Summary literature review of industry recommendations and international developments on IoT security

PETRAS IoT Hub

Leonie Tanczer
John Blythe
Fareeha Yahya
Irina Brass
Miles Elsden
Jason Blackstock
Madeline Carr
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>2</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>INDUSTRY RECOMMENDATIONS</td>
<td>4</td>
</tr>
<tr>
<td>INTERNATIONAL DEVELOPMENT ON IOT SECURITY</td>
<td>6</td>
</tr>
<tr>
<td>CONCLUDING REMARKS</td>
<td>9</td>
</tr>
<tr>
<td>OVERVIEW OF PRINCIPLES AND BEST PRACTICE FOR IOT SECURITY</td>
<td>11</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>14</td>
</tr>
</tbody>
</table>
INTRODUCTION

The Department for Digital, Culture, Media and Sport (DCMS) commissioned the PETRAS IoT Research Hub, a consortium of nine leading UK universities that work together to explore critical issues in privacy, ethics, trust, reliability, acceptability, and security of the IoT to conduct two separate literature reviews. The first, on industry recommendations for government to improve IoT security and the second, on the current international developments around IoT security. There were two aims to these reviews: (i) identify the key themes emerging from the literature and (ii) identify international consensus around core Security by Design principles for the IoT.

In this report, we first summarise the emerging themes from the two reviews, then provide recommendations for government and finish with an overview of the consensus around Secure by Design principles.

---

1 This literature review represents an analysis of publicly available reports made by industry associations and international organisations. It does not capture the independent position of industry or international experts expressed in other primary research currently conducted.
INDUSTRY RECOMMENDATIONS

We conducted a scoping literature review between May and July 2017\(^2\) and included\(^3\) industry reports that provided recommendations for government action.\(^4\) Analysis of the industry reports indicated a number of key issues of focus including the role of regulation, trust labels and standards. Below, we present an overview of the key themes that emerged from the review.

Regulation vs. Self-Regulation
There was general consensus that industry was in favour of self-regulation to allow for growth and innovation in IoT. An incremental and flexible approach was preferred to address evolving threats. Conversely, independent security researchers such as Bruce Schneier were often in favour of legally-binding rules and regulations, arguing it is the best option for dealing with the increasing cyber-physical convergence that IoT brings.

Certification and Trust
The role for a trust label to inform consumer decision making was mixed across industry players. Some were in favour, as it provides a visible means for consumers to understand the security of a product. These players were in favour of a label that was: flexible (to allow for online and offline communication), co-designed by government and industry, and aligned with international standards. However, there was recognition amongst industry that cybersecurity is not as easily measurable as

\(^2\) Final amendments to this scoping literature review were incorporated in November 2017.
\(^3\) Privacy issues were excluded from the review, although they may require further investigation in the future.
\(^4\) Reports from the following institutions were reviewed: Alliance for Internet of Things Innovation (AIOTI), Cloud Security Alliance, Consumer Technology Association, Ericsson, HP, Infineon, NXP, STMicroeletronics, European Union Agency for Network and Information Security (ENISA), Intel, Internet Society, McKinsey Global Institute, Microsoft, Ofcom, Online Trust Alliance, Software and Information Industry Association, and Telecommunications Industry Association.
other labelling schemes (such as energy) and expressed concerns around what the label would actually represent and who would carry out the certification.

**Training and Capacity Building**
Industry was in favour of heightening consumer awareness of the risks associated with IoT and emphasised the need for educational investment in school and universities curricula and wider training programs.

**Standardisation**
Industry want standards that are open, voluntary, collaborative and consensus-based. Most reports were in favour of industry working collaboratively with government to develop standards, but there was concern that too much government intervention is this space may impact on interoperability and routes to market.

**Funding Research**
A few industry reports discuss the need for government to fund future research on IoT security and to develop industry standards.

**Promote Security by Design Principles and Best Practice**
Industry wants government to promote security by design but also to recognise that more sector-specific product development and risk assessment guidelines will be required.

**Public-Private Partnerships**
To address the issue of IoT security, industry expressed the view that there needs to be ongoing collaboration between the public and private sector in order to drive good practice.
INTERNATIONAL DEVELOPMENT ON IoT SECURITY

We conducted a scoping literature review between September and October 2017\(^5\) and included\(^6\) reports from the leading eleven international fora\(^7\) that are shaping the global governance and policy conversations about the security of the IoT.

