Publication: Today , p 26
Date: 15 January 2016
Headline: Phone users to get better protection from hackers

MECHANISM TO PREVENT HACKERS FROM USING PHOTOS OR VIDEOS TO ACCESS MOBILE PHONES

Phone users to get better protection from hackers

LOUISA TANG
louisa@mediacorp.com.sg

SINGAPORE – The widespread use of mobile phones has created more opportunities for hackers to steal information from them, but two projects are under way in Singapore to give users better protection from cyberattacks.

The Institute for Infocomm Research (I2R) has developed a system to detect if fingerprints used in recognition systems, which can be found in newer mobile phone models, are real or spoofed.

Separately, researchers from Singapore Management University (SMU) are working on a detection mechanism for facial authentication functions on mobile phones, which will be able to prevent hackers from using photos or videos to gain access.

These were two projects showcased at the inaugural Singapore Cybersecurity R&D Conference yesterday. The two-day conference, held at the Singapore University of Technology and Design, will bring together about 400 academics and practitioners, through talks and exhibits.

Dr Vrizlynn Thing, department head of I2R's Cyber Security and Intelligence division, said that fingerprint recognition hacking has been a problem ever since the system was implemented in mobile devices.

Motorola first introduced a fingerprint reader in its Android-based Atrix 4G model in 2011, while Apple rolled out the Touch ID function in 2013, with the iPhone 5S. Touch ID is now a widespread feature in the newer Apple mobile devices, including the iPad Air 2 and iPad Mini 4.

I2R's Fingerprint Biometrics Liveness Detection system counters hacking attempts by sensing air bubbles and ridges on fingertips to differentiate from spoofed fingerprints, which hackers fashion from materials like gelatin or latex.

"On your phones, you have a lot of confidential data, emails, contacts, photos. Do you think they are worth protecting?" Dr Thing asked.

"People are getting more and more knowledgeable in terms of attacks. Of course, the common vulnerabilities are being exploited. But there are trends of more sophisticated attackers who have better resources and stronger financial backings to be able to do such type of (hackings)."

Facial authentication hacking is also "quite a common problem" among mobile device users now, said Mr Li Yan, a research fellow at SMU's School of Information Systems.

Facial authentication was first implemented in Android mobile phones in 2011, through the feature "Face Unlock". The system that Mr Li and his fellow researchers are working on, called FaceLive, works with the camera and inertial sensors already available in mobile phones.

It gets users to move the mobile phone in front of their face to capture different angles of it.

The team is currently working on the demo, and is contacting some companies — including local banks — on implementing it in their systems.

> Fingerprint recognition hacking has been a problem ever since the system was implemented in mobile devices.
>
> **Dr Vrizlynn Thing**
> DEPARTMENT HEAD OF I2R'S CYBER SECURITY

Meanwhile, a new National Cybersecurity R&D Laboratory at the National University of Singapore will begin operating by the end of this year, announced A*STAR chairman Lim Chuan Poh, in his opening speech at the conference yesterday.

The lab, supported by the National Research Foundation at a budget of S$8.4 million over three years, will allow researchers in Singapore and around the world to simulate small- and large-scale cyberattacks using its computers.