discribe

IMAGINING SECURE DIGITAL FUTURES

September, 2021

Regulation, Policy and Cybersecurity

Hardware Security

Final Project Report

Authors: Prof. Vladlena Benson
Prof. Steven Furnell
Dr Donato Masi
Dr Tim Muller

This work details the key findings of work conducted by the Discribe Hub+ commissioned project *Regulation, Policy and Cybersecurity.* You can read more about the project by visiting https://www.discribehub.org/research-2-1

The Discribe Hub+ is funded by UKRI through ESRC Grant number: ES/V003666/1.
For more information about the Hub+, please visit www.Discribehub.org

UK Research and Innovation

(C) 2021 Discribe Hub+ Creative Commons 4.0 BY-NC-SA licence. www.discribehub.org/copyright

For public distribution

Regulation, Policy and Cybersecurity

Hardware Security

Prof. Vladlena Benson
Prof. Steven Furnell
Dr Donato Masi
Dr Tim Muller

September 2021

Table of Contents

GLOSSARY OF ABBREVIATIONS 1

EXECUTIVE SUMMARY 2

1. INTRODUCTION 3

1.1. Project aim and objectives 3

1.2. Report coverage and structure 3

1.3. Research methodology 4

2. THE HARDWARE SECURITY LANDSCAPE 6

2.1. A summary of hardware-centric threats 6

2.2. Relationships and responsibilities in hardware security 8

2.3. Hardware security supply chain risk 9

3. EXISTING STANDARDS AND REGULATIONS IN HARDWARE SECURITY 12

3.1. Related standards 12
3.1.1. SOGIS-MRA 12
3.1.2. Common Criteria 13
3.1.3. Security of hardware components within devices 13

3.2. Current good practice guidance 14

3.3. Security within specific devices 16

3.4. Device labelling 18

4. CASE EXAMPLE: AUTOMOTIVE SECTOR 20

4.1. Practices and principles of hardware security in the automotive industry 20

4.2. Regulations, guidelines and standards for hardware security in automotive 23

5. CASE EXAMPLE: FINTECH SECTOR 26

5.1. The international regulatory landscape for fintech 27

5.2. The UK general regulatory landscape for fintech 28

5.3. Fintech hardware security 30

5.4. Counterfeit hardware threat landscape 31

6. STAKEHOLDER ENGAGEMENT AND FINTECH WORKSHOP SUMMARY 33

6.1. Recognition of existing regulation in hardware security 34
6.1.1. Isolating hardware security from software security regulations 34
6.1.2. Legislation and industry standards 35
6.1.3. Reactive approach 35

6.2. Usage and impact of current regulation 35
6.2.1. Insufficient awareness 35
6.2.2. Drivers of compliance 36

6.3. Suitability and sufficiency of existing regulation 37
6.3.1. Contradictory regulations 37
6.3.2. Insufficient regulatory agility 37

6.4. Moving forward 38
6.4.1. Harmonisation of standards and regulations 38
6.4.2. Enhanced monitoring of transactions 39
6.4.3. Enhanced regulatory agility 39
6.4.4. Is more severe legislation realistic? 40

6.5. Recommendations and Conclusions 40

7. DISCUSSION AND CONCLUSIONS 41

8. REFERENCES 44

APPENDIX – WORKSHOP MATERIALS 49

8.1. Session plan 49

8.2. Workshop slides 51

Glossary of Abbreviations

API	Application Programming Interface
CAV	Connected and Autonomous Vehicle
CC	Common Criteria
CCPA	California Consumer Privacy Act
CRA	Consumer Rights Act
DARPA	Defense Advanced Research Projects Agency
DEA	Digital Economy Act
DPA	Data Protection Act
DSbD	Digital Security by Design
EAL	Evaluation Assurance Level
ECSO	European Cybersecurity Organisation
ECU	Electronic Control Unit
ENISA	European Union Agency for Cybersecurity
EPID	Enhanced Privacy ID
FCA	Financial Conduct Authority
FSMA	Financial Services and Markets Act
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HSM	Hardware Security Module
IoT	Internet of Things
ISO	International Organisation for Standardisation
MOD	Ministry of Defence
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OTA	Over the Air
PCI-DSS	Payment Card Industry Data Security Standard
PIPEDA	Personal Information Protection and Electronic Documents Act
POPI	Protection of Personal Information
PRA	Prudential Regulation Authority
PSD2	Payment Services Directive 2
SHE	Secure Hardware Extension
SME	Small and Medium Enterprise
SOGIS	Senior Officials Group Information Systems Security
TPM	Trusted Platform Module
UNECE	United Nations Economic Commission for Europe

Executive Summary

The digital society has a significant reliance upon the secure operation of systems and machinery, including the hardware present in personal and industrial devices. The volume of cyber-physical threats is rising, and their complexity and sophistication have demonstrated that attackers have both the intent and ability to exploit vulnerabilities in hardware security as part of digital products and services. A review of academic research on regulatory frameworks pertinent to hardware security has been conducted. It shows that while progress has been significant, with new legislation, standards and regulation on hardware security, the approaches taken by policy makers have been disconnected.

Despite hardware security being a recognised area within the overall domain of cybersecurity, as well as the presence of long-established and more recent standards for demonstrating aspects of security in related design and implementation of hardware-based products and security solutions, it remains an area of potential vulnerability. Common areas of weakness have been found to include a lack of use of secure mechanisms available in the platforms, a lack of adherence to good practice in system design, and a lack of tamper detection capability. This report provides a taxonomy of hardware-related threats and highlights a variety of guidance and standards that have relevance in this space.

Two sector specific cases are explored in more detail that address the challenges of highly regulated environments, i.e. the automotive and fintech industries. The automotive sector is distinct in the view of cybersecurity being intertwined with safety, as the loss of human life is at stake. On the other hand, fintech emerged as an area which is highly compliance driven and meeting regulatory needs is ingrained as a 'cost of doing business' and 'loss avoidance.' Both sectors share common features in terms of technology being ahead of the regulatory efforts by governments, which are slow in reacting but have a profound effect on industry players in increasing their security efforts and investment.

Feedback from stakeholders in governance risk and compliance has been integrated into this analysis. It emerges that hardware-focused cybersecurity innovations are overshadowed by cost considerations in favour of fast-to-market solutions. In relation to the adoption of Digital Security by Design (DSbD), integrating new solutions could be delivered via discussions with industry associations, regulatory bodies and UK government agencies currently reviewing regulatory interventions in hardware assurance and security by design.

1. Introduction

This report presents the work and findings of a 6-month investigative project examining the cybersecurity regulation and policy landscape relating to hardware security in the context of Digital Security by Design (DSbD). It forms part of a wider portfolio of work funded by the ESRC-funded *Digital Security by Design Social Science Hub+ (Discribe)*.

The project ran from February to July 2021, and was conducted as a collaboration between academics at Aston University and the University of Nottingham.

1.1. Project aim and objectives

The aim of the project was to:

"*Carry out research on the regulatory landscape within the UK digital sector, which is focused on the design and use of hardware security as part of digital products and services*"

In pursuit of this, the accompanying objectives of the project were initially defined as follows:

- Outline the regulatory frameworks for the development and adoption of hardware security in the UK and discuss related regulatory challenges and opportunities (around equality, expectations, investments) as well as barriers and enablers of their adoption in both the inter-organisational (e.g. supply-chain) and intra-organisational contexts;
- Review academic research on regulatory frameworks related to hardware security within the UK and internationally;
- Examine whether there are different regulatory frameworks and approaches in different organisations taking account of different sectors (e.g., public vs private), size (e.g. large vs SME) and the extent of digitalisation (e.g. born digital versus pre-digital);
- Conduct key stakeholder workshops exploring how DSbD might impact the regulatory landscape of digital security.

It should be noted that throughout the report, the term 'regulation' is being interpreted broadly, such that it includes legislation, standards, codes of practice and guidelines, and the scope may be national, international, and industry led. Furthermore, regulation can be relevant in at least two contexts:

- That which places restrictions or requirements on the sector in question (i.e., the regulation is relevant because the sector needs to follow it);
- That which applies to organisations that supply hardware to the sector (i.e., the regulation is relevant because the sector relies on the hardware being compliant).

1.2. Report coverage and structure

The report examines the issue of hardware-related regulation and policy in general terms, as well as in the context of selected industry sectors.

Beginning with an outline of the nature of the hardware security threat landscape itself, Section 2 examines the factors that influence the requirement for security in the hardware context, and the relationships between key parties involved. This is followed by an examination of the general regulatory environment in Section 3, with examples of standards and good practices that have influence in a sector-independent context.

Moving beyond the general focus, the investigation also examines the situation and related awareness in two sector-specific examples. Following guidance from the Discribe Hub+ team, it was determined that desirable candidate areas to examine would be the automotive and financial technology (fintech) sectors. Both have significant and growing dependence upon IT systems, and a corresponding reliance upon secure operation. Moreover, the ability to trust the underlying technological platforms makes them good candidates to benefit from DSbD technology. Case examples relating to both sectors are consequently discussed in Section 4 for automotive, and Section 5 for fintech. The latter is also supported by a discussion of the findings from a related workshop session conducted with stakeholders, which is presented in Section 6.

