Publication: Asian Scientist Magazine
Date: 2 December 2013
Headline: Winning the data security arms race

Winning the data security arms race

By Singapore Management University | Editorials
December 2, 2013

In the era of smartphones and tablets, SMU Associate Professor Ding Xuhua predicts that the battle between data security experts and hackers will increasingly shift to mobile devices.

AsianScientist (Dec. 2, 2013) – By Shuzhen Sim – As human existence becomes inextricably intertwined with technology, important and intimate details of our lives are increasingly being captured and stored by computers. This trend has dramatically raised the stakes for hackers seeking to profit by illegally gaining access to valuable private data from individuals, governments and corporations.

Just how far can we trust our computers to keep our data safe from prying eyes? Most run-of-the-mill machines rely on security features built into their operating systems to fend off attackers. But these operating systems – the software on which the computer runs – tend to be unwieldy, complex beasts composed of millions of lines of code, and are often riddled with weaknesses that hackers all too easily exploit.

Associate Professor Ding Xuhua of the Singapore Management University (SMU) School of Information Systems thinks that a lot more can be done to arm ourselves against modern day cyber-attacks, and envisions a redesign of the current system.

After his undergraduate studies in computer science, Professor Ding was drawn to the field of data security because of the puzzle-like challenges of building defence schemes. “I like solving puzzles, like in detective novels or suspense novels,” he says, explaining that data

security involves much more of this sort of sleuth work than other branches of computer science.

Puzzles aside, however, a major challenge for developers of defence systems is to create solutions that can be applied to real-world problems. “If I come up with a theoretical solution that cannot be deployed, that may undermine its value,” says Professor Ding, whose vision is for an enhanced security system to eventually be used in all personal computers.

An ideal security system must not only be secure and efficient, he says, but also compatible with existing infrastructure and amenable to rolling out on a large scale. This also helps to make the system more palatable to users, who almost always see security as a troublesome cost that does not add tangibly to their profit margins.

Protecting a small safe box versus a large building

“If a building is big, it’s difficult for us to protect it because there will be more ways attackers can compromise it. But a small safe box is easier to protect,” explains Professor Ding. “My ambition is to develop much smaller software that will work beneath the operating system – its job is purely for security purposes.”

Professor Ding and his team are working towards this “security foothold” using a combination of tools in systems security, which aims to protect data storage infrastructure; and cryptography, which makes use of mathematical algorithms to protect the data itself.

Every day, many of us enter passwords into a variety of Internet sites to access functions as diverse as email, banking, social networking or online shopping. Unprotected computers, however, are often crawling with malicious software that could potentially capture and transmit private information.

A novel feature of Professor Ding’s security system is a scheme that will keep passwords invisible to the browser and the computer’s operating system, while still allowing the user to access the website. This prevents private information from being leaked to malware that may be lurking on a compromised computer.

The security system will also have the ability to isolate programmes containing sensitive information from the rest of the system. For instance, if you were editing a confidential document – your financial records, for example, or the world’s next great novel – the security system could build a fence around your word processor to prevent other applications from accessing the information.

Cyber security in the mobile device era

As mobile devices such as smartphones and tablets evolve to become more like pocket-sized replacements for personal computers, Professor Ding predicts that the battle between data security experts and hackers will increasingly shift to this arena. Smartphones make tempting targets; they store contact information of friends and family, and, unless we disable certain features, are almost always connected to the Internet and signed into email, banking and social media accounts.

Publication: Asian Scientist Magazine
Date: 2 December 2013
Headline: Winning the data security arms race

Defending the mobile device realm brings with it a whole new set of challenges, chief of which is the fact that we interact with our smartphones in completely different ways as compared to desktop or laptop computers. For example, smartphones are always on or near a person, and contain many sensors which can detect and track human actions. This human-technology interface and how hackers may exploit it is still uncharted territory in the field of data security, says Professor Ding, who also aims to develop his security system for use in mobile devices.

The intersection of human behaviour and technology is one example of how, while his research primarily focuses on the technical aspects of data security, Professor Ding sees his work as being interconnected with other social science disciplines represented at SMU. One such overlap is with the field of economics, where understanding the financial incentives behind targeted hacking attacks may provide new insights into how to combat them. “Security is like salt; we will never eat salt alone,” Professor Ding quips.

Professor Ding likens his work to an arms race, with no clear end in sight. His job, he says, is to fortify our computer defence systems to a point where we can live with the existing threat level, and where we will be able to mount a quick and effective response against any cyber-attack.

“Security is like a war, or a race between attackers and defenders. The war will never stop. No human can be immune from all virus or bacteria attacks, the same goes for computers.”

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