Our analysis reveals that there have been some nascent international conversations about the policy implications of the IoT over the last five years. Debates around issues such as security by default, (self-)regulation, standardisation and security measures have emerged, though the content and nature of these debates varies and they are not always inclusive of a wide range of stakeholders. Below, we summarise ten of the most commonly shared themes.

\[\text{Security by Default/Design Measures}\]

Security by default and security by design are concepts that are frequently used interchangeably. Measures for secure by default/design are prevalent across various international organisations, although there is a lack of established and internationally agreed global IoT security principles, offering opportunities for future world-wide collaborations. A recent development in this space is the publication of ENISA’s

\[\text{Key Themes}\]

\[\text{Security By Default}\]

\[\text{Collaboration, PPP and Consensus}\]

\[\text{Data Management and Transparency}\]

\[\text{Standardisation}\]

\[\text{Liability}\]

\[\text{Regulation vs. Self-Regulation}\]

\[\text{Training and Capacity Building}\]

\[\text{Procurement}\]

\[\text{Certification and Trust}\]

\[\text{Research and Development}\]

\[\text{Privacy and trade-related issues were excluded from the reviews, although they may require further investigation in the near future.}\]

\[\text{Reports from the following institutions were reviewed: European Commission, EU Article 29 Working Party, European Union Agency for Network and Information Security (ENISA), Alliance for the Internet of Things Innovation (AIOIT), Organisation for Economic Co-Operation and Development (OECD), World Economic Forum (WEF), Association of Southeast Asian Nations (ASEAN), International Organization for Standardization (ISO), International Telecommunication Union (ITU), GSM Association (GSMA), and Institute of Electrical and Electronics Engineers (IEEE).}\]

\[\text{Final amendments to this scoping literature review were incorporated in December 2017.}\]
Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures in which detailed security measures and good practices are outlined.

**Balance between Regulation and Self-Regulation**
International organisations’ focus of attention is currently on the enforcement of existing laws and regulations in opposition to the introduction of new legislation. Self- and a mix of voluntary and legally-binding regulations are perceived as the best near-term options to facilitate the growth of the IoT. The update, adaption, and harmonisation of existing regulations is considered necessary in areas that stand in the way of IoT innovation (e.g., free flow of data, motor vehicle, aviation, workplace regulations, and insurance).

**Certification and Trust**
Contrary to the mixed review by UK industry (above) the certification and labelling of IoT products and services was generally referred to in the international literature as potentially advantageous for both users and manufacturers and as a means to enhance users trust. Certification mechanisms are primarily discussed at the EU level and within technical organisations such as the ITU and IEEE. The recently proposed EU certification framework is a first attempt to explore compliance of specified requirements. It is recommended on a voluntary basis, and may provide a worked example of debates surrounding potential benefits and challenges.

**Standardisation**
The development and promotion of open, internationally-recognised, market-driven standards and interoperable solutions is emphasised across all analysed institutions. The IoT security standards landscape is currently highly fragmented, with several international industry alliances proposing de facto standards and (self-)certification schemes. Although there are signs of convergence towards a set of core technical and organisational requirements for IoT security among these organisations (see Table below), gaps still persist. The need for standards alignment offers an opportunity for the UK government to play a leading role in international efforts to deliver security and interoperability of IoT devices and services.

**Procurement**
IoT procurement is not a focus point of the analysed international organisations. However, there are some national developments such as the US proposed *Internet of Things (IoT) Cybersecurity Improvement Act of 2017*. The nature of the global supply chain and the imperative of coordinating international procurement poses an opportunity for the UK government to foster these debates and best practices globally.

**Training and Capacity Building**
The analysed international organisations highlight that IoT specific training and capacity building initiatives underpin security by default measures and can help create an overarching culture of security necessary for the emerging IoT ecosystem.

**Liability**
Liability issues are primarily discussed on the EU level and have been subject to substantial assessments and scrutiny by bodies such as the European Commission and AIOTI. AIOTI considers the current legislative framework and existing safety and
liability regime as flexible enough to sustain ongoing IoT developments, although clarification on particular principles could be supported through policy documents and guidance. Several organisations highlight that a review and potential change to product safety and liability rules should occur as the IoT develops.

**Data Management and Transparency**
There is a collective demand by international organisations to ensure user transparency, access management control, and consent from the time of purchase throughout the lifecycle of IoT services. Data security and data management are relevant factors for a potential IoT certification scheme.

**Research and Development**
International organisations are actively involved in IoT R&D initiatives, fund and support cross-country projects and foster a multi-stakeholder engagement in this space.

**International Collaboration, Consensus, and Public-Private Partnerships**
Cross-government and cross-industry collaboration are perceived to be needed not only to reach consensus on IoT security and security by default guidelines, but also to facilitate information exchange and identify needs and perspectives of other stakeholders. In particular the World Economic Forum emerges as a suitable platform that possesses a unique ability to focus the attention of decision-makers both in government as well as across industry, and to provide a forum for IoT security multi-stakeholder cooperation. The relevance of CSIRTs for the sharing of best practices and information on IoT vulnerabilities was highlighted across various international organisations.
CONCLUDING REMARKS
It is clear that industry recognise the importance of securing the Internet of Things (IoT) and are keen to work alongside the government in their efforts. Industry are concerned that too much intervention may impact on innovation and government should allow industry the opportunity to self-regulate. Industry are keen to see developments in standards, the promotion of security by design, capacity building and exploring the role of trust marks.

