Standardising a Moving Target: The Development and Evolution of IoT Security Standards

Irina Brass  Leonie Tanczer  Madeline Carr  Miles Elsden  Jason Blackstock

Dept. of Science, Technology, Engineering & Public Policy
University College London, 36–38 Fitzroy Square, London, W1T 6EY, UK
{i.brass, l.tanczer, m.carr, m.elsden, jason.blackstock}@ucl.ac.uk

Keywords: IoT security standards, certification, compliance.

Abstract
The standards landscape for IoT security is currently developing in a fragmented manner. This paper provides a review of the main IoT security standards and guidelines that have been developed by formal standardisation organisations and transnational industry associations and interest alliances to date. The review makes three main contributions to the study of current IoT standards-development processes. First, governments and regulatory agencies in the EU and the US are increasingly considering the promotion of baseline IoT security requirements, achieved through public procurement obligations and cybersecurity certification schemes. Second, the analysis reveals that the IoT security standards landscape is dominated by de facto standards initiated by a diverse range of industry associations across the IoT ecosystem. Third, the paper identifies a number of key challenges for IoT security standardisation, most notably: a) the difficulty of setting a baseline for IoT security across all IoT applications and domains; and b) the difficulty of monitoring the adoption, implementation and effectiveness of IoT security standards and best practices. The paper consequently contributes to a better understanding of the evolution of IoT security standards and proposes a more coherent standards development and deployment approach.

1 Introduction
The Internet of Things (IoT) is receiving increasing attention from industry, policy makers, consumers and the media. A recent report commissioned by OFCOM – the communications regulator in the UK – estimated that the number of IoT connections in the UK will reach 155.7 million by the end of 2024, at an expected compound average growth rate of approximately 36% [1]. This growth can be explained by a number of factors, including the increased adoption of IoT consumer products, especially in the EU, the US and South-East Asia [2], as well as by the “business transformation” that IoT promises in terms of increased efficiency and revenue, risk management and costs reduction [3]. However, increased device connectivity and process integration have exposed new vulnerabilities in IoT device security, data integrity and system reliability. In 2016, compromised IoT devices located all over the world were used to produce the most powerful DDoS attack ever recorded against a DSN, at 1-TBps. This led security analysts at Cisco to conclude that security weaknesses in IoT devices and systems have brought about new attack strategies, coined as “Destruction of Service” (DeOS) [4]. IoT security is thus becoming central to businesses and the public sector. In 2017, Ovum found that “data security and privacy concerns”, “legacy IT infrastructure and systems” and “the lack of a robust business case” were reported as the top three barriers to the deployment of IoT [5]. IoT security standards, especially common and open standards, play a crucial role in lowering these barriers to acceptability, adoption and deployment of the IoT [6–8]. A recent survey conducted by the PETRAS IoT Research Hub, BSI and IoTUK showed (Figure 1) that public and private organisations use IoT cybersecurity standards for several reasons, most notably...
to achieve interoperability (22.9%), for regulatory compliance (18.3%), for certification purposes (14.5%) and for compliance with public tendering (14.5%) [9].

Policy makers, regulatory agencies and the industry are also increasingly agreeing that a baseline for IoT security is required to ensure data protection, service continuity and public safety [10–13]. Yet, given the diversity of IoT application areas and domains, what this security baseline should include and how it should be implemented and monitored, is still a matter for debate.

1.1 Scope of the Paper

This paper provides a review of the main trends in the development and evolution of IoT security standards to date. It aims to offer a detailed analysis of the extent to which standardisation efforts are leading towards the establishment of a baseline for IoT security in some of the most developed IoT markets [2], with particular focus on the UK, EU and US. Standards are defined here broadly to include principles, guidelines, codes of practice and technical specifications that are developed by public, private and not-for-profit entities, including government departments and agencies, national standardisation bodies, industry alliances and associations [1].

Although the paper makes reference to some of the key IoT security standards for specific domains, such as connected autonomous vehicles, medical devices and industrial applications, it does not provide a comprehensive review of standards for each IoT application area. Instead, it focuses on what industry and the public sector have currently identified as technical and organisational specifications for default IoT security.

1.2 Methodology

This paper summarises findings of an ongoing study conducted by the Standards, Governance and Policy (SGP) team of the PETRAS IoT Research Hub, which examines the dynamics between voluntary standards and mandatory regulatory frameworks for ensuring the adoption of a baseline of IoT security.

