Publication: The Business Times, p 11
Date: 17 June 2015
Headline: Protecting mobile devices from attack

A Special Feature Brought to You By **Singapore Management University**

Protecting mobile devices from attack

Professor Robert Deng of SMU is leading a team to address challenges in mobile computing security

IN 2013, researchers in Singapore managed to get past security checks in Apple's iTunes store, successfully uploading applications that contained malicious attacking code.

After the researchers informed the tech giant, Apple corrected the problems before its iOS7 launch and acknowledged the work done by Singapore Management University's (SMU) School of Information Systems and A*STAR's Institute for Infocomm Research (I²R).

"Of course we weren't going to attack other users . . . we had a phone conference with their security product team. They even sent an engineer to Singapore to discuss countermeasures," recalled SMU Professor Robert Deng, who was leading this research effort. Prof Deng cited the Apple breakthrough as an example that motivated SMU researchers to do more mobile computing security work.

Subsequently, SMU established the Secure Mobile Centre with funding from the National Research Foundation (NRF). It is currently involved in four projects such as developing solutions for analysing, detecting and containing mobile malware, or malicious software.

"The overall objective of the centre is to develop state-of-the-art security techniques which can provide end-to-end security solutions, including protection for mobile apps and mobile platforms, Internet mobile computing, as well as online or cloud storage services," said Prof Deng, who is the Centre Director and also Associate Dean at SMU's School of Information Systems. The centre comprises 17 staff; five professors including Prof Deng, and 12 other research staff working full-time on the projects.

Fast-growing problem

The team's work is critical, Prof Deng explained, because mobile computing has become ubiquitous. "The number of mobile devices is increasing so fast that it is more than the number of personal computers today," he said. "If my device is lost or stolen, my data can be lost. Malicious software can steal sensitive information."

Mobile security issues are especially pertinent because of certain ways such devices are being used, said Prof Deng. One's device, which contains private information, is constantly connected wherever one goes, such that mobile service providers know where individuals are, what they purchase, and with whom they communicate.

The trend of permitting personal smartphone use at the workplace, known as "bring your own device", means that personal mobile devices are becoming part of the enterprise information system and that private data is stored on the same device as corporate confidential data.

"If the device is compromised, that has implications for the organisation and individual users," Prof Deng said.

Protecting smartphones from attack

The Secure Mobile Centre was established at SMU in February this year. Its first project centres on creating user-centric, on-demand security for mobile platforms. Currently, the security of mobile platforms depends on the operating system, which is too complex, and hence error prone.

However, there needs to be a mechanism where security can be activated for a specific application such that it remains protected even when the operating system is compromised, Prof Deng said. "If you want to use the online banking app, you can activate the security."

The second project involves creating an antivirus-like software to analyse, detect and contain malware.

"We investigate how the extensive connectivity, extensibility, and mobility of mobile devices as well as user behaviours affect the ways in which mobile malware propagates," Prof Deng said. Mobile malware then needs to be detected as quickly and efficiently as possible, and once detected, the damage needs to be contained, he said.

The third project is about how to protect mobile data, now that much is in the "cloud" – on the Internet where it can be accessed by a third party.

"The best protection in the cloud is to encrypt your data, such that everything uploaded to the cloud is already encrypted. You might be able to compromise and access my account, but what you get is garbage because of encryption," Prof Deng said.

"The issue is once you have encryption, how do you share data with other users within the organisation? The users must be able to decrypt it. So in this project, we want to have 'scalable access control', and control who can decrypt my data stored in the cloud," he said.

Authentication, as the first line of defence, is crucial to securing mobile computing systems and services. The final project involves creating secure and usable user authentication techniques for both local user authentication and remote user authentication across the Internet. For example, we want to make sure that biometric details like faces and fingerprints can be safely used by users to gain access to mobile devices or mobile Internet services.

"My vision for mobile computing security is for users to be able to control their security and privacy. If they don't want to release private information, they can do that. If they want to release private information, they can also do that. This involves not only technical innovations, but also user education on security and privacy."

– Professor Robert Deng, Centre Director of Secure Mobile Centre and Associate Dean at SMU's School of Infomation Systems

Current solutions on face-based authentication do not work well because they cannot differentiate between a photo or the real face of a person, Prof Deng noted. "If you want to use face authentication, you need to make sure the device can detect the actual face of a person, and not just a picture. Some of the techniques can detect the blinking of eye, but that can also be faked. We are working on a low-cost technique to solve the problem," Prof Deng said.

The Secure Mobile Centre is conducting research and development projects with ST Electronics (Info-Security), a subsidiary of listed defence conglomerate ST Engineering; international digital security company Gemalto, which also makes SIM cards; telco StarHub, and computer security firm McAfee Singapore, which is now part of Intel Security Group.

The centre is also collaborating with Singapore government agencies such as the Infocomm Development Authority (IDA), the Defence Science and Technology Agency (DSTA), and the Monetary Authority of Singapore (MAS) to bridge research outcomes with practical needs.

Lifelong researcher

Prof Deng, who first came to Singapore in 1987 after getting his doctorate at the Illinois Institute of Technology in the US, has been involved with computer security research work all of his professional life. His research interests include applied cryptography, data and multimedia security, wireless and sensor network security, trusted computing, and cyber-physical security.

Among other things, he helped develop a security standard for the JPEG 2000 image compression file type that was adopted as international standard in 2007.

Through a collaboration between I²R and Tan Tock Seng Hospital, he was part of a team that designed a secure remote consultation process through which eye specialists can diagnose problems remotely. The system has been in place since 2008. "The patient can just sit in a polyclinic . . . you need security because the communication link is over the Internet and patient data is private information," he said.

A number of skills are needed before someone like him can help design security solutions, he said. "You need to know cryptographic techniques, have good knowledge of networks and computer systems – what you're trying to protect – and also understand software."

Looking ahead, Prof Deng sees a few key trends happening in the realm of cybersecurity. For example, emphasis is shifting towards protection of data and applications, rather than at a lower level of the network.

Priority is also being placed on protecting cyber-physical infrastructure, like power grids and the transportation system, from cyber and physical attacks.

The rise of big data and the Internet of Things (IoT) brings unprecedented challenges in information security, privacy, safety and trust. For instance, tiny items of data in aggregate can identify individuals, their lifestyle, and their health conditions. How to efficiently perform data mining while protecting individuals' privacy? How to design security and privacy solutions that meet the ultra fast response times of streaming data in IoT applications? How to authenticate and enforce access control to the numerous objects or "things" which are embedded with low cost electronics, software, and are interconnected with each other? These are just some of the questions the security research community are searching for answers.

"My vision for mobile computing security is for users to be able to control their security and privacy. If they don't want to release private information, they can do that. If they want to release private information, they can also do that. This involves not only technical innovations, but also user education on security and privacy. I believe it is important for users to learn about and be aware of the impact cybersecurity has on an individual and an organisation," he said.

This is a monthly thought leadership series brought to you by the Singapore Management University.
Next month's feature will look into corporate governance practices and finding the balance between ensuring accountability and fostering innovation.