The last section of the report then takes stock of the findings arising from the entire project, highlighting the potential implications for progressing the DSbD agenda. The main report is supported by an appendix containing copies of the materials that were used to plan and deliver the fintech workshop session.

1.3. Research methodology

The completion of this report required the combination of different methodologies. Firstly, a literature review provided the basis for the identification of the main themes characterising the current regulation for hardware security. These preliminary findings have been validated and refined through two different empirical activities: a workshop and several semi-structured interviews.

Given the small number of studies contained in a limited number of repositories, it was not possible to perform a systematic literature review. The methodology adopted consisted of a narrative review of the literature. A preliminary group of studies have been identified by applying different search strings for the more general regulation background and for the case studies. For the general regulation background, the search strings included terms such as “cybersecurity,” “hardware security,” and “regulation,” combined with several synonyms. For the case studies, the abovementioned terms have been combined with keywords characterising the industrial sectors being investigated, such as “fintech” and “automotive,” again with several synonyms.

The databases used were Google Scholar and Scopus, as these collectively index a range of relevant journals, conferences and wider publications, and offer the facility to construct suitable search strings and combinations. Having identified the preliminary group of studies, more studies have been identified using the snowballing technique. Having identified the studies, the results have been summarised in a report including four different parts: the

hardware security landscape, existing standards and regulations in hardware security, and standards and regulations in the Automotive and in the Fintech Sector.

The sector-specific reviews were supported by a series of discussions with relevant experts. The research team decided to use semi-structured interviews because each sub-theme implied the identification of one expert, interviewed with several questions on detailed aspects of the sub-theme. A series of 1:1 meetings were consequently scheduled between each expert and a member of the research team. Table 1 summarises the job titles of the experts involved in the semi-structured interviews (for confidentiality reasons it is not possible to reveal the specific individuals or organisations involved, but the details in the table make it clear that the participants involved were senior level stakeholders from a range of organisation types). The answers were recorded through contacts notes. The notes have been used for the validation and refinement of the report in a plenary meeting between the members of the research team.

#	Interviewee Role	Organisation type
1	Compliance and Quality Manager	Auditing
2	Information Security GRC Specialist	Auditing
3	Head of Risk – IT Change & Assurance	Banking
4	CISO	Banking
5	Senior Global Privacy Specialist	Financial Services
6	COO Business Risk	Financial Services
7	Head of Procurement & Third Party Assurance	Banking
8	UK Director of Operations	BFSI Law enforcement unit
9	VP Cybersecurity Services	Consulting
10	Head of Information & Cybersecurity	Banking
11	Head of Technology & Cyber Risk	Banking
13	Supplier Compliance Manager	Insurance
14	Partner, specialises in Third Party Supplier Assurance	Auditing
15	CEO	Fintech
16	Consultant	IoT hardware Manufacturer, Transport Sector (France)
17	Associate	Defense consultancy
18	Head of Governance	UK Car Manufacturer
19	Lead, IT Security Architecture	Car Manufacturers Alliance
20	CEO, Research and Development	Supplier to the MoD

Table 1: Details of the experts involved in the semi-structured interviews

Having conduced the individual sector-specific reviews, the workshop was aimed towards more specifically exploring the recognition, impact and relevance of existing regulation with stakeholders from the FinTech sector. This is described in more detail in section 6, along with a presentation of the session plan and supporting materials in the appendix.

2. The hardware security landscape

Levine (2021) offers the tenet that "trust starts in silicon," highlighting the fundamental nature of hardware security as an underpinning assumption upon which other security efforts will typically be based. As he goes on to state, one cannot design a secure system on a compromised base, and unlike software (where vulnerabilities can be patched) there is no opportunity to retrofit a fix to compromised hardware. This means affected devices will need to be replaced.

Levine's comment and observations are framed around the design and production of integrated circuits in the supply of semiconductors. However, the consideration of hardware security can span multiple levels of design, production and deployment. For example, each of the following contexts has a clear relationship to the notion of 'securing the hardware', but each is distinct in terms of what needs to be safeguarded and how this would be achieved:

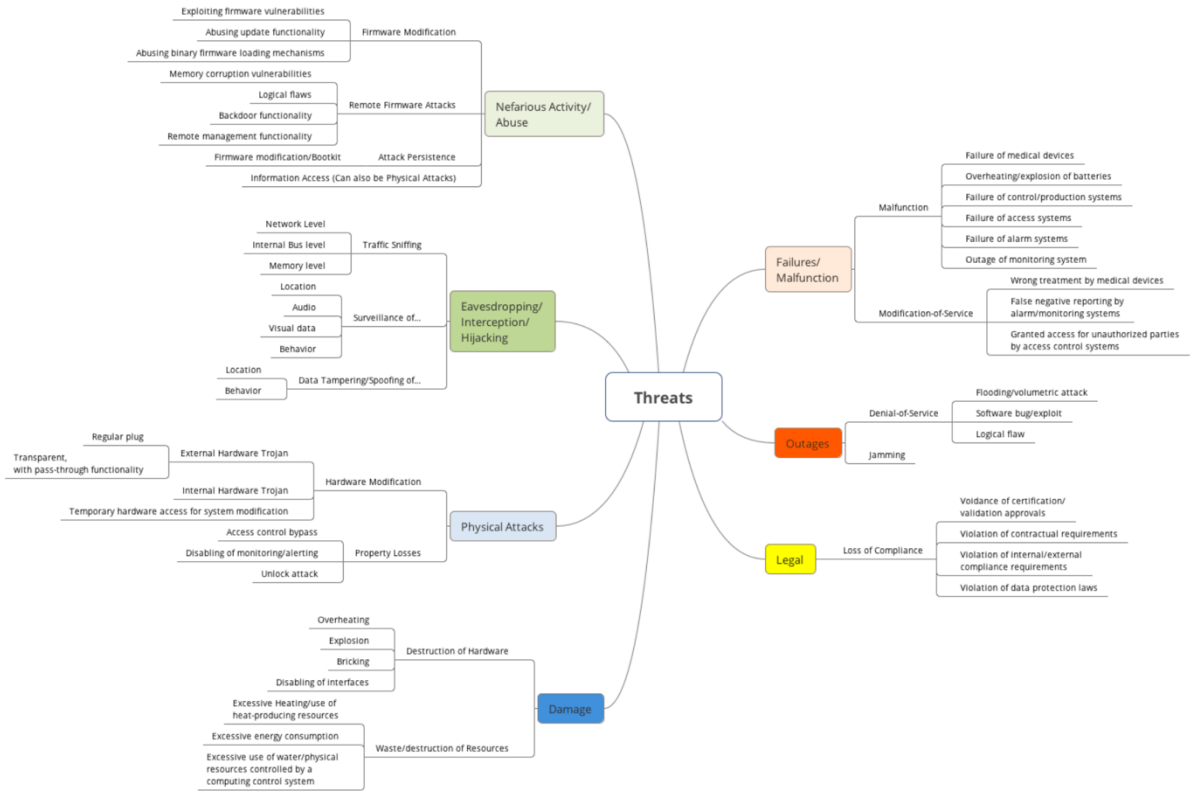
- **Design and fabrication of components** (where there is a need to ensure that the process itself is not compromised);
- **Obtaining hardware components through the supply chain** (where supplies need to originate from trusted sources and arrive free of tampering);
- **Design of products incorporating Original Equipment Manufacturer (OEM) components** (where there are again issues of ensuring that the design and production of the entire device is not compromised);
- **Selection and deployment of hardware** (where an end-user organisation is looking to ensure that it can identify and procure devices with sufficient security and assurance).

The recognition of these issues is by no means a new occurrence. For example, Fazzari and Narumi (2019) provide a good summary of efforts at the IC and microelectronics levels that trace efforts back to 1974, and track things through to more recent initiatives such as DARPA's Trusted, Uncompromised Semiconductor Technology (TrUST)[1] programme. Meanwhile, recent and timely recognition of the significance of hardware-level protection is illustrated by Microsoft's decision to require that end systems have a TPM (Trusted Platform Module) chip in order to run Windows 11 (Weston, 2021). In this case the move was at least in part driven by a rise in firmware level attacks (e.g., targeting credentials and encryption keys), with findings suggesting that 83% of businesses had experienced a firmware attack in the previous two years (Microsoft, 2021), and a recognition that a hardware-level safeguard would raise the bar against related attackers.

2.1. A summary of hardware-centric threats

The hardware threat landscape is broad in scope, as illustrated by the mind map summary produced by ENISA (2017) shown in Figure 1. The majority of these threats can at least partly be linked back to considerations at the design stage (the main exception being the "damage" category, but there are further individual items within other categories for which design-stage actions would have little or no bearing).

[1] It should be noted that the same DARPA programme is varyingly referred to as *TRUSTed Integrated Circuits*, *TRUST in Integrated Circuits*, and *TRUST*.



(Source: ENISA, 2017)

Figure 1: ENISA hardware threat mind map.