The research is underpinned by methodological triangulation based upon:

1. Desk-based research of IoT security guidelines, codes of practice and technical specifications, developed by public, private and not-for-profit organisations;

2. An online ‘Cybersecurity of the Internet of Things Standards Survey’, exploring the use and implementation of IoT security standards, conducted by PETRAS IoT, BSI and IoTUK (March 2017);


A fourth stage, consisting of a series of semi-structured interviews with key standards development organisations, trade associations and UK regulatory bodies, is currently being conducted in order to gather more evidence on the barriers to the adoption and implementation of IoT security standards.

1.3 Key Findings

This paper puts forward the following findings, as discussed in the sections below:

1. While the policy and regulatory status quo is still based on a ‘light touch’ approach to standardising IoT security, governments and regulatory agencies in the EU and the US are increasingly considering the promotion of baseline IoT security requirements, achieved through public procurement obligations and cybersecurity certification schemes.

2. This policy shift can be seen as a response to the slow pace of IoT security self-regulation achieved by the market. Specifically, the IoT security standards landscape is dominated by de facto standards, developed by a diverse range of industry alliances and associations across the IoT ecosystem. Although there is some degree of convergence towards baseline specifications for IoT security across these schemes, there is also considerable competition between them, evident in the parallel development of industry-led testing and certification schemes.

3. Two main gaps in the development of a commonly agreed baseline for IoT security can be identified. First, there is clear divergence across the reviewed standards on the basic scope and relationship between IoT security, safety, consumer trust, trustworthiness and system integrity. Second, at present, there is limited information about the adoption, implementation and review rate of government and industry-led standards for IoT security, which makes their effectiveness difficult to monitor and evaluate.

2 Policies, Regulatory Frameworks and High-Level Guidelines for IoT Security

The policy landscape for IoT security is currently mixed, especially across the three regions that are estimated to “represent 67% of the overall IoT installed base in 2017” – Western Europe, North America and East Asia [2]. Over the past years, governments and regulatory agencies across these regions have
promoted a ‘light touch’ approach to securing the IoT, issuing a combination of non-binding high level guidelines and sector-specific recommendations. In other words, governments have predominantly utilised their advisory and steering powers, rather than their rule-making capacity to promote IoT security.

In the UK, this approach was detailed in the ‘Cyber Security Regulation and Incentives Review’ conducted by HMG Department for Digital, Culture, Media and Sport (DCMS), which stated that “for now, [the UK] Government will not seek to pursue further general cyber security regulation for the wider economy over and above the GDPR” [15]. Simultaneously, the UK National Cyber Security Centre (NCSC) has developed a set of eight principles for ‘secure by default’ devices and systems, including security by design, transparency and usability [16].

This steering approach adopted by the UK Government does not mean that IoT data integrity and security are fully unregulated [17–19]. At present, several regulatory frameworks apply to aspects of IoT data integrity and security, such as the forthcoming General Data Protection Regulation (GDPR 2016/679) and the Network and Information Systems Directive (NIS 2016/1148). These require data protection impact assessments or cybersecurity risk assessments for organisations that use new technologies or provide essential services that result in a high risk to the rights and freedoms of individuals or the integrity of critical infrastructure. In addition, security guidelines for specific IoT applications have been put forward by other UK Government departments, such as the ‘Key Principles of Cyber Security for Connected and Automated Vehicles’ developed by HMG Department for Transport [20].

A similar policy landscape has taken shape in the US. In 2016, the US Department of Homeland Security produced a set of non-binding ‘Strategic Principles for Securing the IoT’, proposing an integrated, end-to-end approach to securing the IoT based on security by design as well as continuous product, system and business lifecycle risk assessment [21]. In addition, specialised agencies in the US have also promoted non-binding cybersecurity guidelines and recommendations for automated vehicles [22] and for medical devices [23], [24].

### 2.1 Mandating IoT Security?

Recently, the policy landscape for IoT security has undergone important changes that raise questions about the extent to which a baseline for IoT security could be driven by new legislative and regulatory initiatives. Two major developments are pointing in this direction: a) two legislative proposals in the US and the EU; and b) the increasing role of formal standardisation, communications and cybersecurity agencies in promoting detailed guidelines that apply to IoT security.

In August 2017, a bill entitled the ‘IoT Cybersecurity Improvement Act’ was introduced in the US Senate, proposing “minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes” [25]. Currently in referral to the Committee on Homeland Security and Governmental Affairs, the proposed bill requires written proof of third-party security certification in public acquisition contracts and procurement of Internet-connected devices (Sec 3.1 A(i)).

