IoTAA submission to:

Department of Home Affairs consultation on:

Securing the Internet of Things for Consumers

Draft Code of Practice

1 March 2020

Contents

Executive Summary 3

Introduction 4

About IoT Alliance Australia (IoTAA) 4

Comments on the Draft Code of Practice 5

Security of the overall (end-to-end) IoT system architecture 5

Greater clarity on responsibilities 5

Don't inadvertently mandate forced firmware upgrades 6

Supply chain security 6

IoTAA's Security Trust Mark (STM) Scheme 7

Do not legislate to make accreditation schemes mandatory 8

Conclusion 9

Appendix: IoTAA Strategic Plan to Strengthen Security 10

Executive Summary

The IoT Alliance Australia (IoTAA) welcomes the opportunity to provide a submission to the Department of Home Affairs consultation on its *Draft Code of Practice for Securing the Internet of Things for Consumers*.

We commend the Australian Government for the creation of the Draft Code of Practice, and for its close alignment with the UK Government's code of practice. We believe it is important that such codes are aligned across the five-eyes nations, and we believe the creation of the code is an important step in improving IoT security for consumers (and businesses) in Australia.

We make four general recommendations about the draft code, including:

- Adding a principle to cover security of the overall (end-to-end) IoT system architecture;
- Clarification of responsibilities, especially when multiple actors are required to work in concert to achieve compliance with the Code;
- Avoiding inadvertently mandating firmware upgrades; and
- Adding a principle covering supply chain security.

In addition, our submission makes a recommendation for the endorsement of the IoTAA's Security Trust Mark (STM) labelling scheme. The STM scheme provides consumers, business and government critical visibility and confidence that the devices and solutions they are purchasing and using meet the vendor's claims of its security capabilities independently. The STM scheme we propose is an industry led initiative which uses market signals and responses to drive vendor and user behaviour (e.g. somewhat like the ANCAP or Energy Rating marks). It provides a compelling commercial incentive for vendors, practitioners and users to ensure good IoT security practices. We contend that consumer concerns regarding IoT security coupled with awareness and recognition of an IoT Security Trust Mark will drive demand for IoT products and services that display the Mark. This in turn, **will drive more suppliers to voluntarily meet the requirements**. Government endorsement of the STM scheme coupled with procurement policies requiring IoT devices to carry the Mark will further drive demand for, and adoption of the scheme.

The design for the STM scheme draws on the industry approach documented in the IoTAA's 2017 **Strategic Plan to Strengthen IoT Security in Australia**[1], and focuses on the full end-to-end IoT services and solutions "eco-system", not just IoT devices (as IoT is commonly thought of). Any IoT eco-system can be defined by the **IoT Reference Framework**[2] which has also been developed by the IoTAA.

With the rapid evolution of IoT services across consumer and industrial domains, the lagging adoption of security technologies and the shifting of IoT security attack vectors, an industry-led model for implementing the STM offers the best option for adaptability and efficient adoption. Further, the proposed STM offers greater protection beyond the minimum set of voluntary requirements, which will enable Australia to be a global leader in IoT Security.

We close our submission by noting our recommendation against legislating to make accreditation schemes mandatory.

[1] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf
[2] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

Introduction

The IoT Alliance Australia (IoTAA) welcomes the opportunity to provide a submission to the Department of Home Affairs consultation on its *Draft Code of Practice for Securing the Internet of Things for Consumers*.

Our submission is in two parts:

- Firstly, we provide feedback on the draft Code of Practice; and
- Secondly, we propose an approach that provides a compelling incentive for vendors to embrace the Code of Practice through the introduction of a Security Trustmark scheme.

About IoT Alliance Australia (IoTAA)

IoTAA, www.iot.org.au, is a not-for-profit industry association incorporated in July 2016. We are the peak Australian IoT industry body. The vision of IoTAA is:

> **"To empower industry and society by accelerating IoT innovation and adoption for Australian economic and societal benefit."**

We see ourselves as a prime instigator of IoT collaboration and advancement in Australia through a network which includes community and citizens, government, research and industry – all of whom contribute to our work.