Outline descriptions of each of the main categories depicted in Figure 1 are provided as follows (ENISA, 2017):

- **Nefarious activity/abuse (NAA):** This threat category comprises intended actions that target IT systems with the purpose to steal/modify/tamper with/destroy assets;
- **Eavesdropping/Interception/Hijacking (EIH):** This threat category comprises actions striving to access communication in an unauthorized way;
- **Physical attacks (PA):** This threat category comprises actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets as defined above;
- **Damage (DAM):** This threat category comprises intended actions which result in destruction, harm, or injury of property or health and can result in a loss of value/function;
- **Unintentional Damage (UD):** This threat category is comparable to DAM, however the impact is the result of an unintentional action**;**
- **Failures or malfunctions (FM):** This threat category comprises unwanted behaviour of an IT system affecting the ability to execute the desired function**;**
- **Outages (OUT):** This threat category comprises events leading to unexpected/undesired disruptions in the delivery (quality) of services – which are not limited to IT services**;**

- **Disaster (DIS):** This threat category is defined as serious disruption of the functioning due to some physical or man-made disaster;
- **Legal (LEG):** This threat category comprises legal actions of third parties with the potential effect to impact assets in numerous ways.

The full ENISA report goes on to provide a more detailed description of each of the threats, including consideration of potential effects and affected assets. However, this is beyond the scope of the current report, and in this context it is sufficient to know that the need for hardware security by design is motivated from several directions and drivers.

Looking specifically at hardware as a route for *intentional* compromise, recent draft work from NIST highlights that increased attention to software and application-level security is causing attackers to shift focus towards the firmware and hardware levels. This leads to multiple resulting threats. These include (Bartock et al., 2021):

- "Unauthorized access to and potential extraction of sensitive platform or user data, including direct physical access to dual in-line memory modules (DIMMs)
- Modification of platform firmware, such as that belonging to the Unified Extensible Firmware Interface (UEFI)/Basic Input Output System (BIOS), Board Management Controller (BMC), Manageability Engine (ME), Peripheral Component Interconnect Express (PCIE) device, and various accelerator cards
- Supply chain interception through the physical replacement of firmware or hardware with malicious versions
- Circumvention of software and/or firmware-based security mechanisms"

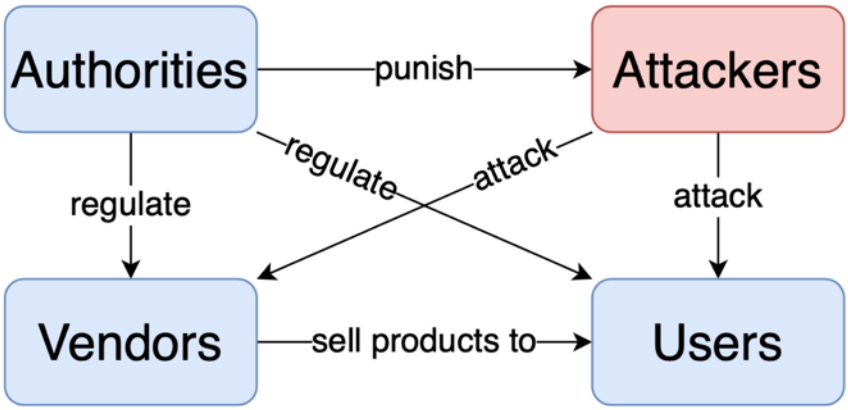
The resultant layered safeguards that are suggested in the NIST report, including Platform Integrity Verification – via approaches such as Hardware Security Modules and Trusted Platform Modules – rely on the security of these underlying components. Thus, while not mentioned by name in the NIST draft, DSbD is implied as an underlying basis for trusting these elements.

2.2. Relationships and responsibilities in hardware security

Mulligan and Schneider (2011) propose four "Doctrines of Cybersecurity:" prevention, risk management, security as a public good, and deterrence. Building upon this, more recent work from Hastings and Sethumadhavan (2020) proposes "a Doctrine of Shared Burdens for Hardware Security" to codify a series of relationships exists between various involved parties as depicted in Figure 2. In the context of security by design, the most relevant players here are *vendors* and *authorities*. The former are the parties designing and building the products[2], who have the 'burden' of bearing the costs associated with ensuring that their products are secured against exploitation. This is essentially in line with the Doctrine of Prevention, and is arguably susceptible to failure because vendors may be motivated by opposing incentives (e.g., market advantage by releasing products that appear earlier, but with less security). This necessitates the regulatory role wielded by an *authority*, which may be represented by

[2] As such, the term *manufacturer* may be more appropriate than *vendor*, but we have chosen to retain the vocabulary used in the source paper.

government bodies, but could also be regulatory groups for related industry sectors. Findings from Hastings and Sethumadhavan's paper indeed suggests that trade organisations and standards committees can fulfil this role.



(Source: Hastings and Sethumadhavan, 2020)

Figure 2: Relationship between different players in the context of hardware security.

2.3. Hardware security supply chain risk

The compromise of components during manufacture or transportation is a potential threat in the supply of physical products. It is a particularly relevant concern in the context of securing hardware for two reasons: an adversary targets the weakest link in the chain, and a compromise could lead to fundamental vulnerabilities being embedded within deployed devices. Additionally, a small number of countries essentially hold a monopoly in the device component sector, which has implications for the feasibility and impact of compromise within the supply chain.

In practice, a lack of attention toward security within the supply chain is not solely a problem relating to hardware. For example, a more general 2019 study from Dun & Bradstreet drew upon responses from 630 procurement and compliance professionals and revealed that almost half (48%) had not implemented a cyber risk approach in relation to third parties (Dun and Bradstreet, 2019). This was despite cybersecurity being cited as the top concern amongst the respondent group. However, the report went on to specifically identify the *lack of clear global standards* as an obstacle to effective screening of suppliers (resulting in each organisation being left to determine and decide its own approach on the issue). Given that this concerns dealing with cybersecurity in the supply chain in general, it is unreasonable to assume that hardware security – an area that generally receives less explicit attention – would be treated as significant. Ideally, hardware security should receive greater attention in the supply chain context, given that any resulting vulnerabilities would be exceedingly difficult to identify, resolve and/or eradicate once they are present within deployed devices.

Considering what organisations in general ought to be doing in this space, Wood (2020) identifies the following ten "best practices" for designing a strong supply chain:

1. Perform a risk analysis of the business;
2. Create and maintain an inventory of third-party hardware providers;
3. Identify the devices that provide business-critical functionality and services;
4. Perform a third-party risk assessment on each critical provider/device;
5. Establish a communication plan with each critical provider;
6. Build and maintain a software dependency tracker for your organization's hardware;
7. Establish an assessment process for third-party hardware that is delivered to your; organisation;
8. Conduct ingress and egress filtering;
9. Request documentation and proof of assessment for devices that implement critical infrastructure;
10. Understand the vendors' supply chains as part of the system selection process.

Examining this list, it is apparent that some of these points (particularly items 1 and 8) seem to relate to the organisation's security posture more generally rather than specifically relating to security in the supply chain. It is also apparent that the ordering of the list does not strictly relate to the order in which the items would become relevant in practice. While item 1 can be considered as an overarching starting point, the other aspects come into play at different points in the supply and deployment of devices:

- Items 2, 4, 5, 7, 9 and 10 are elements that ought to be established as part of the organisation's supplier selection and procurement processes;
- Items 3, 6 and 8 ought to be applied to any devices procured and deployed within the organisation.

While it is difficult to argue with the logic behind the recommendations and the value of such controls, there is no clear incentive for any individual organisation to follow them. If they are to become embedded within normal supply chain operations, then they need to be reflected in an explicit standard or code of practice to formally govern supply chain security, as opposed to a series of best practice tips.

Supply chain security requirements *are* expressed within the ISO/IEC 27002 code of practice for information security controls, with the following provisions being amongst those highlighted within the implementation guidance (ISO, 2013):

- "for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organisation;
- for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased from other suppliers;
- implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;

- implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;
- obtaining assurance that critical components and their origin can be traced throughout the supply chain;
- obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;
- defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers."

While these points are not being made with explicit reference to hardware components, they do apply to hardware. As such, hardware clearly falls within the intended scope of ISO/IEC 27002.

However, as things currently stand, even attention to supply chain security in general is notably lacking. For example, the UK Cybersecurity Breaches Survey 2021 indicates that only 5% of UK businesses formally consider the risks of their wider supply chain, and even in large firms the figure is still only 20% (DCMS, 2021).

The effect of supply chains on organisations is so profound that the National Cybersecurity Centre (NCSC) has developed the Supply Chain Security Guidance (NCSC, 2018). While this refers to digital supply chain security across data processing and interconnected software systems, it also encompasses principles of assuring hardware security. Developing its guidance further, the NCSC also offers support to organisations by providing a template Supplier Assurance Questionnaire, providing avenues for the discussions between the supplier and customer around effective cyber risk management practices (NCSC, 2020). Several priority areas are defined to help ensure that suppliers have put appropriate cybersecurity mechanisms in practice, including measures around security governance and responsibility, as well as independent testing and assurance. These are clearly relevant issues to consider in the context of hardware adoption and/or related component procurement.

3. Existing standards and regulations in hardware security

Typical standards and regulations focus on a specific application, domain or technology. After all, a particular business should be able to easily find regulations relating to their operations. A distinction is therefore not typically drawn around hardware security versus the security of other aspects. Nevertheless, within set regulations there are explicit references to hardware security, as well as implicit ones.

Explicit references to hardware security can relate to good practices with respect to the security requirements and security support of hardware. They can relate to security within specific devices, such as suggesting more targeted technological requirements aimed at concrete threats for the specific devices. Or they can relate to labelling devices, pushing for transparency throughout the supply chain.

