Hot issues

How safe are IoT devices?

Consumers are increasingly buying Internet-connected appliances for their homes. Often referred to as the Internet of Things (IoT), the range of internet-connected products already available includes not only the obvious things like Smart TVs, gaming consoles, security and safety cameras, but smart light bulbs, sewing machines and even dishwashers.

Telstra says the average home already has 11 or 12 connected devices and predicts that by 2020 a typical home will have about 30.

As well as being useful by enabling us to remotely manage our home environments, many of these devices also collect a lot of data. Conceivably, this data collection can pose huge risks to consumers' privacy and security.

To find out more about possible threats to privacy and security, researchers from the University of NSW profiled some real devices available in the market with the aim of developing materials to educate consumers and inform policy-makers on the risks associated with widespread adoption of IoT. The project was funded under the ACCAN Grants Scheme.

Benefits come with risks

The report produced by the researchers, *Inside job: Security and privacy threats for smart-home IoT devices*, found that we now rely on connected devices in our everyday lives. These devices save us money and time, help us stay fit, healthy and safe and allow us to communicate effectively with friends and family.

But with these benefits there are also risks. The project found that consumer-focused IoT devices are susceptible to attack by those wishing to do us harm, or simply to just make mischief.

Many internet-connected devices have poor in-built security measures that make them vulnerable, and these flaws have the potential to reveal private data and information that may further hurt or alarm us.

A typical smarthome with many IoT devices is under significant risk of cyber-attack, or may in turn form part of an attack on other internet-connected sites or systems.

What are the risks?

The researchers tested 20 IoT devices, including cameras, motion sensors, smoke alarms, printers, light bulbs and a connected talking doll.

They found that:

- Five of the devices did not retain data in encrypted form, making it easy for intruders to snoop on user information.
- Four of the devices allowed attackers to manipulate them so they could run fake commands, and two of the webcams tested had weak passwords, making them easy to hack.
- More than half the devices tested could be rendered dysfunctional after being bombarded with a high volume of attack traffic.
- Most of the devices tested could be manipulated in some way to participate in attacks on other devices.

The results showed that all of the IoT devices tested have at least some level of vulnerability to attack.

Conclusions

The rapidly increasing demand for IoT devices poses many security and privacy issues. Internet-connected devices will soon become commonplace in homes and businesses, and will offer consumers many productivity and lifestyle benefits.

The testing suggests that many current IoT devices are vulnerable to attacks in a number of ways. Hackers can use quite unsophisticated technology and methods to gain access to personal data within IoT devices from anywhere in the world. They can also use simple, everyday consumer items to create powerful reflection attacks on other internet networks and systems.

It's a complex problem, and there doesn't appear to be any simple solutions to make IoT devices safer and more secure. Currently, there is no basic set of agreed security standards or one body in Australia that is capable of overseeing the industry as a whole. A further risk with such a fast-moving sector is that basic acceptable standards might become obsolete as quickly as they are established.

The present IoT environment raises many unresolved questions for consumers, manufacturers, regulators and insurers. Of particular concern is whether the cost of regulation and insurance will stifle innovation in the IoT industry.

It is apparent that consumers will demand greater levels of security and privacy from their IoT devices once they are more aware of the potential risks.

This project, in conjunction with anecdotal evidence in the media, clearly exposes the large-scale lack of security in smarthome IoT devices.

It is hoped that the findings will begin a dialogue between consumers, suppliers, regulators and insurers of IoT devices to develop appropriate methods to tackle the problem. The project has already facilitated more rigorous security testing in the Australian marketplace.

What should consumers do?

The following steps are worth considering if you are contemplating any new home internet-connected device. Just as the front gate needs the occasional oil and the oven needs cleaning, with any home internet appliance there is likely to be occasional housework and maintenance required.

- Read the manual, and follow any recommended security steps.

- Check the packaging to ensure any device you are about to use hasn't been tampered with.
- Update the software and set it to auto-update where possible.
- Change the password – keep a record in a secure location if you need to, and don’t use obvious ones.
- If the device runs additional services in the background, turn off any you don’t need.
- Back up important home network data.
- Connect devices with cables (not Wi-Fi) where long term connections are desired (eg TVs).
- Place stickers over internet-connected cameras and microphones that are not in use.
- Turn equipment off at the power switch and disconnect when not needed.
- Run an up to date virus checker on home computers and monitor home network traffic levels. If any unaccounted spikes occur, it could be worth investigating.
- Use a good quality home network gateway and set the firewall features to block incoming connections.
- Don’t share unnecessary personal information when using these devices.