Discussions in international organisations around IoT security are relatively immature. There are therefore substantial opportunities for the UK to take the lead in shaping the future governance of the IoT. It is unclear how soon a viable international mechanism, or consensus, will coalesce around the key themes identified in this report. If the UK wishes to influence the formation of IoT working groups, best practices and guidelines, there is currently a window of opportunity to take the lead. The UK’s expertise in ICT procurement through its Cyber Essential Scheme and its experience of promoting an environment for self-regulation may therefore be suitable starting points to foster international discussions.

RECOMMENDATIONS

Balance Between Regulation and Self-Regulation

There is an international consensus on promoting self-regulation, although there is increasingly a mix of positions, some quite in favour of regulation. The UK would be well placed to take a principal role in developing a global approach to regulation of future IoT systems, given its expertise in the use of market-driven, self-regulatory approaches.

Standardisation

Internationally and within industry, there is a general recognition of the need to promote open, internationally recognised, market-driven standards and interoperable solutions to support innovation and growth of the IoT. There is an opportunity here for the UK to actively engage and/or take a leading role in the development of these standards using its strong reputation and links in the international standardisation community.

Training and Capacity Building

The global position on training and capacity building closely aligns with the UK skills agenda. This provides an opportunity for the UK to mobilise its world-leading education sector to provide both the national need and export to the global market.

International Collaboration, Consensus, and Public-Private Partnerships

There is clearly an opportunity to lead on the development of international cooperation, standards, and regulation and to guide the advancement of international agreements that will be necessary to ensure a safe and secure IoT. There is currently a lack of
consensus and leadership in most of the international organisations on these subject matters, with the World Economic Forum seeming to be the most obvious forum where all key players are engaged. This, together with the OECD and potentially the WTO, would likely be the best route to influence the international agenda. There is an opportunity for the UK to direct and shape this debate.

Certification and Trust

The proposed EU cybersecurity certification scheme may form the basis for future international discussions in this space. While the certification process is meant to be of voluntary nature, the EU proposal includes an obligation for member states to implement the institutional requirements to support the scheme at the national level. This expectation – and concerns such as the measurability of cybersecurity, the consistency and equivalence of evaluation methods as well as the enforceability of certificates across the entire lifecycle of IoT products and services – continue to be the subject of debate.

Over the next year, the UK’s ongoing involvement in the negotiations on the certification scheme provides a potential forum for advancing the UK’s leadership in this space. The UK has an opportunity to drive the development of specified certification criteria and may, in the course of these negotiations, explore alignment with self-governance and standardisation agendas pursued elsewhere.
OVERVIEW OF PRINCIPLES AND BEST PRACTICE FOR IoT SECURITY

Presented below is a tabular summary of the key overarching principles around best practice for IoT security. We have included recommendations that have been referenced at least twice in reports and use the following colours to indicate frequency:

- **Green** – Referenced in 10 or more reports
- **Orange** – Referenced in 5-10 reports
- **Yellow** – Referenced in less than 5 reports