The implicit references are, in a sense, more numerous. Any technical security requirement must, to some extent, be a hardware security requirement too. This claim is based on the observation that if the hardware is compromised in the right way, then it can be made to behave as the attacker intends. According to Baumgarten et al. (2011), Trojan exploits can be inserted in every step in the supply chain, varying from undocumented components, to tampering with random number generators to cripple cryptographic functions. Trojans are powerful tools that are often used as the basis of all kinds of attacks. Hence, any form of security (implicitly) presupposes hardware security.[3]

3.1. Related standards

There are a number of relevant standards in the context of IT products and the security of the components within them.

3.1.1. SOGIS-MRA

To give it the full name, SOGIS-MRA is the Mutual Recognition Agreement of the Senior Officials Group (SOGIS, 2010). It is relevant to this study in that the aim of the agreement is to improve the availability of evaluated, security-enhanced IT products, and to ensure that evaluations are performed to a high and consistent standard.

It is focused on hardware at the product level rather than on underlying components, and identifies two key technical domains, defined as follows (SOGIS, 2011):

- **Smartcards and Similar Devices** - for smart cards and similar devices where significant portions of the required security functionality depend upon hardware features at a chip level (e.g., smart card hardware/ICs, smart card composite products, TPMs used in Trusted Computing, digital tachograph cards, etc.)

[3] In fact, the industry partners we had contact with during the project seemed to be most focused on the implicit requirements for hardware security that arise from the more general security standards and regulations.

- **Hardware Devices with Security Boxes** - for products produced from a series of discrete parts on one or more printed circuit boards whereby significant proportions of the required security functionality depend upon a hardware physical envelope with countermeasures (a so-called "Security Box") against direct physical attacks (e.g., payment terminals, tachograph vehicle units, smart meters, Hardware Security Modules, etc.)

Further documents are indicated within each domain, each of which provides supporting material for the evaluation of related products.

3.1.2. Common Criteria

The Common Criteria (CC) scheme is an established approach for assessing the security functionality has been tested within the design, development and implementation of hardware, firmware and software products (Common Criteria, 2017).

For the purposes of this study, a key aspect of relevance with the Common Criteria approach is the use of Evaluation Assurance Levels (EALs), which provide an indication of the rigour and extent to which a given product has been evaluated:

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested and reviewed
- EAL5: Semi-formally designed and tested
- EAL6: Semi-formally verified design and tested
- EAL7: Formally verified design and tested.

The resulting EAL rating provides a basis for the comparability of products, and is assessed via independent evaluations. From the 'rules of thumb' presented in guidance from the German Federal Office for Information Security, hardware-based products would be expected to aim for EAL4 and above (Federal Office for Information Security, 2007).

The CC provides the basis for the Common Criteria Recognition Arrangement, enabling the international certification and recognition of CC-assessed products across 31 participating countries (17 as certificate authorising members, and 14 as certificate consumers only)[4] and is currently being used by ENISA as the foundation for the EU Cybersecurity Certification scheme (ENISA, 2020), which in turn supersedes the SOGIS-MRA.

3.1.3. Security of hardware components within devices

One of the fundamental requirements in providing assurance in relation to a given device is the ability to understand and verify the security of the various hardware components within it. These are likely to come from diverse sources, and so the overall assurance depends upon

[4] See https://www.commoncriteriaportal.org/ccra/members/ for details.

being able to appropriately decompose and track these, with the ideal situation ultimately being that each can be traced back to a compliant point of origin.

In the United States, the National Institute of Standards and Technology and the National Cybersecurity Center of Excellence have conducted a project to demonstrate how organisations can verify that the integrity of components within their acquired computing devices. As summarised in the abstract of the final report, there are three elements within this work (Diamond et al., 2020):

1. how to create verifiable descriptions of components and platforms;
2. how to verify devices and components within the single transaction between an OEM and a customer;
3. how to verify devices and components at subsequent stages in the system life cycle in the operational environment.

Even this brief list illustrates the non-trivial breadth of the challenge, and the fact that it extends from the initial identification of relevant components through to ensuring their ongoing integrity in operational contexts. Such tight control is unlikely to represent normal practice in most environments, as evidenced by the earlier survey findings presented in relation to risk assessment within supply chains. While manufacturers themselves might be expected to have more explicit control and tracking of their components, it is not typical for such details to be routinely passed onwards to end customers.

Nonetheless, NIST guidance for Federal Information Systems and Organisations suggests the use of an "Information System Component Inventory" as part of wider Configuration Management controls (Boyens et al., 2015). While not exclusively targeting hardware, this is stated to include "hardware inventory specifications" and it is suggested that it is done to "the level of granularity deemed necessary for tracking and reporting." Within the illustrative discussion in the NIST guidance this is expressed as including manufacturer, device type, model, and serial number. However, it is easy to envisage a more granular level being appropriate for organisations that wish to more specifically understand the provenance of the devices/components being used.

3.2. Current good practice guidance

Consideration of material that currently exists as good/best practice guidance is relevant insofar as this often has the potential to inform later standards and requirements. A good example of this is the ISO 27000 series, which has its origins in a UK Department of Trade and Industry code of practice from the mid-1990s, and quickly progressed to becoming a British Standard, then an International Standard, and ultimately an extensive series of standards.

ENISA's 2017 *Hardware Threat Landscape and Good Practice Guide* provides a series of 16 specific measures, which are summarised in Table 2 (noting that the source report accompanies these details with descriptions, as well as references to further sources from which the guidelines were derived). The full list is presented for completeness (and in the same order as listed in the source document), but the applicability of the different items clearly varies depending upon the type of hardware/device concerned, as well as whether

they are related to pre- or post-market phases of the lifecycle. In the context of the current study, the most relevant points are clearly those that have developers within their target audience, but even here some aspects (e.g. Language Security) are not relevant for this investigation.

Guideline	Target audience
Minimal Hardware Access	Developers
Lock Logical Access	Developers, Vendors
Secure Embedded Design and Development Lifecycle	Developers
Firmware Tamper Detection	Developers, Vendors
Secure Update/Modification Management	Developers
Support Secure Development and Verification Standards	Vendors, Industry
Open Security Validation	Developers
Avoid Backdoor and/or PhoneHome Functionality	Vendors, Industry
User Awareness Process	Vendors, Industry
Secure Key Storage	Vendors, Industry, Developers
Platform Security Mechanisms	Developers
Establish Chain of Trust	Developers
Language Security	Developers
Secure by Default	Developers
Encryption of Data at Rest and in Transport	Developers
Remote Wiping	Developers

Table 2: ENISA good practice measures for hardware security. *(Source: ENISA, 2017)*

The 2017 ENISA report conducted a gap analysis comparing recognised threats to current good practice. They concluded that while various standardisation bodies were covering both IT security in general and hardware development in general, the intersecting area of hardware security remained at the time a new field. As such, one of the key recommendations arising from the report was the need to "*use and contribute to standards.*" This recognises that industry/de-facto standards needed to be progressed to provide comprehensive baseline

protection levels. While the field is now correspondingly older than it was at the time of the report, the recommendations remain broadly relevant (as is reflected in some of the later discussion of the case examples in this report).

3.3. Security within specific devices

When examining the security provisions within hardware-focused products, IoT devices emerge as a particular context of increased focus at present. This is at least in part motivated by the recognised deployment of IoT technologies that have proven to be vulnerable (either due to a lack of security by design, or as a result of subsequent poor configuration), and which have in turn led to exploitation and resultant breaches. While the most widely recognised example was the Mirai malware in 2016, which targeted vulnerable IoT devices and enlisted them into botnet activities (Williams, 2016), it is far from the only case. In addition to numerous further malware examples, there have also been instances of corporate IoT devices being compromised in targeted attacks. As an example, in 2019, Microsoft reported cross-sector attacks by an "activity group" called STRONTIUM that had targeted vulnerable IP phones, printers and video decoders across multiple locations (MSTIC, 2019).

The vulnerability of IoT devices has prompted a variety of resultant activity in relation to guidance, standards and (to some extent) regulation. A good example again comes from the National Institute of Standards and Technology, which has released the NISTIR 8259 series of Interagency/Internal Reports, as follows:

- NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers (Fagan et al., 2020a);
- NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline (Fagan et al., 2020b);
- NISTIR 8259B - IoT Non-Technical Supporting Capability Core Baseline (Fagan et al., 2020c);
- NISTIR 8259C - Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline (Fagan et al., 2020d);
- NISTIR 8259D - Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government (Fagan et al., 2020e).

The main standard addresses the so-called foundational activities for manufacturers and presents a set of pre- and post-market cybersecurity aspects that they should be considering in their provision of IoT devices. Specific reference is made to the need to identify required cybersecurity capabilities as early as feasible in the device design processes, so that they can be considered within relevant hardware and software design decisions.

Highlighted amongst the pre-market considerations are several points that are relevant to influencing and informing design decisions:

- *Should an established IoT platform be used instead of acquiring and integrating individual hardware and software components?*
- *Should any of a device's cybersecurity capabilities be hardware-based?*

- *Does the hardware or software (including the operating system) for a given device include unneeded capabilities with cybersecurity implications? If so, can these be disabled to prevent misuse and exploitation?*
- *How can customers verify the hardware or software integrity of an IoT device?*
-

This guidance outlines the implications relating to each of these questions, and the manufacturer's consequent decisions will of course have implications for security in the resulting device design.