IoTAA now has over 500 organisation members and 1000 participants. IoTAA runs twelve programs (workstreams) covering:

- Industry sectors:
  - Transport;
  - Cities;
  - Manufacturing;
  - Water;
  - Energy;
  - Health;
  - Food and Agribusiness;
- Collaboration;
- Data use, access and privacy;
- Cyber security and network resilience;
- IoT start-up innovation; and
- Platforms and Interoperability.

Comments on the Draft Code of Practice

We commend the Australian Government for the creation of the draft Code of Practice, and for its close alignment with the UK Government's code of practice. We believe it is important that such codes are aligned across the five-eyes nations.

In this section we provide feedback on the draft Code of Practice.

Security of the overall (end-to-end) IoT system architecture

The draft Code of Practice identifies four generic actors: Device Manufacturers; Service Providers; Mobile Application Developers; and Retailers. While we agree with the Department of Home Affairs that this is the correct set of actors for responsibility for IoT security, we are concerned that this may overly simplify the perceived architecture of an IoT solution.

Take for example, a smart toy capable of "listening" to a child and responding with return speech. Speech recognition processing is well beyond the computational capabilities of a battery powered child's toy. In this scenario, an audio recording is sent to the cloud for processing and for the application of AI to create an appropriate response. Likewise, a Smart Home solution will comprise several devices, sitting behind a hub which itself is behind a home gateway connecting the consumer via the nbn or mobile network to their retail service provider. This layered architecture may prevent software updates (Principle 3) of the end devices where they are not directly visible to and protected from directly communicating over the internet.

To meet consumers' expectation of security, the full end-to-end architecture of the service needs to be assessed. We recommend adding a new principle to the Code of Practice requiring the IoT Service Provider (and possibly Mobile Application Developers) to map the full end-to-end architecture of the service/solution and assess each point for security. Ultimately, there should be one single actor accountable for performing this task and ensuring the end-to-end security of the service/solution.

The **IoT Reference Framework**[3]**,** developed by the IoTAA, is an excellent resource for identifying all the actors in an IoT solution, including aspects such as third-party cloud data storage providers, providers of service such as speech recognitions and AI capabilities.

Greater clarity on responsibilities

We recommend some principles in the code would benefit from greater clarity of the roles and responsibilities of the various actors in consumer IoT applications.

Take Principle 3, "Keep software securely updated" as an example. It may not be possible for a device manufacturer to update software in a device where that devices sits behind a hub or gateway (such as a Smart Home), as the device may not be openly visible across the internet. This therefore requires Device Manufacturers and IoT Service Providers to work together to enable timely and secure updates to multi-layered IoT offerings such as Smart Homes, tracking/locator services and some smart toys.

[3] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

We recommend the Code of Practice is amended to clarify that in many cases it is expected that multiple actors in an overall IoT solution will be required to work collaboratively together to implement the principles in the Code of Practice.

Do not inadvertently mandate forced firmware upgrades

Principle 3 says "*Software (including firmware) on IoT devices … should be securely updatable*." We understand this to mean that where the capability exists in an IoT device or solution for software and/or firmware to be updated, then it must be done securely, and we support this.

However, we caution against inadvertently creating a mandate that all devices, regardless of their function or use, should have the ability to be updated. Any device capable of accepting either a software or firmware update remotely, has an increased attack surface. This then requires appropriate levels of security to prevent rogue actors updating the device or solution, thus adding complexity and cost.

We acknowledge that Principle 3 contemplates "constrained devices" (devices that cannot physically be updated), demonstrating the Department is aware that some devices can never be updated (potentially making them more secure). In the same way Principle 7 on communication security includes the phrase "*appropriate to the properties of the security technology and usage*" in acknowledgement that some devices (e.g. a weather sensor), we suggest words are added to the first sentence of Principle 3 to say "… *should be securely updatable* ***appropriate to the properties of the security technology and usage***."

