Nanotechnology for IoT Security

Abstract

Within the past decade, the number of IoT devices introduced in the market has increased dramatically. The total is approaching a staggering 15 billion, meaning that there are currently roughly two connected devices per living human. This trend is expected to continue at a rapid pace, with an estimated 50 billion connected devices by the year 2020. However, the massive deployment of IoT devices has led to significant security and privacy concerns given that security is often treated as an afterthought for IoT systems. Security issues may come at different levels, from deployment issues that leave devices exposed to the internet with default credentials, to implementation issues where manufacturers incorrectly employ existing protocols or develop proprietary ones for communications that have not been examined for their sanity. On the hardware side, a device may also be vulnerable. An attacker with physical access to a device may be able to alter its functionality. A compromised device, whether by remote or physical access means, can then be used as a tool to exfiltrate sensitive network information, attack other devices, and as means of automatically sending malware over the internet. In this talk, I will first introduce the emerging security and privacy challenges in the IoT domain as well as our effort to systematically summarize IoT security vulnerabilities. I will then present a design-for-security flow towards trusted IoT and their applications leveraging emerging nanotechnology based hardware protection methods. A demo will also be shown to prove the effectiveness of the proposed solution.