Strengthening cybersecurity through research

March 14 2017

A new technique allows efficient decryption on mobile devices and supports user revocation in real time. Credit: nicolasmenijes / 123rf

Mobile computing has become a fundamental feature in modern day life as people develop an unprecedented reliance on smart phones and tablets. However, along with their ubiquity comes a host of risks that can affect personal privacy, sensitive corporate information and even national security.

Professor Robert Deng from the Singapore Management University (SMU) School of Information Systems (SIS) believes that current approaches to mobile computing security have been ineffective because they fail to consider differences between platforms and applications.

"Mobile devices are power- and resource-limited compared to desktop computers due to their smaller sizes. They are open to more channels such as mobile networks, Bluetooth, Wi-Fi and storage cards. They also have increased functionality due to their ability to download applications. The mobility, connectivity and extensibility of mobile devices mean they require targeted and efficient security solutions," says Deng, who is also the director of SMU's Secure Mobile Centre (SMC).

This calls for a new approach to security research in mobile computing, one that he and his colleagues at the SMC aim to develop.

One of the centre's many projects focuses on developing practical and secure solutions for sharing encrypted data in the cloud.

"Cloud data storage is becoming increasingly popular. However, since software systems are not guaranteed to be bug-free and hardware platforms are not under the direct control of data owners in the cloud, security risks are abundant. A common solution to mitigate users' privacy concerns is to encrypt their data before it reaches the cloud. This keeps the data private even if service provider systems are compromised or untrusted," says Deng.

However, he notes that it is extremely challenging to share large amounts of data that are encrypted using traditional techniques because of the difficulty in distributing decryption keys and managing decryption key revocations. For example, when people leave an organization, their decryption keys must be revoked so they can no longer access the organization's data.

The SMC has filed a patent on a new technique that will allow individuals and organizations to share encrypted data in the cloud in a scalable and efficient manner. This new technique allows efficient decryption on mobile devices and supports user revocation in real time.

Another project, headed by Dr Li Yingjiu, focuses on designing secure and usable authentication systems for mobile users.

Mobile platforms that authenticate the face of a legitimate user are an attractive alternative to passwords, which are often difficult to remember. However, most face- authentication systems currently in use are intrinsically vulnerable to forgery by means of photos or videos of the legitimate user.

To overcome this problem, researchers at the SMC have developed FaceLive, a system that can differentiate between a photograph or video of a user and a 'live' one. FaceLive corroborates facial video information with live motion data from the mobile device to verify an actual live feed from the user. It uses a front-facing camera, an accelerometer and a gyroscope to detect three-dimensional characteristics of a live user's face.

FaceLive simply requires users to hold and move their mobile device in front of their face while the front-facing camera captures a video of their face and the sensors simultaneously record motion data about their device. A live user is authenticated if changes in head movement in the

video are consistent with movements captured by the device.

Like most systems, FaceLive could be vulnerable to sophisticated attacks, but the system is an improvement on current face-detection software. "Our technique significantly raises the bar for adversaries to perform attacks," says Li.

Provided by Singapore Management University