ISPANZ POSITION PAPER

THE INTERNET OF THINGS (IoT)

There is much discussion of IoT in the media. ISPANZ is concerned that end users with IoT devices may not be implementing adequate security measures.

The Problem

Many companies are developing sensor network devices and data solutions for a number of industry verticals. The reality is that these devices are often simply "plugged in" to the public internet by way of a data SIM, thereby becoming directly connected to the broader internet (with a public IP address) and with no border security.

At the small, low power, low cost end of IoT devices there is often little scope to include any form of firewall, leaving the device wide open in both traffic directions. It is not viable to enforce security at the device level unless it can be baked into the GSM modules themselves (something that companies like uBlox may well consider) but that would come at a cost in terms of processing power (affecting battery life and producing more heat) as well as the actual financial cost of the module.

As an example: You can now buy an 802.11g WiFi module with 4MB of flash memory for under NZ$2, attach a power source and you have an IoT sensor with multiple I/O and a WiFi interconnect. There is no scope to add a firewall to such a device given the extremely low amount of memory space for code combined with the low performance processor.

Devices like this can easily be incorporated into a multi-thousand node network capable of disrupting critical services such as DNS. The compute power and bandwidth requirement to effect a distributed denial of service (DDoS) attack does not come from the capability of a single device, it is the cohesion of thousands of devices working in unison – sometimes across the globe.

The Solution

Unfortunately, there is no obvious silver bullet, a sentiment reinforced by the fact that 'IoT Discussion' groups are forming all over the world, this is a new and very distributed attack surface and needs to be controlled sooner rather than later.

One concept is that of a separate network for IoT devices, with inherent 'per IP' security controls, much like what NSX does on the VMware stack, allowing per IP protection within a

common subnet by forcing all switched traffic to route via a known point (router) rather than simply locating peers on the local network.

Some companies achieve this by running their own VPN to their mobile network provider and picking up their own private IP subnet of devices directly, so they are never internet routable and therefore much more secure. That is not viable for mass-market solutions of "plug and play" design.

ISPANZ encourages its members to make their customers aware of the security issues associated with IoT devices and be in a position to advise them appropriately.