Publication: The Asian Scientist
Date: 2 May 2014
Headline: Keeping data safe from prying eyes

Keeping Data Safe From Prying Eyes

An expert in information security research, SMU Professor Robert Deng is constantly trying to beat hackers at their own game.

By Singapore Management University | Editorials
May 2, 2014

AsianScientist (May 2, 2014) – By Alan Aw – In 2011, Rupert Murdoch's News International sparked a heated controversy for spying on celebrities and public figures to obtain tabloid fodder. Revealing the dangers of data leaks, this incident remains a stark reminder of how crucial information security is even after three years have passed.

In this day and age where the economy is powered by huge swathes of data, information systems are highly valued yet susceptible to great risks.

"Risk and value are positively related, i.e., if value increases, so does risk. Twenty years ago, information security research and education are unheard of. But information systems today have become so valuable that hackers are paying a lot of attention to them. This has led to a tremendous increase in risk," explains Professor Deng, Associate Dean of the Singapore Management University (SMU) School of Information Systems (SIS).

Since his entry into the-then nascent field, Professor Deng has actively pursued his research interest in keeping information safe and secure. Information systems consist of processed data that is either stored in repositories (e.g., CD-ROMs or hard drives), or flowing within networks (e.g., SMS text messages). Such systems are not fail-safe, and thus, have loopholes. For example, a confidential document may be accessible to the public due to poor encryption schemes, despite the owner's efforts at protecting its privacy.

Publication: The Asian Scientist
Date: 2 May 2014
Headline: Keeping data safe from prying eyes

Even smartphones, which are perceived by some to be the greatest industrial innovation of the 21st century, are vulnerable to unauthorised access by third parties or hackers.

This underscores the significance of one of his latest research projects that has given him immense satisfaction: exposing the security flaws of Apple's iPhone Operating System (iOS). Together with his team from the SIS (including Professors Yingjiu Li and Debin Gao, and their PhD students), as well as collaborators from the Agency of Science, Technology and Research (A*STAR), he identified a generic method in which third party applications such as mobile games could be used to launch attacks on iOS devices. The team demonstrated that the method could be used to perform hacking functions, such as cracking personal identification numbers and taking screenshots, without the owner's knowledge.

Having noticed this potential vulnerability that could be exploited by hackers, Professor Deng and his team devised mitigation strategies to allow Apple's engineers to vet third party applications. The team then contacted Apple's Product Security team, who incorporated these strategies into the iOS7 system update. When iOS7 was released in September 2013, the team's contribution was acknowledged by Apple.

From iOS to logistics and law

In reality, the application of information security is much more diverse. Besides smartphone operating systems, Radio-Frequency Identification (RFID) – a ubiquitous technology that enables non-contact identification of objects via electromagnetic waves – is commonly used in logistics and accounting.

For example, in the context of supply chain management, containers of goods are tagged with unique RFID chips for more efficient processing and logistics operations. But third parties can eavesdrop into specific radio-frequency channels and monitor the RFID chips embedded within containers. This is where Professor Deng extends his research focus to examine potential loopholes in RFID technology, and devises countermeasures to strengthen existing security protocols.

According to him, information security also has an impact on law. "In the real world, we have handwritten signatures. In cyberspace, there are digital signatures that are used to authenticate and identify users. There are (parliamentary) acts that allow digital signatures to be used as evidence in the court of law. In law research, researchers should understand how digital signatures are made secure. Some of the technical implications of the validity of such evidence should also be clarified."

Big data and mobile computing security

When asked what the future holds for information security, Professor Deng says research directions will align with social, economic and cultural trends. In particular, interest in big data and increasing pervasiveness of mobile technologies will play monumental roles.

"Data mining involves analysing raw data to derive useful information, for example, on understanding consumer behaviour. We could venture further by looking into data mining on encrypted data. There exists some research in this area, but so far, its practicality has not been proven. This domain is worth exploring, as information security grows into a more robust field, and more information gets encrypted by the day," shares Professor Deng.

Equally interesting is the rise of mobile computing security, as people develop stronger reliance on their smartphones and tablets. Professor Deng notes that the novelty of mobile technology means the field is still amorphous, with much room for exploration by both hackers and security experts. His recent contribution to iOS7 is but the tip of the iceberg.

"Current approaches to mobile computing security have failed to consider key differences between platforms and applications when adopting traditional technologies from non-mobile environments. This calls for a new approach to security research in mobile computing," he explains.

But as hacking strategies evolve, so will Professor Deng's research. He is looking forward to expose more security flaws in the mobile technology space, and to find solutions to beat hackers at their own game.

Asian Scientist Magazine is a media partner of the Singapore Management University Office of Research.

——-

Disclaimer: This article does not necessarily reflect the views of AsianScientist or its staff.