<table>
<thead>
<tr>
<th>Overarching principle</th>
<th>Specific recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strong authentication</strong></td>
<td>Strong authentication by default (ship with password protection)</td>
</tr>
<tr>
<td></td>
<td>No default passwords</td>
</tr>
<tr>
<td></td>
<td>Follow accepted and secure password reset processes</td>
</tr>
<tr>
<td></td>
<td>Use two-/multi-factor authentication</td>
</tr>
<tr>
<td></td>
<td>Use certificates securely</td>
</tr>
<tr>
<td></td>
<td>Consider biometrics for authentication</td>
</tr>
<tr>
<td></td>
<td>Salt, hash and/or encrypt credentials</td>
</tr>
<tr>
<td></td>
<td>Require “strong” passwords</td>
</tr>
<tr>
<td></td>
<td>Reaffirm authentication throughout time of access</td>
</tr>
<tr>
<td><strong>Software updates</strong></td>
<td>Routine, reliable secure updates from vendors providing firmware and software patches</td>
</tr>
<tr>
<td></td>
<td>Cryptographic checks to allow updates from an authorized source – signed/verified from trusted source</td>
</tr>
<tr>
<td></td>
<td>Mechanism for automatic secure software updates</td>
</tr>
<tr>
<td></td>
<td>Fall back/rollback option</td>
</tr>
<tr>
<td></td>
<td>Thoroughly tested updates</td>
</tr>
<tr>
<td></td>
<td>Ship with most up-to-date stable version</td>
</tr>
<tr>
<td><strong>Device functionality</strong></td>
<td>Build in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality</td>
</tr>
<tr>
<td></td>
<td>Offer some functionality or notify user if internet connectivity/cloud back end fails</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td>Easy to find and understand policies covering privacy and security, support policies, data retention</td>
</tr>
<tr>
<td><strong>Disclosures and transparency</strong></td>
<td>Empower user to understand what is going on with the device and the data it is sharing</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Disclose duration of product support including what to expect at end of lifespan</td>
</tr>
<tr>
<td></td>
<td>Disclose what sensitive data is collected and how it is used</td>
</tr>
<tr>
<td></td>
<td>Disclose what happens to data when ownership is transferred</td>
</tr>
<tr>
<td></td>
<td>Disclose what will happen to device functionality when services fail</td>
</tr>
<tr>
<td></td>
<td>Disclose what happens when user declines/opts out of policy and the consequences of this to product functionality</td>
</tr>
<tr>
<td></td>
<td>Disclose product capabilities and limitations (e.g. encryption, data communication)</td>
</tr>
<tr>
<td><strong>Reset mechanism</strong></td>
<td>Provide a mechanism to reset to manufacturer state</td>
</tr>
<tr>
<td></td>
<td>Support label – to help authorized operator identify device and find support information</td>
</tr>
<tr>
<td></td>
<td>Manufacturers should provide clear options on contacts for support</td>
</tr>
<tr>
<td></td>
<td>Mechanism for dissemination of information about software vulnerabilities or other issues to consumer</td>
</tr>
<tr>
<td><strong>Vulnerability reporting and disclosures</strong></td>
<td>Report discovery and remediation of vulnerabilities that pose threats to consumers</td>
</tr>
<tr>
<td></td>
<td>Provide a vulnerability report process</td>
</tr>
<tr>
<td><strong>Cryptography protocols and best practices</strong></td>
<td>Encryption by default, especially in instances where sensitivity of data is being collected</td>
</tr>
<tr>
<td></td>
<td>Use best practice cryptography protocols</td>
</tr>
<tr>
<td><strong>Secure the supply chain and associated services</strong></td>
<td>Secure the supply chain, including raw circuit board components e.g., cryptographic tokens, read only memory (ROM), firmware, and other core attributes of an embedded system</td>
</tr>
<tr>
<td><strong>Minimum requirements necessary</strong></td>
<td>Design devices to minimum requirements necessary required for operation</td>
</tr>
<tr>
<td>Compliance and risk assessment</td>
<td>Conduct security and data compliance risk assessments including data classification and security across the data lifecycle</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secure development</td>
<td>Undergo a secure development process (such as threat modelling, inventory of codes)</td>
</tr>
<tr>
<td>Test and harden devices</td>
<td>Test and harden devices</td>
</tr>
<tr>
<td>No backdoors or known vulnerabilities</td>
<td>Do not ship with backdoors or known vulnerabilities</td>
</tr>
<tr>
<td>User choice</td>
<td>Provide opt-in/opt-out requirements for IoT devices</td>
</tr>
<tr>
<td></td>
<td>Provide user or proxy option to delete personal data on company services upon end of service with company</td>
</tr>
<tr>
<td></td>
<td>Request users consent to share personal data with third parties</td>
</tr>
<tr>
<td></td>
<td>Allow for data control by the user at any point of the lifecycle</td>
</tr>
<tr>
<td></td>
<td>Provide privacy-friendly default settings</td>
</tr>
<tr>
<td></td>
<td>Provide controls to edit privacy settings</td>
</tr>
<tr>
<td></td>
<td>Provide choice for data collected beyond what is needed for device operation</td>
</tr>
<tr>
<td>Physical security</td>
<td>Implement measures to help prevent physical tampering of devices and physical access to devices</td>
</tr>
<tr>
<td>Logging</td>
<td>Secure event logging for aiding fault and security management</td>
</tr>
<tr>
<td>Secure device boot</td>
<td>Trusted/secure boot sequence minimises the risk of rogue code being run at boot time</td>
</tr>
<tr>
<td>Network segmentation</td>
<td>Establish smaller local networks using VLANs, IP address ranges to create security zones controlled and connected by a firewall</td>
</tr>
</tbody>
</table>
REFERENCES


AIOTI WG03, “High Level Architecture (HLA; Release 3.0),” Alliance for Internet of Things Innovation, Brussels, 2017.


AIOTI WG09, “Smart Mobility,” Alliance for Internet of Things Innovation, Brussels, 2015.


AIOTI, Cable Europe, and GSMA, “Joint Industry Statement: Enabling Europe to be the Future Leader in IoT and Innovation,” The Alliance for the Internet of Things Innovation, Brussels, 2017.


European Commission, “COM(2009) 278 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social


McKinsey Global Institute, “The Internet of Things: Mapping the value beyond the hype”, 2015.