In contrast, few hardware-related questions are raised in relation to the post-market phase, but the following consideration clearly has a relevant link back to the choices made at the design phase:

- *What information do customers need about the sources of the device's software, hardware and services?*

The four further documents then build around this, with 8259A being of potentially the most direct relevance to the current discussion. Specifically, this standard covers a technically focused core baseline, which it defines as "a set of device capabilities generally needed to support common cybersecurity controls that protect an organization's devices as well as device data, systems, and ecosystems." The stated aim of this standard is "to provide organizations a starting point to use in identifying the device cybersecurity capabilities for new IoT devices they will manufacture, integrate, or acquire."

Quoting further from the standard itself, the specific capabilities that are identified within the baseline are listed as follows:

- "*Device Identification*: The IoT device can be uniquely identified logically and physically;
- *Device Configuration*: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only;
- *Data Protection*: The IoT device can protect the data it stores and transmits from unauthorized access and modification;
- *Logical Access to Interfaces*: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only;
- *Software Update*: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism;
- *Cybersecurity State Awareness*: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only."

Several of these can be clearly related to the hardware design and provisions within the device concerned, and so there are implications tracking back to the choice of device components and the design into which they are combined.

Looking at how requirements can then translate into legislation, a notable US example comes from the California Legislature, with Senate Bill 327 on the information privacy of connected

devices. This introduced a requirement that, from the start of 2020, manufacturers of Internet-connected devices must:

> "*equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure*" (California Legislature, 2018).

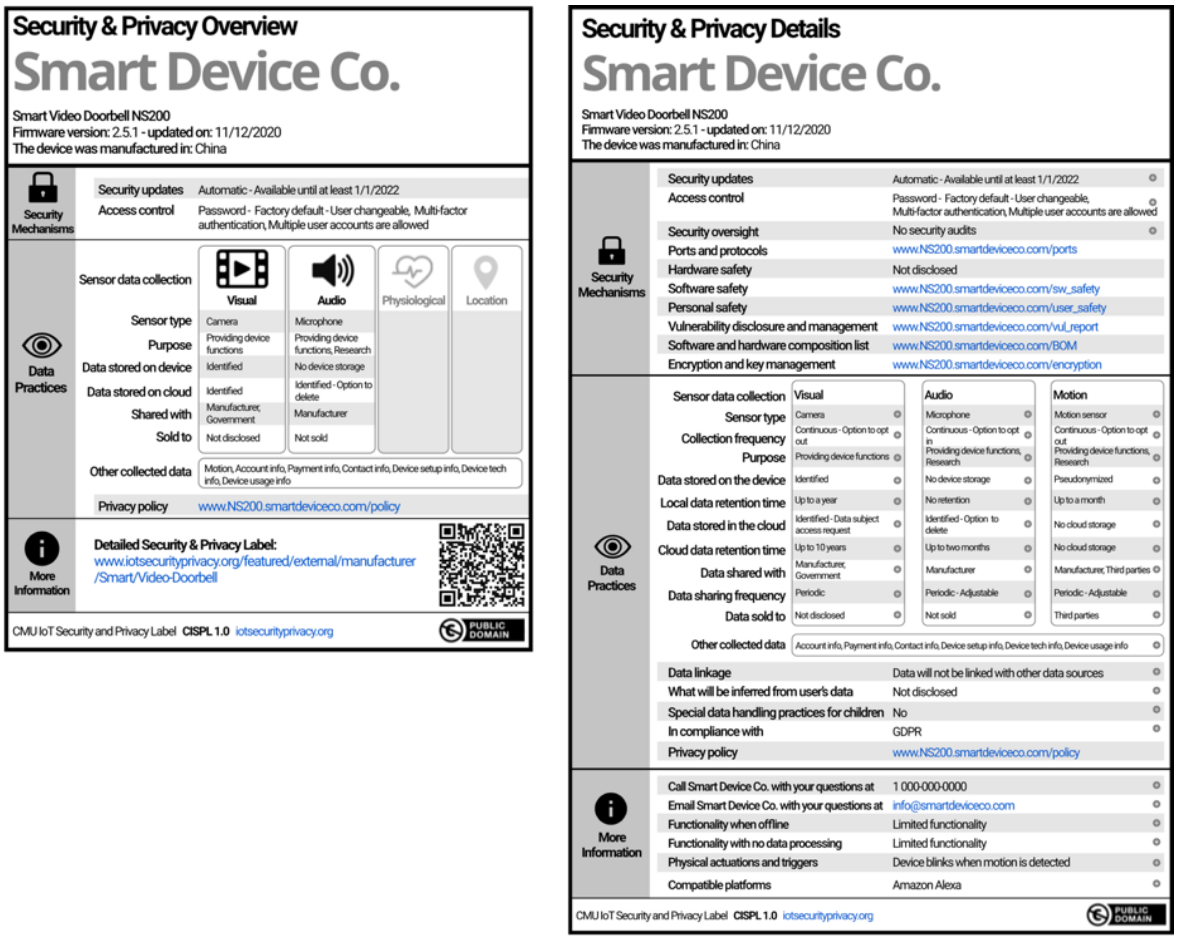
Again, while not specifically or solely addressing the *hardware* perspective, the bill has a clear relevance in this context in order to ensure that the connected device has the necessary facilities and safeguards incorporated within its design.

While this specific example again originates from the United States, it arguably has the potential to become a model for similar provisions elsewhere.

3.4. Device labelling

Alongside having been designed and implemented securely, there is also a consideration of how this information can be communicated onwards to the adopters and users of technology further down the chain. Looking at this from the perspective of end-users, the European Cybersecurity Organisation (ECSO) highlights the need for trust labels to be applied alongside the certification of products (ECSO, 2016). It also recognises that, rather than a single label to denote that the product is 'secure,' there needs to be labels denoting distinct levels according to the level of security provided (the report gives the example of G to A+++).

ECSO does not suggest that there should be any legal or regulatory obligation for customers or companies to buy higher labelled products, but believes that the presence of labels would inform decision making and lead to better choices. At the same time, the ECSO study does not present an actual example of what the Trust Labels would look like in practice, and there is not currently a specific standard for manufacturers to apply and consumers to refer to. However, it is possible to identify related emerging work in other domains, such as the IoT Security and Privacy Label from researchers at Carnegie Mellon University and the University of Washington (Emami-Naeini et al., 2021). In this particular case, as illustrated in Figure 3, the label adopts a two-layer approach, with a primary layer aimed at conveying information to consumers (e.g., displayed on packaging or on websites), and secondary layer offering more detailed information for experts (and accessed online via a link or QR code, as shown in the figure).



(a) (b)

(Source: Carnegie Mellon University)

Figure 3: IoT Security & Privacy label example, showing (a) primary layer and (b) secondary layer.

Linked to the ability to identify and represent the trustworthiness of hardware components that are utilised within other products as part of the supply chain, Hoque et al. (2020) propose a trust metric to enable comparison of the countermeasures used within hardware design and production. Unfortunately, however, the concept is not explored in any depth within the work concerned and is not supported by any direct indication of how it would be implemented and utilised.

4. Case example: Automotive sector

The digitalisation of vehicle technologies and systems has triggered huge changes in the sector. Current cars have more than 150 electric control units and they embed up to 100 million lines of software code, which could triple by 2030. These advancements come with higher cybersecurity risks, since hackers could access a vehicle's data and electronic systems threatening the vehicle's safety and the customer's privacy (UNECE, 2020). There are specific systems closely connected to the core physical characteristics of the vehicle. At the same time, user-accessible systems contain personal and confidential information. If any of these systems are compromised, the vehicle's information and control sector is at danger and the risk of damage or theft is high. In response to this scenario, security has come a long way since the advent of basic technologies like vehicle alarms and keyless access,. Now the security elements in automobiles must not just encompass data protection and physical access but also include critical safety systems such as power steering and drive-by-wire braking systems. Since the control systems or modules of automobiles are becoming highly integrated, there is no such thing as safety without security (Soja, 2014).