In September 2017, the European Commission proposed a regulation that would formally establish the European Union Agency for Network and Information Security (ENISA) as the ‘Cybersecurity Agency’ of the EU. ENISA is tasked with several cybersecurity coordination and operational functions, including the preparation of an initially voluntary cybersecurity certification scheme based on three assurance levels (‘basic’, ‘substantial’, ‘high’) [26].

The proposed legislations make reference to key security principles and technical specifications which have been put forward by formal standardisation, communication and cybersecurity agencies in the US and the EU. These guidelines are increasingly converging towards a set of minimum specifications for IoT security at the device and at the system level (Figure 2).

At device level, minimum security requirements such as vulnerability disclosure, upgradability and service lifecycle management are proposed by a number of public agencies in the US, including the National Telecommunications and Information Administration (NTIA) [27] and the Federal Trade Commission (FTC) [28]. At the system level, authentication, authorisation, access controls, cryptographic key management as well as integrity management are proposed by the US National Institute of Standards and Technology (NIST) [29] and ENISA [30]. In addition, these agencies have set up several multistakeholder engagement processes for the continuous development and review of baseline requirements for security in IoT devices and critical infrastructure domains [11], [31–33].

Overall, the policy landscape in the UK, EU and US reveals increased convergence towards a baseline for IoT security. However, given that the proposed guidelines are supported by non-

![Fig. 2: Converging Principles for IoT Security in Legislations and High-Level Guidelines (EU, US)](image-url)
binding frameworks and recommendations, it can be easily argued that a ‘light touch’ approach to IoT security continues to be the predominant policy option, at least at present.

While differences between the certification schemes in the US and the EU remain – with the US bill proposing a more flexible, contract-by-contract ‘written certification’ requirement (Sec 3.1 (i)), and the EU regulation proposing a more centralised scheme developed by ENISA (Art 44) – these developments could pave the way towards the emergence of an international baseline for IoT security [13].

3 Industry Codes of Practice, Technical Specifications and Certification Schemes

The recent policy shift towards the establishment of a baseline for IoT security via new legislation and certification can be, at least in part, explained by the fragmented and increasingly competitive landscape for IoT security standardisation.

The PETRAS IoT ‘Cybersecurity of the Internet of Things Standards Survey’ confirmed the fragmented standards landscape for IoT security [9]. When asked about their awareness of both formal and de facto standards\(^2\) that apply to IoT cybersecurity, respondents showed limited convergence towards a predominant standard (Figure 3). However, the ISO/IEC 27000 series of information security management standards emerged as most popular.

With regard to their awareness of de facto standards, the respondents identified the GSM Association (GSMA) IoT Security Guidelines [34–37] and the Open Web Application Security Project (OWASP) IoT Security Guidance [38–39] as the most well-known standards related to IoT security.

The distribution of responses in Figure 3 underlines pressing issues about IoT security standardisation. First, although relevant for IoT security, the ISO/IEC 27000 series of information security management standards does not apply to all components of the IoT ecosystem. There is, thus, a clear gap in the development of formal security standards specific to the IoT which take into account both device and end-to-end security. Second, formal standards development organisations (SDOs) have to clearly highlight the extent to which their activities cover all aspects of IoT security and the extent to which established standards, such as the ISO/IEC 27000 series, apply to the IoT.

3.1 Formal Standards Relevant to IoT Security

At present, the development of formal standards pertaining to IoT security is relatively slow moving. There are at least two reasons that explain this pace of development. First, formal standardisation processes are generally longer than market-driven ones, due to the highly institutionalised approval and review process. In addition, formal standards development in regional and international organisations is more politicised, due to the complex voting structure (e.g. national weighted voting in ETSI) or the competitive promotion of national standards for international adoption (e.g. ISO or ITU).

Second, the topology of the IoT ecosystem (i.e. edge, connectivity, services) as well as its large application area (e.g. consumer goods, critical infrastructure and essential services) challenge the current organisation of formal standards development activities. This can be observed through the development of formal standards in the International Organisation for Standardisation (ISO) [40–43] and the national and regional standardisation organisations [44] that have partnered to create oneM2M [45] (Figure 4).

In addition, the formal standards landscape is complicated by standardisation activities pertaining to specific IoT application areas, such as the development of security standards for smart grid systems in CEN/CENELEC (EU) [46] or NIST (US) [47].

Thus, although formal standardisation processes relevant to IoT security are advancing, it is difficult to say that a baseline for IoT security has so far been achieved in formal SDOs. As seen in the case of ISO (Figure 4), the IoT challenges the organisation of formal standardisation activity, and requires coordination and a more careful alignment between technical committees working on IoT architecture and interoperability,
security, risk management, supply chain management and consumer product safety.

