South China Morning Post

PUBLISHED TUESDAY, OCTOBER 12, 2004

Even a severed hand will not fool this biometric system thanks to Techsphere's new vascular recognition technology

Hands-on ID system proves hack-proof

Sidney Luk

Like any good biometric identification system used to guard access to secure areas, the VP-II is hack-proof: even a chopped off hand will not fool it.

The machine, developed by South Korea's Techsphere, works by taking an infrared scan of a person's hand, mapping the veins underneath the skin. This map is then compared with information in a database. Cutting off a person's hand simply alters the map and so access is denied.

"The size of the veins will immediately change because the blood will come out [them]," said Derek Elmer, managing director of I-onAsia, the sole distributor of Techsphere products in Hong Kong, the mainland and Macau.

Biometric identification systems can be "hacked" in many other ways, but Mr Elmer claims the vascular pattern recognition technology upon which the VP-II is based defeats these as well.

While most fingerprint scanners reject severed digits, frequently used devices are susceptible to forgery. This is because they collect human residue on their sensors.

A latent fingerprint can be obtained by stretching an adhesive film over the sensor's surface and gently applying pressure.

In some cases, simply breathing on traces of fat left by fingerprints is enough to fool the device.

"All other biometrics systems are easy to forge. [The VP-II] is truly something you cannot forge and has a false acceptance rate of 0.0001 per cent," Mr Elmer said.

Derek Elmer, manager director of I-onAsia, demonstrates the hand vascular pattern recognition system in his office in Kwun Tong. Photo: Oliver Tsang

Even iris scanners have been known to fail. According to Mr Elmer, tests have shown a digital image of a human eye – printed on matte inkjet paper at a resolution of 2400 x 1200 dots per inch – can deceive the devices.

The primary selling point of Techsphere's device is not its skill for foiling forgeries but its ability to be used by the widest number of people. Two per cent of the general population do not have proper fingerprints which can be used with scanners, while scars or cuts also interfere with the devices. Those with eye diseases are not able to use iris scanners.

By comparison, the VP-II has an estimated 99.98 per cent usability rate.

Japan has been an early adopter of vein-pattern recognition systems. Suruga Bank has installed the system in more than 60 branches to help identify customers at the teller window.

The Bank of Tokyo-Mitsubishi, the country's third-largest bank, has also deployed biometric security systems at its branches.

The biometrics market was estimated to be worth US$400 million last year and is forecast to reach $2 billion by the end of next year.

I-onAsia is in talks with Wynn Resorts in Macau to install the system for hotel room door access. The hotel is scheduled to open late next year.

The company is also in discussions with Virgin Atlantic about using the technology as a part of cockpit security access.

In addition, Mr Elmer is speaking to government departments in Hong Kong and Macau about using the VP-II inside offices.

Installation costs are about US$2,300 to $2,600 per unit, though this can be brought down to a few hundred dollars if implemented on a wide scale such as in a hotel.

I-onAsia expects to install 500 to 1,000 units in Hong Kong and Macau in the coming year.

Potential customers include wealthy businessmen, Mr Elmer said. "They are sick of using keys. Just like when Mercedes launched its keyless car, now they can have a keyless home."

I-OnAsia
20/20 Vision
Suites 1603-05,
16/F Lever Tech Centre,
69-71 King Yip Street,
Kwun Tong, Kowloon, Hong Kong
Tel: (852) 2896 4489
Fax: (852) 2217 4449

Copyright © 2004 South China Morning Post Publishers Ltd. All rights reserved.
Reprinted with permission from South China Morning Post Publishers Ltd. Any redistribution of this information without prior written approval is strictly prohibited.
For reprint permission, please send your email to reprint@scmp.com.