Supply chain security

According to the US National Institute of Standards and Technology (NIST), "*Cyber supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cyber supply chain.*"[4]

Cyber Supply Chain Risk Management C-SCRM for IoT is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. Weaknesses in the supply chain can lead to security issues in an IoT solution or devices.

We recommend adding a new principle to the Code of Practice requiring the IoT Service Provider to adopt a cyber supply chain risk management framework. This should be in accordance with ISO28000[5].

[4] https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management
[5] https://www.iso.org/standard/44641.html

IoTAA's Security Trust Mark (STM) Scheme

Voluntary codes can be effective mechanisms to set minimum industry standards of behaviour and compliance and have a very positive track record in the telecommunications sector in Australia. However, ultimately a voluntary code of practice is just that, *voluntary*. While we certainly do not propose that the code should be made mandatory (complete with regulatory oversight), IoTAA are of the view that the uptake and efficacy of a voluntary code can be substantially increased through the introduction of compelling commercial incentives to adopt the code. This can best be achieved through the creation of a Security Trust Mark (STM) scheme. Trustmark schemes have the added benefit of providing consumers confidence that the devices and services they purchase have been tested recently, and that the vendor's claims about the security of the device have been tested and substantiated – and that security measures beyond the minimum have been implemented, **which would support better competition for higher levels of IoT security**.

The IoTAA's STM scheme is a transparent and accredited industry operated scheme that is critical to Australia's cyber security. In developing the STM scheme, IoTAA has engaged with Government and has welcomed feedback and input over recent years.

The objective of the STM scheme is to meet the needs of government and industry for cost effective and efficient functionality claims testing and clear labelling of the security of IoT devices or services. The STM scheme is aimed primarily at IoT devices and services to meet information assurance requirements at the higher impact levels, for purchase by central government and the wider public sector, particularly in the areas of transport, health, agricultural, industrial control systems, and smart cities.

While the certification program itself is ultimately self-funding, financial assistance will be required for the initial phases required to launch, administer and market the scheme to accelerate and broaden adoption; and to maintain and update the scheme as IoT and technologies evolve. The STM scheme is industry developed, and to date, has relied on the good-will of volunteers, albeit experts in their fields, donating their time and effort to build the program.

Our thesis is that through the STM scheme, government, industry and the community will contribute to building a more resilient and secure national IoT infrastructure. This will be achieved by consumers, businesses and government having access to, and confidence in STM evaluated products; enabling them to ascertain which vendors and products are currently certified and their status at any given time. This in turn sends a strong signal to vendors of IoT products and services to build in security into their products and practices, and to advertise their security compliance as a competitive advantage.

The government, by both publicly endorsing the scheme and taking the lead in prioritising procurement for STM accredited products and services would provide a powerful catalysing effect in encouraging and assisting industry adopt and demonstrate good IoT security practice.

Key elements of our scheme that differentiate it from other schemes:

- Verification is against the **vendor's security claims**, with a minimum baseline required set (i.e. either legislated such as in California – although, we recommend against this - or baseline defined by organisations such as ENISA). This overcomes a 'one-size-fits-all' approach to IoT security, while still maintaining a minimum-security baseline. It also allows

for different testing at the different layers in the Reference Framework covering any IoT device.

- A Decision Authority (DA) oversees the scheme, including administration, the accreditation of the test facilities (ATFs), technical oversight, review of Initial Claims Documents (ICDs), review of ATF letter of recommendations, the issuance of certifications and the publication of the Evaluated Products List (EPL) enabling the vendors to label their products.
- Testing under the scheme is performed by a **third-party** Accredited Test Facility (ATF) engaged by the vendor. This is an important differentiator compared to other certification schemes which operate on the basis of self-assessment and compliance.
- The vendor and the ATF jointly work to develop an ICD which includes details about the product seeking certification, the vendor's security claims and a draft testing methodology. This ICD is then submitted to the DA for review and approval.
- Once the ICD is approved the ATF executes the evaluation and, within 30-days, provides to the DA a full test report, a summary test report and a letter of recommendation.
- The DA reviews the documents and decides on a fail or pass and issuance of a certification.
- Once certified the vendor's product, firmware and any other relevant particulars are published on the EPL along with the summary test report.

