Tackling 5G-based mobile computing and cloud computing security concerns head-on

2 March 2020, by Alvin Lee

The sheer number and wide variety of devices connected via 5G mobile networks demand differentiated security solutions. SMU Professor Robert Deng points to the need to ask the right questions, and a multiparty approach to create effective solutions. Credit: Alvin Lee

In a June 2019 report, telecommunications equipment provider Ericsson predicted that there will be 8.3 billion mobile broadband subscriptions by the end of 2024, which translates to 95 percent of all subscriptions by then. Total mobile data traffic will reach 131 exabytes per month (1 exabyte = 1 billion gigabytes), with 35 percent carried by 5G networks.

While mobile phones will consume the bulk of the data, the sheer number and wide variety of devices that will be connected via 5G technology is likely to pose security threats not faced by previous generations of mobile networks, explains Professor Robert Deng at the SMU School of Information Systems.

"When 5G becomes pervasive, the majority of the devices connected to mobile networks will not be mobile devices anymore," he says, referring to things such as household appliances, lightbulbs, or indeed something mobile like an autonomous car that is itself filled with smaller IoT devices such as sensors. "Some of them will be as powerful as the mobile device we're using today, while some will have minimal computational and communication capability.

"Given the variety of IoT devices, given their different capabilities and deployment environments, the security requirement of solutions will be very, very different."

Solving cybersecurity concerns, in the mobile world and on the cloud

Professor Deng is the Director of the Secure Mobile Centre (SMC), which hosts the National Satellite of Excellence in Mobile Systems Security and Cloud Security (NSoE MSS-CS). As he runs the research initiative aimed at building "a mobile system security and mobile cloud security technology pipeline for smart nation applications", Professor Deng points out the main questions that need answering when designing security solutions:

- What is the application context?
- What is the threat model, i.e. who is going to attack you?
- What are the risks?

He elaborates: "When the IoT becomes pervasive, the requirements will be very different from those for today's mobile applications. You have to come up with new security solutions for any particular type of IoT application, [which necessitates] differentiated security services."

The resource constraint of some IoT devices also poses cybersecurity challenges. A lot of existing security solutions would not work on a surveillance camera mounted on a lamp post, which is much more limited in computational and storage capabilities.

"Given that kind of devices, how do you add in security?" Professor Deng points out. "I have the IoT devices but there's no user interface. How do I perform user authentication? Those are the new requirements we are going to deal with."

Bigger devices such as cars and drones also demand attention, Professor Deng says. With the advent of autonomous cars, vehicles need to have the capability to stop themselves in the event of emergencies even if they are infected by malware. Similarly, a drone must be able to execute critical operations such as returning to home base in the event it is hacked.

The other main concern of the NSoE MSS-CS is mobile cloud security, especially when "data records in real time monitoring system may contain sensitive information".

"As a data owner, I upload my data to the cloud. How do I know that data is still under my control and not under the control of the service provider or my adversaries?" asks Professor Deng, who is also the AXA Chair Professor of Cybersecurity at SMU. That is the reason for cybersecurity experts' continuing efforts to build stronger encryption capabilities, but which also leads to the difficulty in sharing critical data. He notes:

"My folder is encrypted and I want to share my folder with you, but you must have the decryption key. But how do I pass the key to you? We are designing a solution where I don't even have to pass the key to you, but it automatically gives you all the permission to access my folder even if it's encrypted. The other issue is how do you do the computation to process and access the data that is encrypted? Those are the things we do."

Co-operation

The SMC is one of seven research projects funded by Singapore's National Research Foundation (NRF) aimed at developing research expertise and capabilities in cybersecurity. While technical challenges in designing solutions are obvious obstacles to the stated aim, Professor Deng highlights structural and ecosystem concerns that should not be overlooked.

"Because most of the Principal Investigators are professors and academics, how do you get in touch with partners who will quiz you?" muses Professor Deng. "You may have an interest in a solution, but that interest may only be a component of the solution. It's not the whole solution.

"How do you integrate your novel component solution with a larger system so that the larger system can improve? And how do you turn the solution into a product? It's a challenging process."

He concludes: "All this requires close collaboration between the university researchers, government agencies and also the industry. These are the practical challenges for technology transformation."

Provided by Singapore Managment University

APA citation: Tackling 5G-based mobile computing and cloud computing security concerns head-on (2020, March 2) retrieved 28 November 2022 from https://techxplore.com/news/2020-03-tackling-5g-based-mobile-cloud-head-on.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.