RSiS Nanyang Technological University | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

RSIS COMMENTARY

www.rsis.edu.sg No. 143 – 13 June 2016

Pitfalls of the "Internet-of-Things"

By Tan Teck Boon

Synopsis

The global network of Internet-enabled sensors, devices and systems called the "Internet-of-Things" promises many upsides. But many IoT products are vulnerable to hacking. In the IoT age, it is vital to strike a balance between the risks and rewards.

Commentary

THE "INTERNET-OF-THINGS" (IoT) is a catchall phrase for the global network of Internet-enabled sensors, devices and systems that collects and shares a vast amount of personal data. Wildly diverse and growing fast, the billions of IoT products out there right now include fitness trackers, medical devices, household appliances, mobile gadgets and even Barbie dolls. According to IT research company, Juniper Research, there are now more than 13.4 billion IoT products in use and by 2020, the figure will hit 38.5 billion.

Proponents contend that once we are fully immersed in IoT, the technology will engender myriad benefits. They claim that energy-saving IoT products will enhance our situational awareness and quality of life too through automation. For example, when a sleep tracker is connected to a smart air-conditioner and coffeemaker, the wearer not only wakes up to a freshly-brewed cup of coffee but also feeling totally refreshed because the temperature in his bedroom is synced to his sleeping pattern. So not only does the wearer of the sleep tracker know the quality of his sleep, he is also doing his part for the environment by letting the smart air-conditioner adjust the temperature accordingly throughout the night. As appealing as this high-tech option may sound, it is unfortunately clouded by serious cybersecurity concerns.

The Downsides of IoT

The biggest fear right now is that a large number of IoT products are susceptible to hacking. Indeed, many IoT products are resource-constrained, meaning that they do not come with firewalls, encryption/authentication and antivirus capabilities built-in. We install security protection into our smartphones, PCs and tablets; but doing so with the smart toothbrush or kettle may not be possible because they have limited computing power. Even if it were possible to patch IoT products with security upgrades after they had left the factory, it would be a logistical nightmare given their sheer numbers out there.

According to estimates from Hewlett Packard, a staggering 70% of IoT products currently in use are vulnerable. In a sign of things to come, penetration tests (or "pen-testing") designed to uncover security vulnerabilities in IoT products have shown that it is possible to breach home Wi-Fi networks via IoT appliances. So hackers could in theory exploit weaknesses in everyday IoT products and work their way into corporate or government networks as employees bring their infected gadgets to work.

Sounds incredible but in 2013, we inched closer to this dystopian nightmare when hackers breached the database of Target and stole the credit card numbers of 40 million customers apparently by hacking the US retailer's Internet-enabled heating and air-conditioning system.

Implications of a Cyber Takedown

In the worst case, hackers could take over or shut down major infrastructure networks throwing critical sectors like banking, transportation and telecommunications into chaos. The consequences would be catastrophic. Or they might attempt to retrieve sensitive information stored in these networks. Bear in mind, IoT products collect a vast amount of personal data. Not just plain information like names, birth dates and contact details but revealing information like energy consumption patterns, geo-location data and lifestyle habits. To the untrained eye, this kind of information means nothing but in the hands of sophisticated criminals, it can be used to make scams more elaborate and convincing.

The reality is that IoT is a "double-edged sword". Indeed, having an IoT security cam that lets you see what is happening in your house via your smartphone might make a lot of sense when you are away but it also means that cyber criminals could watch you in your own home if the system had been compromised. Likewise, owning a smart TV that is voice-activated might seem like a nifty idea except that your privacy would vanish if hackers were able to listen in on your private conversations.

Common sense tells us that we should never share anything online that we do not want others to know about. But with the advent of IoT, the datafication of our most intimate personal information is unavoidable; more importantly, we will not have a choice about it. So if you are concerned about your online data privacy, then you should definitely be very worried about IoT.

It's Not All Bad – And besides Do We have a Choice?

Shunning IoT products completely would be unrealistic since they do bring important benefits. Furthermore, as existing electronic products get phased out, users have no choice but to replace them with IoT ones. Try buying a rear-projection TV today or apply for a job without a smartphone and you will see the impracticality of snubbing the latest technology. If turning our backs on IoT products is not feasible, then what we need is prepare for its inevitable arrival.

For major organisations, this would mean integrating IoT products in a step-by-step fashion – taking the time to evaluate the technology with great care. The government can certainly help by assessing every IoT product for potential risks. If an IoT product is deemed too much of a cybersecurity risk then it should definitely not be integrated into a broader network.

The government also needs to set industry standards to ensure that IoT product manufacturers do not cut corners on their products since building in added security features will eat into their bottom-line. Apart from tightening security in the cyber domain, the government also needs to put tough data protection measures in place to limit abuses of personal information collected by IoT products. Lastly, consumers play a crucial role too; besides ensuring that their IoT products are secure, they must also be responsible enough to avoid those that are not.

When all is said and done, we need to recognise that at the moment no software-based product is really “hacker proof” and sooner or later, some IoT products will be breached by hackers. So some loss of online data privacy is to be expected as we enter the IoT age. The key then is finding that balance between risks and rewards – that sweet spot which allows us to enjoy the upside while keeping the pitfalls to a level that is tolerable.

Tan Teck Boon is a Research Fellow with the National Security Studies Programme in the Office of the Executive Deputy Chairman, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. An earlier version appeared in TODAY.