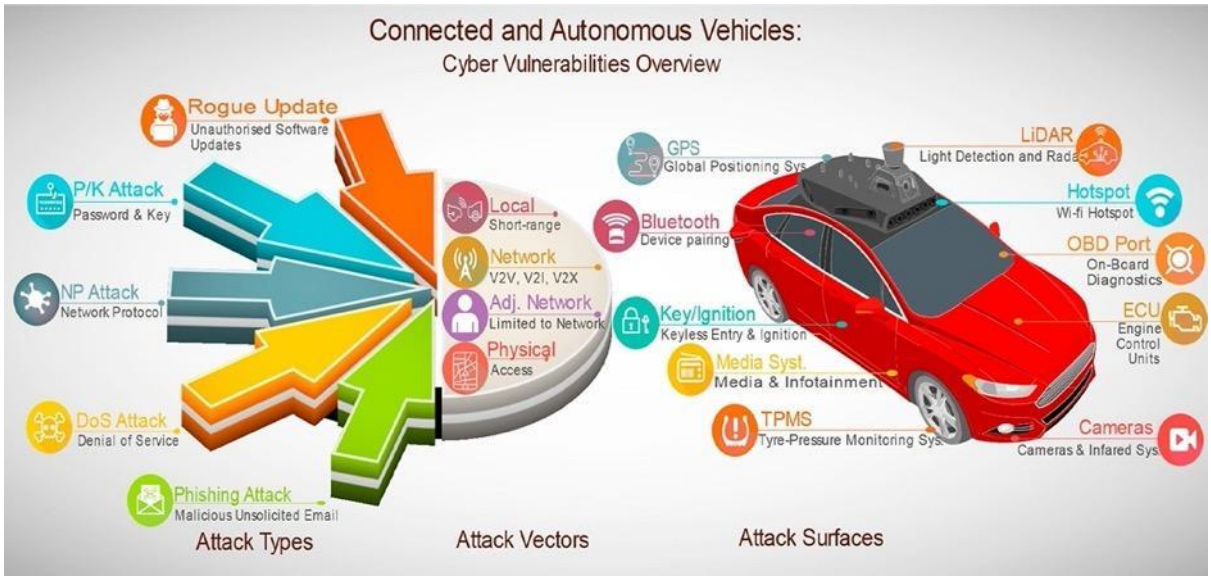
4.1. Practices and Principles of Hardware Security in Automotive Industry

Suppliers, dealers, drivers, owners and manufacturers of automobiles today face an undeniable and clear threat of cyber-attacks, particularly for Connected and Autonomous Vehicles (CAVs). Growth in the automotive industry, vehicle-to-infrastructure/vehicle connectivity, and advancement in autonomous driving make data privacy and computer security cornerstones for customer confidence and the automobile industry's continuation and success. Software and hardware play a significant role in automobile safety, functionality and value, from stability control to electronic fuel injections, theft prevention and navigation (McAfee, 2017).

The security of CAVs depends on both software and hardware components. However, the security of software components often depends on the security of the underlying hardware. For example, an in-vehicle communication network relies on an array of electronic control units (ECUs), sensors, actuators and interfaces. While the main goal of a CAV is to minimise road accidents and the loss of life due to human error, another set of vulnerabilities is introduced while designing and manufacturing CAVs with inherent defects or vulnerabilities (Sheehan et al., 2019).

Automobile safety can be classified into active and passive safety. The objective of active safety is to prevent crashes, while the objective of passive safety is the safety of the vehicle's occupants in the event of an accident; passive safety is also known as crash-worthiness. Multiple possible risks in an automobile are continually monitored by active safety features. If a problem arises, continuous working active safety features rectifies the problem automatically. Active safety systems and devices are almost mostly automated and improve the level of protection in a car. Some of the basic active safety systems include the braking system, visibility, cruise control, lane departure warning, electronic stability, door open warning, park assist, reverse assist, and dashboard warning signals and minor design aspects (Hamsini and Kathiresh, 2021). Compromised hardware can negatively impact safety features.

Figure 4 shows known areas of CAV vulnerabilities, attack vectors and surfaces. Most cyber-attacks are perpetrated through a CAV's software systems to compromise behaviour of the vehicle's physical/hardware components.



(Source: Sheehan et al., 2019)

Figure 4: Overview of cyber-attack types, attack vectors (or modes) and CAV attack surfaces.

To protect the buses and ECUs, several hardware security building blocks are employed in a variety of ways. These hardware security features and practices include software attested secure boots, software attested keys for automobiles and examined digital signatures, which help to quickly detect manipulation in boot loaders and tampering with files. Any invalid or manipulated files are prevented from being executed, establishing a secure basis for the ECU's operation long before it is infected by altered data (Hamsini and Kathiresh, 2021).

The computer security industry has developed a vast range of hardware security building blocks which provide security to the ECUs and buses. Trusted execution technologies such as TPMs are a particularly good example of a hardware security system. This technology makes use of cryptographic methods to generate a unique identification for every permitted feature in an automobile. This unique identification allows a precise comparison of the parts of a start-up environment against well-known valid sources and successfully halts the execution of code that is not original and does not match with original coding (McAfee, 2017).

Another hardware security feature is tamper protection. This feature encrypts the most valuable information and data in automobiles, such as encryption keys, account credential, intellectual property and other critical information at compile time. The information is only decrypted when it is required during a brief execution window. Tamper protection also prevents the reverse engineering of important information. Another main hardware security

feature is cryptographic acceleration, which offloads encryption tasks to specialised hardware, and boosts cryptographic performance (Intel and McAfee, 2015).

There are two other hardware security features which are considered vital in terms of the overall security of automobiles: The first one is active memory protection, which helps to prevents buffer overflows that might be exploited by malicious code. It does this by incorporating pointer-checking capabilities into hardware. The second one is to imprint an identifier directly on an automobile or device. This feature allows manufacturers to identify each device's unique identity, providing secure identification and barring unauthorised devices from accessing the automakers' network or systems. Intel EPID (Enhanced Privacy ID), which may be incorporated into Intel and other CPUs, maintains anonymity by enabling devices to be confirmed as part of a group rather than by their unique identifier (McAfee, 2017).

The UK government has also set out some principles for security systems in the automotive industry. These principles are created by the Centre for the Protection of National Infrastructure (CPNI) with the help of the Department of Transport. These principles are specifically designed for the automotive industry, ITS and CAV ecosystems, including their supply chains. There are eight main principles. The first principle suggests that the security of an organisation is governed, owned, and promoted at the board stage. The second principle focuses on the need for proper assessment of security risks and their appropriate and proportionate management which also includes the security risks which are specific to the supply chain. The third principle places emphasis on the aftercare of products that have already been manufactured by automotive companies and mandates regular check-ups of security features to make sure that the systems are secure throughout their lifetime (HM Government, 2017).

The fourth principle suggests cooperation between all companies involved in the supply chain, including suppliers, sub-contractors, and third parties to enhance or upgrade the security of systems. This would also be lucrative for all of the parties involved in the automotive business. The fifth principle focuses on the importance of design and the approach automakers should take to design the systems in such a way that security is ensured in the design stage. This is also known as a design-in-depth approach. The fifth principle focuses on coding practices and the importance of secure software systems and their management throughout the lifecycle of an automobile. The seventh principle entirely focuses on the storage and transmission of data. The data stored on vehicles is confidential, and the security of the vehicle depends on it. Therefore, the incoming and outgoing communication and transfer of data must be done securely and should be controlled fully by the sender and recipients. The eighth principle focuses on the automation of an automobile's security features. The systems which are designed by automakers should withstand or be able to recover from an attack instantly by themselves and respond in an appropriate manner when their sensors or defence systems are disabled or not working properly (HM Government, 2017). It is possible to highlight that amongst the abovementioned principles, 2, 4 and 5 would be collectively applicable to DSbD, and would provide the foundation for upholding some of the other principles (e.g. 6-8).

4.2. Regulations, Guidelines and Standards for Hardware Security in Automotive

Efforts are being made around the world to improve and regulate automotive security. At present, many countries have legislative proposals such as those by the United States Congress, China's ICV Initiative, the European Union Cybersecurity act and new guidelines for automotive manufacturers in Japan by JASPAR. These standards and guidelines share a focus on improving cybersecurity in the automotive industry through compulsory regulation (Escrypt and KPMG, 2020).

Regulation that is being introduced further increases the emphasis on cybersecurity and hardware security for vehicles, and is increasingly trying to harmonise and standardise national regulations. To manage and ensure vehicle security, the United Nations (UN) has set up an organisation named The World Forum for Harmonization of Vehicle Regulations, which is also known as WP.29. This organisation works within the institutional framework of the UN, and it functions as a global platform for deliberating and setting out standards and regulations for motor vehicles. Apart from this there are two other big entities that work together and define the management system in automotive security, the International Organization for Standardization (ISO) and SAE International. The most recent UN regulations on cybersecurity and updates for vehicle improvement have been adopted by the UNECE World Forum for Harmonization of Vehicle Regulations in agreement with 54 countries including the EU, Japan and South Korea (UNECE, 2021).

These newly adopted regulations will come into force by 2022. The first regulation that is to be adopted, UNECE WP.29 TF-CS/OTA, makes it necessary for vehicles to meet cybersecurity compliance requirements. This involves two basic requirements, the first of which is the operating of a certified cybersecurity management system (CSMS) and the application of CSMS in all sorts of vehicle types at the time of approval. The second regulation, which is regulated by UNECE alongside TF-CS/OTA, is ISO/SAE 21434. This is a standard for the cybersecurity of automobiles, and it has already been adopted by the International Organization for Standardization (ISO) and SAE International. ISO/SAE 21434 is similar to CSMS, and its main purpose is to defend automobiles from cyber assaults. This standard places emphasis on having an appropriate security organisation and having suitable methods throughout the vehicle's life cycle (Escrypt, 2020).

The new guideline by the UN sets a benchmark for automotive manufacturers in terms of the performance requirements for vehicles and the requirement for regular audits of a vehicle's IT, hardware and software security. This is the first ever binding and harmonised international standard in the automotive sector. Automotive makers are required to take specific measures as per the UNECE regulations such as managing the cyber-threats to automobiles, reducing risk around the value chain by securing the vehicle in the design and development stage, detecting and defending against intrusion for the whole fleet of vehicles, and providing secure software and hardware updates. This works alongside the regulatory framework created for Over The Air (OTA) updates (Escrypt and KPMG, 2020).