Security is an ever-moving target, and a product that meets its security claims one day may be vulnerable the next. Therefore, the STM scheme has been designed to ensure there is a mechanism in the certification baseline that vendors have for mandatory notification of vulnerabilities. In our STM scheme, once the DA is aware there is a vulnerability, i.e. reported via a source such as a Cyber Emergency Response Team (CERT) alert, the vendor will be contacted and their product certification will be placed into a suspended status until the vulnerability has been addressed and the product regressively tested and verified by the vendors' ATF and a letter issued to the DA by the ATF confirming this.

Do not legislate to make accreditation schemes mandatory

While there are moves in the United States and the United Kingdom to introduce accreditation schemes into law, we do not recommend mandating schemes through legislation because technology, and especially its security, is a rapidly moving landscape. Before standards are set, let alone legislated, the technology has moved and those with malicious intent have discovered other vectors of attack, thereby rendering the standards and associated legislation redundant. Attackers do not follow standards or commercial timeframes. Furthermore governments, policies and resources change. An industry led voluntary certification and labelling scheme can endure such fluctuations and deliver consistency over time that vendors, consumers, business and governments require.

Conclusion

We commend the Australian Government for the creation of the Draft Code of Practice, and for its close alignment with the UK Government's code of practice.

We have provided feedback on the Draft Code of Practice, including recommending the addition of a principle to cover security of the overall (end-to-end) IoT system architecture, avoiding inadvertently mandating firmware upgrades and the addition of a principle covering supply chain security.

We have also proposed the introduction of our STM labelling scheme is the best way to ensure uptake and efficacy of the Code of Practice by providing a compelling commercial incentive for vendors and practitioner to ensure good IoT security practice and at the same time, providing consumers and businesses confidence in the devices and solutions they are purchasing.

Appendix: IoTAA Strategic Plan to Strengthen Security

In September 2017, the IoTAA released version 4 of its **Strategic Plan to Strengthen IoT Security in Australia**. The plan outlines eight key items and describes proposed policy, stakeholders and steps required to implement them. Four of the eight were identified for priority focus, and while good progress has been made, more remains to be done.

The second of the eight key items, and the one we focus on here, is to:

> **Develop, implement and promote an IoT product security certification program: an independent IoT product security claims-testing, evaluation and certification "Trust Mark" program for demand-side assurance.**

Importantly, it is not just about the individual IoT devices; it is the full end-to-end solution that requires security consideration. Each IoT deployment is unique and can be quite diverse. Take a smart city as an example. It would be impossible to define a traditional IT security architecture for such an environment given the complex array of scenarios under the smart city umbrella. Smart cities embrace everything from environmental monitoring (air and water quality), smart solutions to reduce energy consumption (smart streetlights and monitors to detect when bins need emptying), to transport, road and parking monitoring. Each of these individual scenarios can be ecosystems in their own right, with separate networks and platforms implementing individual scenarios.

That's why we have developed and released the **IoTAA Reference Framework**[6] and **Application Guide**[7] – so IoT practitioners, vendors, solution designers, businesses and even consumers could see all the layers where security, privacy and safety need to be considered. Users of the framework can build a model of their ecosystem and wrap governance, risk, compliance and regulatory requirements around it, so that each element of the IoT ecosystem can be viewed from the perspective of any of the stakeholders.

In addition to the Reference Framework, we have completed the design for the **Security Trust Mark (STM) scheme**, and it is ready for the education, distribution and implementation phases. The STM is an industry led initiative which uses market signals and responses to drive vendor and user behaviour (e.g. somewhat like the ANCAP or Energy Rating marks).

More detail on the scheme is in the section below titled IoTAA's Security Trust Mark (STM) Scheme. But firstly, a review of the landscape of security guidelines and schemes.

[6] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf
[7] http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-Application-Guide-v1.0.pdf