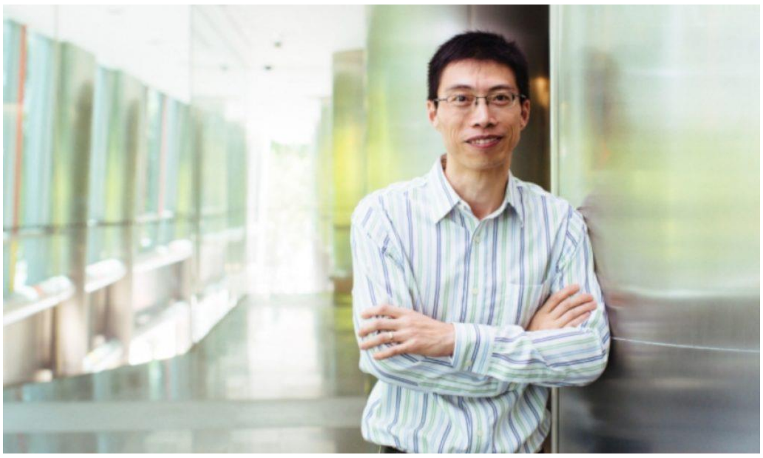
**Publication: Asian Scientist Online**
**Date: 23 November 2018**
**Headline: Levelling Up In The Real-Life Game Of Cybersecurity**

## Levelling Up In The Real-Life Game Of Cybersecurity

Secure systems that combine hardware and software tools are necessary to protect mobile devices and autonomous systems against increasingly sophisticated cyberattacks, says SMU Associate Professor Ding XuHua.



AsianScientist (Nov. 23, 2018) – By Jeremy Chan – When physical spaces need to be kept secure, fences are built around them, locked gates prevent access by unauthorized personnel, and security cameras are positioned at strategic areas to watch for suspicious activity. There was a time when these measures were sufficient to grant a person peace of mind. But as society increasingly operates in cyberspace as well as physical space, new barriers need to be erected to keep our private information—analogous to private property—safe from prying eyes and malicious intent.

Building strong, secure systems to defend against cybersecurity threats is all in a day’s work for Associate Professor Ding XuHua at the Singapore Management University (SMU) School of Information Systems. Having graduated with a PhD in computer science from the University of Southern California, Professor Ding’s interest in cybersecurity was sparked by the advent of the Trusted Platform Module (TPM). This is a chip embedded within connected devices that monitors the state of their hardware and software, ensuring that they behave as intended. Think of it as the CCTV system of the computer world.

What fascinates Professor Ding is how a hybrid of software and hardware tools can synergise to better protect one’s electronic gadgets and personal data. He notes that “the scale and complexity of cybersecurity issues today are totally different from those ten or twenty years ago,” warranting research that fully leverages such tools to help shore up cyberdefences.

Hello, can I trust you?

With the proliferation of mobile phones and the Internet of Things (IoT), Professor Ding thinks that hackers will increasingly target these devices to steal valuable information. While many device manufacturers do include trusted components such as TPMs in their products, how can users be assured that these cybersecurity features are indeed present and providing constant protection against cyberattacks?

“One of my recent projects is to help human users establish trust on their mobile phones by verifying whether the phone’s trusted component is active or not,” says Professor Ding.

This is what he calls presence attestation—a trusted component such as the phone’s on-board cryptoprocessor must not only prove its own existence, but also vouch for its location and function on the device.

The first step requires the trusted component to communicate with an external entity that can verify its existence. This is akin to a phone conversation between two individuals who are familiar with each other's habits and personal preferences—without meeting face-to-face, one can confirm the existence of the other.

But this strategy could fail should there be a skilled impersonator—the equivalent of a hacker—who can produce a valid response to queries about private details. Hence, Professor Ding recommends a second step known as residence checking, whereby other capabilities of a mobile phone, such as its GPS and camera, are used to prove that the mobile phone's trusted component is generating the responses, and not a remote device.

Professor Ding discussed these strategies in a paper titled 'Presence Attestation: The Missing Link in Dynamic Trust Bootstrapping', which was published in the Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security.

## Finding the right fit

Despite the numerous available strategies to ensure the security of mobile phones and IoT devices, they must be deployed appropriately for them to be effective.

"In terms of the academic or technical challenges of my work, I would say that striking a good balance between security, compatibility and usability is the biggest challenge," says Professor Ding.

Trade-offs have to be made in the design of secure systems—enhancing one feature usually means compromising on something else. Put simply, you can't have your cake and eat it.

For example, relying on a presence attestation protocol that is highly secure but requires the user to perform a tedious task will result in poor adherence to the protocol, thus undermining its raison d'être. To further complicate matters, user behaviour is not the only factor to be considered when making decisions about which security strategy is the most feasible. If a presence attestation protocol requires mobile phone manufacturers to include additional hardware features simply to beef up security, then the uptake rate of such approaches may not be high.

Therefore, Professor Ding makes it a point to think through the possible scenarios that would promote or prohibit the implementation of secure systems in his research. He also takes into account how the methods he proposes may be subverted by skilled cyberattackers, putting himself in the shoes of the adversary to sniff out cybersecurity loopholes and potentially patch them.

## Securing the autonomous future

Acknowledging that new technologies such as unmanned drones and driverless cars will inevitably contain digital components that are vulnerable to hacking, Professor Ding senses some urgency in developing the right tools to protect these autonomous systems.

"I am interested in exploring techniques that can protect critical functions of autonomous systems against malware attacks," he explains, citing, as an example, malware designed to impair a drone's ability to send out a distress signal to its home base.

"Techniques to ensure the availability of such functions are vital to the adoption of autonomous systems," he adds.

Therefore, while most developers of autonomous systems tend to focus on the 'intelligent' aspects of their products, whether or not these products become accepted by society may well depend on the strength of their cybersecurity features.

**Publication: Asian Scientist Online**
**Date: 23 November 2018**
**Headline: Levelling Up In The Real-Life Game Of Cybersecurity**

“The importance of cybersecurity can be attributed to the fact that almost all software exists in an environment with other software, each interacting with the other. Building a secure system is very much like building a safe community,” Professor Ding emphasizes.