These new regulations are set out to be compulsory by the UN, and provide a framework for assisting the automotive industry to manage security risks in the design stage. They also ensure verification that risks are tested and handled properly, alongside regular risk

assessments, the monitoring of security attacks and the provision of effective responses to them. The regulations also mandate the dynamic analysis of attempted or successful attacks, and manufacturers' responses to new vulnerabilities and security threats. Homologation authorities and national technical services will audit the automakers in order to see if they fulfil these requirements (Marty, 2021).

Most secure and encrypted systems presently available are those that can withstand scrutiny — in other words, open source cryptography algorithms and security specifications that do not need to be kept secret and are freely available in the public domain. A variety of specification initiatives are ongoing or have matured enough to be adopted as standard within the automotive engineering industry. For example, the Secure Hardware Extension (SHE) specification, which was created in 2008 by Escrypt for luxury car brands like BMW and Audi in partnership with the HIS Working Group and Freescale, is now accepted as a standard for security in the automotive industry. The SHE standard specifies a collection of functions and an application programming interface (API) that enable a secure zone to interact with any electronic control unit in automobiles. These characteristics assist to increase flexibility while lowering expenses. The design of the SHE implemented on Freescale's MPC5646C is a single-chip microcontroller is geared towards body control applications, where security functions may be employed for car and ECU theft prevention, such as the activation of an immobiliser (Stumpf, 2018).

There are various projects commenced by the EU to set out guidelines and regulations for the automotive industry. One of the biggest projects was EVITA[5], which focused on generating rules for automotive ECUs. The guidelines mostly focused on verification, as well as designing and prototyping a wide range of security architectures. Some of the biggest automotive companies such as Fujitsu, Bosch, Infineon and BMW were involved in the EVITA project. The entire functionality of the EVITA project revolved around three stages of hardware security methods: complete, medium and light. It also defined complex parameters and functions for handling and controlling security keys, as well as the decryption and encryption of procedures. The entities that were involved in the EVITA project later launched a new project named PRESERVE. The aim of this project was developing, implementing and testing a measurable security subsystem for vehicle-to-infrastructure and vehicle-to-vehicle application which was later called V2X (EVITA, 2011).

An example of a security standard and regulation covering both software and hardware security in the automotive sector was the Federal Information Processing Standards (FIPS) developed by National Institute of Standards and Technology (NIST). FIPS introduces four levels of security systems ranging from level one to level four. Level one is a single security system that has no requirement for physical security, whilst a level four security system consists of protection against environmental attacks such as temperature and voltage (Soja, 2014).

The UK government has also set out some regulations and guidelines to be followed by the automotive industry. They have made it strictly essential for every party that is involved in the manufacturing supply chain, including retailers, senior level executives, engineers and

[5] See https://evita-project.org

designers. Everybody involved in the automotive industry in the UK is provided with a set of guidelines and regulations that need to be followed. The Centre for the Protection of Natural Infrastructure (CPNI) in conjunction with the UK Department of Transport have set out guidelines which are to be treated as regulations. Table 3 contains the regulations, guidelines, and standards for the automotive industry (HM Government, 2017).

Regulation/Standard	Brief Description
SAE J3101	Hardware-protected security requirements for ground vehicle applications.
SAE J3061	Implementing cyber physical vehicle systems and cybersecurity guide for implementation.
ISO 12207	Systems and software engineering – software lifecycle processes.
ISO 15408	Specifies a model for evaluating security aspects within IT and Evaluation of IT security.
ISO 9797-1	Message authentication codes: security approaches – defines a paradigm for secure message authentication codes based on block cyphers and asymmetric keys.
ISO 27001	Information security management system
ISO 27002	Code of practice – security – provides recommendations for information management.
ISO 27010	Information security management for inter-sector and inter-organizational communications.
ISO 29119	Software testing standard.
ISO 27034	Application security techniques – guidance to ensure software delivers necessary level of security in support of an organisations security management system.
ISO 29101	Privacy architecture framework.
ISO 27035	Information security incident management.
DEFSTAN 05-138	Cybersecurity for defence suppliers.
NIST 800-30	Conducting Risk assessment.
NIST SP 800-50	Building awareness and training programs for the information technology security.
NIST 800-88	Guidelines for media sanitization.
NIST SP 800-61	Computer security incident handling.

Table 3: Regulations, Guidelines and Standards for the Automotive Industry. *(Source: UK Department of Transport)*

5. Case example: Fintech Sector

Emergent technologies, including artificial intelligence, big data, robotic process automation, and blockchain, are innovating the way in which financial services are delivered. When applied collectively these are termed financial technologies or 'fintech.' The Financial Stability Board defines fintech as 'technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services' (FSB, 2017). Since its appearance in the twenty-first century, fintech has been growing progressively, and EY (2019) has estimated that one-third of consumers regularly use at least two or more related fintech services.

The adoption of fintech offers effectiveness, efficiency, convenience, and transaction processing benefits (Ryu, 2018) for customers. Economic benefits include lower transaction and capital costs compared with traditional financial services (Mackenzie, 2015). Convenience benefits include flexible access to financial services, enabling consumers to use smartphones and tablets to manage their finances at any time and from any location (Okazaki and Mendez, 2013). Increases in transaction process speeds accelerate rates of approval compared with traditional financial services, e.g., an approval process is now generally completed within 24 hours.

Benefits aside, the adoption of fintech also implies risks. These risks can be classified into financial, legal, security, and operational (Ryu, 2018). Financial risk describes the potential for financial losses. Legal risk refers to the lack of a single and universal regulatory framework for fintech, despite the global scale at which the sector operates. Security risk and operational risk describe all potential failures and losses originating from fraud or cybercrime, or from inappropriate internal processes within fintech companies.

Consequently, fintech policymakers as well as industry regulatory authorities are introducing a growing number of instruments aiming at regulating the sector and controlling the risks without compromising the potential benefits for customers and for the broader economy.

The regulatory framework here is complex, with different countries adopting different regulations and with various aspects in need of dedicated and specific regulation. While several reviews cover the regulatory framework for fintech related activities (see Crisanto et al., 2021; Restoy, 2021), the hardware side and the technologies enabling fintech have received less attention, and reports describing the overall regulatory framework for hardware security in fintech are missing entirely.

The next section introduces fintech and clarifies the similarities and differences between related activities, enabling technologies, and policy enablers. Subsequent sub-sections introduce the international regulatory landscape for fintech, with a specific focus on hardware security.

5.1. The international regulatory landscape for fintech

Several international organisations have proposed taxonomies and theoretical frameworks that characterise the fintech environment, related activities, technologies, and policy enablers. The Financial Stability Institute published a cross-country overview on the policy responses to fintech (Ehrentraud et al., 2002), focusing on seven fintech activities (digital banking, fintech platform financing, robo-advice, digital payment services, e-money services, Insurtech business models, financial activities related to crypto-assets) and on the six enabling technologies (application programming interfaces [API], artificial intelligence [AI], machine learning [ML], biometric-based identification and authentication [biometrics], cloud computing [CC], distributed ledger technology [DLT], 4G/5G telecommunications) identified in their framework. This report considers hardware security regulation at the nexus of fintech activities and enabling technologies. The authors argue that the policy response changes depending on the specific activity considered.

Digital banking is regulated in most jurisdictions by existing banking laws and regulations, with specific regimes in only a few jurisdictions. *Fintech platforms* face requirements that depend on the activities performed; the parties involved, and the risk management approach taken. *Robo-advice* has the same regulatory treatment that traditional advisers receive in most of the surveyed jurisdictions. *Digital payment services* and *E-money services* are regulated by fintech-specific regulations, because of the amount of risk involved. Specific regulations vary depending on the role and service provided. *Insurtech* business models have no specific licensing regimes or requirements, while regulatory and policy responses to crypto-assets differ considerably between different jurisdictions.

The report highlights how policy response changes depending on the specific technology considered. *Application programming interfaces* are regulated essentially with respect to granting access to data. Examples of this regulation in the EU are the Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 (EBA, 2018). *Cloud computing* is regulated in most jurisdictions through specific requirements relating to outsourcing, governance, risk management and cybersecurity. These requirements are often the results of a modification or a clarification of existing regulation. Only very few jurisdictions have issued specific regulations on *distributed ledger technology*, and similarly there are no specific regulatory requirements for the use of *machine learning* and *artificial intelligence* by financial institutions.

ENISA's Minimum Security Measures for Operators of Essentials Services [6] guidance incorporates banking and finance into its essential services list, alongside critical national infrastructure such as water and electricity supply. Consequently, the Directive on the Security of Network and Information Systems [7] (the NIS Directive) becomes applicable. It defines common security measures in terms of incident reporting and security measures for the operators of essential Services and digital service providers.

