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

Conference Paper · June 2018

DOI: 10.1049/cp.2018.0024

5 authors, including:

Irina Brass
University College London
22 PUBLICATIONS **66** CITATIONS

SEE PROFILE

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

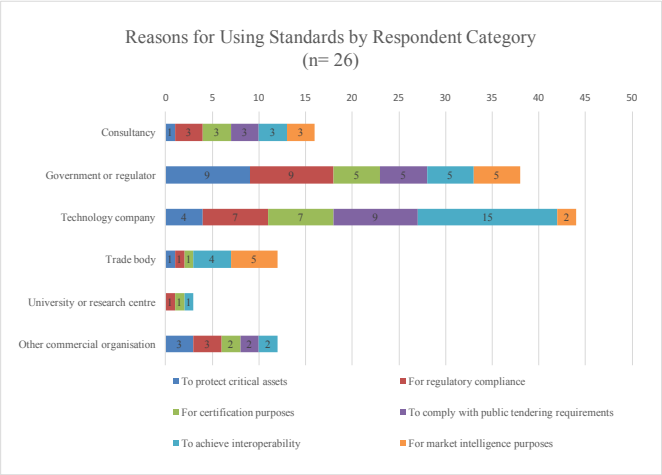

Fig. 1: Reasons for Using Standards Related to Cybersecurity of the IoT. Data shows responses to Question 9 of the 'Cybersecurity of the Internet of Things Standards Survey' [9]: "*Please tell us what goal the standards you identified support. Select all that apply.*

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);
3. A workshop on 'IoT Security by Default' with PETRAS IoT researchers and partners, exploring standards development in IoT consumer goods, transport, health, and utilities (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

[1] This broad definition is adopted because technical (or design) specifications represent only one type of standards, which generally address behaviour at *the prevention stage*. As outlined in the specialist literature, standards can also focus on "the *act* that gives rise to a harmful result" – known as performance standards, such as risk assessment in the context of cybersecurity, or they can focus on "*the harmful result* itself" – known as target standards, such as joint incident responses conducted by CERTs. For a foundational description of standards typologies, see Baldwin et al [14].