"Who Watches the Watchmen?" A Critical Analysis of British Standards Concerning Security and Trust in Cyber–Physical Systems

Group 4

16th February 2021

Trust, but verify.
Russian proverb

Introduction

[placeholder-text]

Terminology

It is important when discussing any kind of security to clarify terminology. Cybersecurity possesses a unique and extensive nomenclature and to ensure the accessibility of this blog post, we will be using it minimally. However, two core concepts for cybersecurity, trust and composition, are crucial to define for the context of this piece.

- **Trust** – The sociological definition of trust, which has been widely adopted by the cybersecurity community, is the reliance on an entity to behave as expected, despite its capacity to defy those expectations. In the context of this blog post, if a cyber–physical system were to behave as expected, only expected kinds of processing or computation would occur. We consider this definition sound and congruent with the topic of this blog post.
- **Composition** – Composition is the primary engineering approach to construct complex systems by composing preexisting components in layered designs. While the properties of individual components may be known and understood, the same properties of a combined system may be more difficult to ascertain, potentially resulting in unexpected behaviours.

Part I

BS 10754–1:2018 or: How The British Standards Institution Learned to Stop Worrying and Copy NIST's Homework

The Cybersecurity Framework 1.0 published by the US Department of Commerce's National Institute of Standards and Technology (NIST) is internationally recognised as the benchmark standard for establishing effective cybersecurity policies, across both the public and private sectors. Originally published in February 2014, the framework categorises cybersecurity risk assessment and management under five broad functions: identify, protect, detect, respond andrecover. A revised version of the publication, the NIST Cybersecurity Framework 1.1 was published in April 2018, shortly after the publication of the Information Technology–Systems Trustworthiness Part 1: Governance and Management Specification document (BS 10754–1:2018) by the British Standards Institution (BSI) in February 2018. Despite the 218 GBP price tag to purchase BS 10754–1:2018 in comparison to the freely available NIST Cybersecurity Framework 1.1, the similarities between the two documents bear remarkable resemblance. In light of this, the following blog post will observe the commonalities between the two documents while critically assessing the risk assessment and management approach of BS 01754–1:2018, in the context of the security use case of cyber–physical systems.

BS 10754–1:2018 categorises risk assessment as "Understanding general risks" and "Understanding trustworthiness risks", though one may argue these are one and the same in the context of cybersecurity. The first section, "Understanding general risks", outlines the steps necessary to critically assess the composition of system architectures, which is consistent with the preliminary steps of a security engineer's workflow and the NIST Cybersecurity Framework (subsection ID.RA) and the NIST Security and Privacy Controls for Federal Information Systems and Organizations Special Publication (NIST SP 800–53 Rev. 4). To "assess the risk to trustworthiness", identifying and enumerating assets and their threats and vulnerabilities, which collectively manifest risks for systems, are asserted as sound methodology. This is consistent with the "Identify" section of the NIST Cybersecurity Framework, specifically subsections ID.AM, ID.R–3

and ID.R–1, respectively. The techniques listed to understand "general risks" may be considered vague and lacking technical specificity, which one may infer as indicating a lack of critical engagement with stakeholders from the technical community when developing the document.

The second section, "Understanding trustworthiness risks", outlines a rudimentary threat intelligence framework to identify threats and vulnerabilities, utilising common cybersecurity resources such as the Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) databases, in addition to the Common Vulnerability Scoring System (CVSS). While these databases are undeniably important resources in a security engineer's intelligence–gathering arsenal, this might be described as a "minimum viable framework" for threat intelligence, excluding common intelligence–gathering methods frequently utilised by security engineers, such as monitoring activity on darkweb forums and internet relay chat (IRC) channels, which serve as bastions for cyber threat actors. Additionally, in the context of cyber–physical systems, monitoring and analysing data collected from the Shodan search engine for internet–connected devices and the United States Department of Commerce's Centre for Applied Internet Data Analysis (CAIDA) network telescope is common practice for threat intelligence concerning Internet of Things (IoT), cyber–physical systems and industrial–control systems, which is not included in the document, further indicating a lack of critical stakeholder engagement. Again, all of the proposed steps are consistent with the NIST Cybersecurity Framework (subsection ID.RA–2) and NIST SP 800–53 Rev. 4.

[risk-management]

[placeholder-text]

[conclusion]

On the balance of evidence, we assert that BS 10754–1:2018 provides little, if any, meaningful value over and above the NIST Cybersecurity Framework 1.1, of which it appears largely derivative. Its content clearly reflects lack of critical engagement with stakeholders, particularly those from the technical community. Although it is intended as a high–level document, its recommendations are generally reductive and lack technical specificity to such a degree that it almost invalidates the document's credibility. As such, we find BS 10754–1:2018 to be inadequate to provide effective recommendations for ensuring the trustworthiness of information and communication technology systems, including cyber–physical systems.

Part II

Risk management – Risk assessment techniques (IEC 31010:2019)

In this part, we will critically analyse two risk assessment methods proposed in the Risk Management – Risk Assessment Techniques standard (IEC 31010:2019), published by the International Organization for Standardization (ISO) Risk Management Technical Committee (ISO/TC 262) in June 2019. In congruence with the topic of this piece, we have selected **[method1]** and **[method2]**and we will assess their salience, benefits and limitations.

[method1]

[placeholder-text]

[method2]

[placeholder-text]