3.2 De Facto Standards Relevant to IoT Security

Several industry alliances and interest associations have responded to the gaps in formal standards development by proposing their own guidelines for securing the IoT. Increasingly, these guidelines are complemented by compliance testing procedures for members or interested parties. Some industry associations are also promoting their own certification labels and trust marks, as a way of showcasing compliance with the proposed guidelines. In addition, open certification marks are currently developed by not-for-profit organisations targeting consumers and start-up companies [48].

Table 1 provides a summary of the main industry and interest associations that have to this date developed IoT security-related guidelines [34–39], [49–56], compliance testing procedures and certification marks [57–67] to signal their conformity with a responsible level of IoT security.

Table 1 shows that the IoT security standards and best practice landscape has been predominantly shaped by the market via transnational industry alliances and interest associations. A quick review of the guidelines, testing and certification schemes proposed by these associations reveals three main findings.

First, there is growing convergence in de facto standardisation towards a set of core technical and organisational specifications to ensure a responsible level of IoT security. This convergence has also been noted by cybersecurity agencies and standardisation bodies in the EU and the US [30, 32, 68], and includes:

Core Technical Specifications
- Identification, authentication, authorization
- Cryptography
- Security auditing
- Self-protection and component isolation
- Data integrity and minimisation

Core Organisational Specifications
- Risk and asset management
- Threat analysis and use case assessments
- Lifecycle and end-of-life support
- User awareness through clear policies and labelling

Second, the development of de facto guidelines and certification schemes increases the complexity of the current standards landscape for IoT security, especially for new entrants and small and medium size enterprises (SMEs) who have to navigate through the complex landscape of standards, guidelines and best practices currently available.

Participants of the ‘Secure by Default’ Workshop organised by PETRAS IoT (March 2017) echoed this, emphasising that the decision to select the most appropriate standards for their particular business is one of the main challenges faced by entities in the IoT ecosystem, especially at the manufacturing and service level.

In addition, the PETRAS IoT ‘Cybersecurity of the Internet of Things Standards Survey’ revealed an already mixed picture when it comes to the ease of implementing and deploying current standards for IoT security (Figure 5). This reality can explain, at least in part, why legislators and public agencies are increasingly preoccupied with setting a level playing field for IoT security.

Lastly, current IoT security best practices expose new interdependencies that challenge and will continue to challenge standardisation processes in the future. The list of market-driven
The development of de facto guidelines and certification schemes increases the complexity of the current standards landscape and reinforces fragmentation as well as the difficulty for new entrants and SMEs to identify the most suitable standards and guidelines currently available.

Third, the paper identified a number of key challenges for the current IoT security standards landscape, most notably: a) the difficulty of setting a baseline for IoT security across all IoT applications and domains, which adds complexity to defining specifications that clarify the relationship between data integrity — cyber and physical security — safety — resilience — trustworthiness; as well as b) the difficulties of monitoring the adoption and implementation of IoT security standards and best practices by market entities involved in the development, manufacturing and service provision of IoT.

The analysis of the evolution and current state of deployment of IoT security standards contributes to a better understanding of the need for a more aligned standardisation approach. Standards development organisations are encouraged to seek more extensive coordination across technical committee and have to a) fill the gap of developing formal security standards which take into account both device and end-to-end security, and are specific to the IoT; and b) articulate more clearly the extent to which their activities cover all aspects of IoT security and the extent to which their published standards, such as information security standards, apply to the IoT.

Additionally, the review affirmed that more research on the barriers to adoption and implementation of IoT security standards is needed. This will be pursued by the PETRAS IoT Research Hub in the course of a further analysis stage which involves semi-structured interviews with key standards development organisations, trade associations and UK regulatory bodies. This holistic assessment can feed into ongoing policy reviews and standardisation processes, by revealing the main opportunities and challenges to achieving a secure IoT.

Acknowledgements

The authors would like to express their appreciation to Robert Thompson (PETRAS IoT, UCL), Graca Carvalho (PETRAS IoT, UCL), Tim McGarr (BSI), Alberto Garcia Mogollon (BSI) and Idris Jahn (IoTUK) for their valuable contribution to the development and dissemination of the ‘Cybersecurity of the Internet of Things Survey’ and the coordination of the ‘IoT Secure by Default’ Workshop.

This research was supported by the UK Engineering and Physical Sciences Research Council and partner contributions under grant EP/N02334X/1.

References


[51] Cloud Security Alliance, ‘Future Proofing the Connected World: 12 Steps to Developing Secure IoT


