Re: Statutory Review of the Security of Critical Infrastructure Act 2018

Author: Paul Wilkins

Date: 19 February 2021

Supplementary

Contents

The author wishes to contribute the following supplementary to his original submission.

Rust Code Base as Best Practice for Embedded Software

It's not possible to have a serious discussion around infrastructure cyber security, without due consideration of the implications of the Rust [1]programming language's disruption of established code base security paradigms and frameworks. Wet finger in the air [2]suggests that migration of code bases from C/C++ to Rust reduces the threat landscape by a factor of 3. There is no exaggeration that an entire industry of firewall and antivirus vendors has been built on the mitigation of memory out of bounds exploits.

The Rust language paradigm integrates compile time mechanisms that ensure strong memory protection, that virtually eliminate memory out of bounds exploits. As the software industry moves to adopt this new paradigm of strong memory protection, an entire category of cyber exploit mechanisms[3] are eliminated. This is pertinent to this enquiry's current concerns, as it will:

- Greatly reduce the incidence of effective exploits – by estimated factor of 3.
- Greatly reduce the incidence of software vulnerability reports – by estimated factor of 3.
- Greatly improve the content value of vulnerability reports in identifying risk.

When it comes to defining actual standards for cybersecurity, there will need to be consideration for endorsement of Rust as establishing a best practice baseline requirement for memory out of bounds protection.

---

[1] https://www.rust-lang.org/
[2] https://www.zdnet.com/article/chrome-70-of-all-security-bugs-are-memory-safety-issues/
[3] https://cwe.mitre.org/data/definitions/787.html

Recommendation:

SoNS' embedded computing devices be able to demonstrate that drivers and system services, if not developed in Rust, can provably demonstrate equivalent memory out of bounds protection.

Internet of Things as an Existential Threat to National Cyber Security

IOT should be recognised as a "System of National Significance", under the definition of s52b for its potential adverse impacts on "other critical infrastructure assets". There is a present need for regulation of the sale of IOT devices. This could take the form of mandatory compliance with an Australian Standard for IOT devices as a condition of sale of the device within Australia.

Best case for such a standard would include the following requisites:

- Recognise IOT as a "System of National Significance".
- Drivers and system services if not developed in Rust, can provably demonstrate equivalent memory out of bounds protection.
- Software updates to be available free of charge for the usable lifetime of the product.
- Software updates to be distributed through a nationally centralised, permanently resident IOT patch update server, thus ensuring the security and scale of the patch update server, and guaranteeing the availability of an automated patch mechanism for the life of the product.