Security considerations for using the Perth Internet of Things Communications Network

Published 19 September 2017

Prepared by

Robbie Whittome CISSP

Background

The Internet of Things (IoT) is increasingly pervading in our society. Whilst there are millions of unrealised use cases which could help and enable individuals and society, security threats may be realised to cause great disruption or harm. With these security threats in mind, this document has been developed to support the community members of the Perth Internet of Things Communications Network (PIoTCN), with considerations to enable improved recognition of digital security within the PIoTCN.

Intentions and use of the PIoTCN

Whilst the majority of the Perth Internet of Everything community seek to learn and support others, and act in accordance with the PIoTCN memorandum of understanding (MOU), there will be parties who by accident or deliberate actions seek to disrupt or cause harm to community members. To support your fellow community members, it is vital to consider and review how you are using the PIoTCN so as not to disrupt or harm others.

Here are some questions you could ask yourself to identify if you are supporting the PIoTCN mission:

- Have I read and understood the Things Network Manifesto and PIoTCN MOU?
- Am I using the Things Network or PIoTCN in a way that may harm or adversely impact others? This might include modification or alteration of devices, network communications or settings to the detriment or loss of another community member.
- Could I do more to understand the "Things" I am connecting further before I send or receive data? Have I searched the internet for how to configure my "Things" securely, for example manufacturer's website and forums or community user forums? A useful starting security resource you can review is the OWASP IoT Project – especially the IoT Vulnerabilities page.
- What risks am I assuming when connecting my "Things" to the PIoTCN? If something goes wrong, what are the foreseeable adverse consequences that could happen to me, the community, my data or my devices and I am happy to accept these risk to obtain the benefits of being a community member?

Protecting myself

There are unfortunately a significant number of people (bad guys) that seek to disrupt or harm our technology enabled society. The skills of these bad guys are increasing, primarily supported by criminal organisations and hostile governments. We must assume that there is someone out there whose intent is to cause harm to us through our technology and as such, we must do everything within our ability to protect and defend our technological devices.

Here are some questions you could ask yourself to consider if you have done everything reasonable to protect your data and "Things" from the bad guys.

ISOLATE

Have I isolated my "Things" from any technology I really care about (home medical devices, expensive appliances, appliances that are hard to replace)?

Threat: bad guys might cause harm or damage to attached appliances. You only have to look at the impact of Stuxnet more than a decade ago to see the potential harm that could be caused by an absence of security measures.

Mitigation: avoid connecting any appliances you aren't happy to replace, and consider isolating devices you are connecting using separated internet connections, configuring separate VLANs to segment network connectivity, separate power feeds, and disconnecting internet connectivity when devices or "Things" are not in use or needed.

RESTRICT

If I am the gateway owner, have I restricted the internet services which may result in the conduct of illegal activities (e.g. torrents, illegal websites)?

Threat: bad guys may use these services to conduct illegal or immoral activity. As a consequence, law enforcement organisations or your internet service provider may issue you with notices or hold you liable for the actions undertaken on your provided internet service.

Mitigation: you could contact your internet service provider to apply parental restrictions on your service, or acquire additional security solutions which site in front of the gateway, managed by a professional service provider, such as a web application firewall, load balancer and/or web content filtering solution to address reduce opportunities for bad guys. You could also block ports and IP addresses which may not be needed for the services you are offering (i.e. file transfer ports, blacklisted IP address ranges, forged IP address packets).

DATA SENSITIVITY

Are any "Things" connected to, or able to access data or information that may be personal or sensitive (i.e. names, date of birth, address, tax file numbers, credit card numbers, etc.)?

Threat: this sensitive information may be accessed and disclosed or used by bad guys causing harm to individuals through identity or financial theft.

Mitigation: is there a need to access or connect to this information? If not, the simplest measure is to disconnect access to this information or move it to a separate location to prevent access by bad guys. If there is a need to access this information, determine if you need consent to use this information. Consider what security you will need to implement to limit access to view or modify this data when stored (such as access restrictions, auditing, and data encryption) or transmitted (such as use of robust internet protocols, encryption in transit, and validation of internet connections inbound).

ENCRYPTION

Where I am transmitting data, is there a need to ensure my data isn't read or tampered with by anyone I don't know?

Threat: unencrypted data or more generally data broadcasted could be listened to by bad guys or the gateway owner. This data could be accessed, modified, deleted or additional unwanted data injected into the network, causing an inability to rely on the information and maintain data confidentiality.

Mitigation: consider who should receive the information transmitted by your "Things". Limit visibility through encryption or data obfuscation; set specific network routes to specific destinations where you don't want the whole world knowing of your data's existence; and use robust internet protocols to prevent replay attacks.

VULNERABILITIES

Have I mitigated common vulnerabilities for my "Things"?

Threat: Common vulnerabilities such as weak passwords or insecure firmware are easy ways for bad guys to access and disrupt your "Things" and data.

Mitigation: Consider security from the commencement of your journey with the IoT. Tackle simple and quick wins such as changing default passwords, using complex passwords, upgrading firmware and turn on logging to see what is going on. There are several detailed considerations provided by the OWASP IoT Project in the form of IoT Security Guidance.