---

[6] See https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

[7] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

5.2. The UK general regulatory landscape for fintech

In the UK fintech is not governed by a single regulatory framework, and the firms that carry out activities such as consumer credit, banking and advising on investments will be authorised and regulated by one or more of the following bodies (GLI, 2020):

- The Financial Conduct Authority (FCA) – an independent public body funded entirely by the firms that it regulates that pay fees. It is accountable to the Treasury, which is responsible for the UK's financial system, and to Parliament. It aims to ensure that the relevant markets function well and does so through three operational objectives: protect consumers, protect and enhance the integrity of the UK financial system, and promote effective competition in the interests of consumers. The FCA acts as the conduct regulator for nearly 60,000 financial services firms and financial markets in the UK and the prudential supervisor for 49,000 firms, setting specific standards for 19,000 firms. It aims to make markets work well – for individuals, for businesses large and small, and for the wider economy. Any firm which carries out regulated activities by way of business in the UK will need to be authorised and regulated by FCA[8].

- The Bank of England (BoE) – the UK's central bank that must answer to the people of the UK through Parliament. It produces banknotes (cash), oversees many of the other payment systems and keeps the cost-of-living stable by changing the main interest rate in the UK. Moreover, through the Prudential Regulation Authority (PRA), it regulates UK banks and other financial firms so that they are safe and sound[9].

- HM Treasury (HMT) – the government's economic and finance ministry, maintainscontrol over public spending, setting the direction of the UK's economic policy and working to achieve strong and sustainable economic growth.[10] HMT sets the policy surrounding financial services and works closely with the BoE, FCA and PRA to maintain and develop the UK's financial services legislative and regulatory framework.

The nature of fintech activities as well as the scale and size of their business will determine the relevant regulatory framework from the UK regulators. In general terms, the **Financial Services and Markets Act 2000** (HM Treasury, 2018) is a key part of the UK's legislative framework for financial services regulation, which sets out the activities and entities that fall within the scope of UK financial services regulation. These activities are regulated and supervised by the two main financial services regulators: the FCA and the PRA. The legislation also provides the financial services regulators with the necessary functions and powers to grant authorisation to firms, to supervise their activities, and to enforce financial services requirements. These rules are detailed within the FCA Handbook of Rules and Guidance and the PRA's Rulebook. Fintech firms wishing to operate in the sector will need to identify the relevant rules for their business and comply with them. Failure to do so could result in significant fines and, for individuals, potential prohibitions from working in the industry altogether.

---

8 See https://www.fca.org.uk/about/the-fca

9 See https://www.bankofengland.co.uk/about

10 See https://www.gov.uk/government/organisations/hm-treasury/about

While, generally, the FCA and PRA's rules are technologically neutral, the rise in number of fintech firms in recent years has led to two important regulatory developments: greater clarity on the regulatory approach to crypto assets and **Project Innovate**. Launched by the FCA in October 2014, it includes three core innovation initiatives:

1) The Regulatory Sandbox: "a safe space where both regulated and unregulated firms can experiment with innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in such activity" (HM Treasury, 2017).

2) The Advice Unit: "to provide regulatory feedback to firms developing automated advice models with the potential to deliver lower cost advice to unserved or underserved consumers, following the Financial Advice Market Review (FAMR). The Advice Unit focuses on models in the investments, protection and pensions sectors" (HM Treasury, 2017).

3) The Innovation Hub: "helps new and established businesses (both regulated and non-regulated) introduce innovative financial products and services to the market. There are no restrictions on the areas of financial services covered by the Innovation Hub: firms innovating in mortgages, capital markets and pensions can all access the Innovation Hub for help in introducing their products to market. The Innovation Hub also performs a horizon-scanning role by identifying recent technologies and areas where the regulatory framework needs to adapt to enable further innovation in the interests of consumers" (HM Treasury, 2017).

Since issues relating to cryptocurrencies were raised throughout our consultations with sector stakeholders, it is also necessary to give some attention to the regulatory frameworks relating to virtual financial assets. The systemic risks posed by cryptocurrencies have grown as a concern for member states of the G20, a key objective of which is to maintain secure and sustainable growth of the global financial system. In the UK, cryptocurrencies have been divided into regulated and unregulated instruments. The UK has not published first-hand legislation to regulate the crypto space, instead extending its existing directives to neutralise challenges. For crypto assets to be regulated like the broader financial services sector in the UK, they must fall within the scope of the Financial Services and Markets Act 2000 (FSMA), or under the Payment Services Regulations 2017 (PSR) and the Electronic Money Regulations 2011 (EMR).

The Fifth EU Money Laundering Directive (5MLD)[11] came into force in January 2020, and has been integrated into the Money Laundering and Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The directive clearly holds "custodian wallet providers" and "virtual currency exchanges" accountable to the stipulations of 5MLD. While the regulatory instruments mentioned above do not necessarily link directly to hardware 5MLD has overlooked crucial members within the cryptocurrency market. For instance, miners have the required skills and capacity to initiate openings for invaders to exploit and

[11] See https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en

facilitate conditions for Money Laundering / Terrorist Financing. As key actors, they have the potential to join investments through the mining industry, which can be later sold for fiat currencies. This is an attractive opportunity for offenders to convert funds into cash holdings. Likewise, mining cryptocurrencies in the UK is legal, and no tailored legislation exists to regulate such activity. Therefore, miners should be included in the scope of regulation to enhance Anti-Money Laundering (AML) / Counter-Terrorist Financing (CTF) accountability. As such, mining activity presents a blind spot in existing legislative frameworks which may cause concerns attributable to hardware security considerations within the cryptocurrency regulatory space.

5.3. Fintech Hardware security

In addition to the described standards that refer to fintech in general, there are some regulatory frameworks that are relevant to IoT products, and therefore affect the security of hardware introduced into the market by fintech firms. There are three main regulations worth mentioning (IoT Security Foundation, 2020):

- The **Data Protection Act 2018** (DPA) controls how personal information is used by organisations, businesses or the government, and it is the UK's implementation of the General Data Protection Regulation (GDPR)[12]. Among other provisions, the DPA includes requirements related to automated decision-making to protect a subject's rights from decisions with legal or "significant" impact. This may be particularly relevant to fintech providers as fintech products and services can offer automation as a service for consumers or be incorporated within providers' business models.

- The **Consumer Rights Act 2015** (CRA) aims to 'consolidate, modernise and simplify consumer protection law in the UK.[13] The act includes a new section on consumer rights regarding digital content that is particularly relevant to fintech providers. Indeed, fintech providers may be liable for damages from low quality digital content like malware (IoT Security Foundation, 2020).

- The **Digital Economy Act** (DEA) is particularly relevant to fintech providers because they are subject to information sharing and processing requirements, and because their devices might receive marketing materials and spam subject to additional requirements (IoT Security Foundation, 2020).

Furthermore, **Regulation (EU) No 910/2014** of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal market replaced Directive 1999/93/EC. It applies to customer identity checks performed based on "documents, data or information from a reliable and independent source." It covers areas of hardware and software required for identity verification (e.g. smart cards, digital signatures and "electronic seal creation devices – configured software or hardware used to create an electronic seal). The main implication of this regulation for

[12] See https://www.gov.uk/data-protection for details.

[13] See https://www.cms-lawnow.com/ealerts/2015/10/financial-services-and-the-consumer-rights-act-2015

hardware is the requirement for interoperability across EU states where cross-border online services are used, which requires secure electronic identification and authentication.

The **Revised Directive on Payment Services ("PSD2")** helps enhance security by including multifactor authentication for online European payment card transactions while promoting the development of innovative online and mobile payments. The following authentication requirements are found in PSD2:

- requirements for a strong customer authentication and secure communication;
- elements which dynamically link transactions to a specific amount and specific payee;
- clear synergy with the 4th AML Know Your Customer (KYC)/Customer Due Diligence (CDD) requirements.

The US based 3DS2 meets the PSD2's authentication requirements by having support for biometrics and one-time passwords. It also integrates with mobile device authentication solutions such as Apple Pay.

Recent regulatory changes have been aimed at personal data protection. While not directly related to hardware security, but focusing on information processing practices, there are areas where hardware may be compromised by adversaries leading to loss of personal data. Examples of novel Privacy Regulations are: **GDPR, CCPA, PIPEDA, POPI, LGPD, HIPAA, PCI-DSS**. For example, PCI-DSS requires that assurance be provided to end users and financial organisations so that the risk of losses due to cyber threats are minimised. One particular area relevant to hardware security is the role that Hardware Security Modules (HSMs) play in ensuring PCI-DSS compliance. This is an instance where software and hardware security (and their respective regulation) are closely intertwined. Cryptography in financial transactions ensures endpoint authentication, transaction integrity and PIN verification. Such cryptographic processes use HSMs to ensure confidentiality, integrity and the availability of keys and transaction data. The role of HSM consists of generating and storing cryptographic keys compliant with FIPS 140-02 standards. As such, while the PCI-DSS regulatory instrument does not dictate constraints on hardware security, it does affect devices which support transaction processing and other fintech operations.

5.4. Counterfeit Hardware Threat Landscape

Being the top industry targeted by cyber-attacks, reports show the escalating costs spent on fintech as the percentage of gross revenue reaching at least 7%, the highest among all sectors of the economy (Eliot and Santos, 2011). Not only heavily affected by the direct losses of cyber threats, the financial industry is also adversely impacted by both direct losses and additional costs of cybersecurity overheads. Hardware threats have been known for decades to the sector. As the supply chains grow and manufacturing is largely outsourced, the threat becomes more complex and challenging to detect. The counterfeit typology, illustrated in Figure 5 shows the extent and variety of vulnerabilities introduced through counterfeits into the financial system worldwide (Guin et al., 2014).

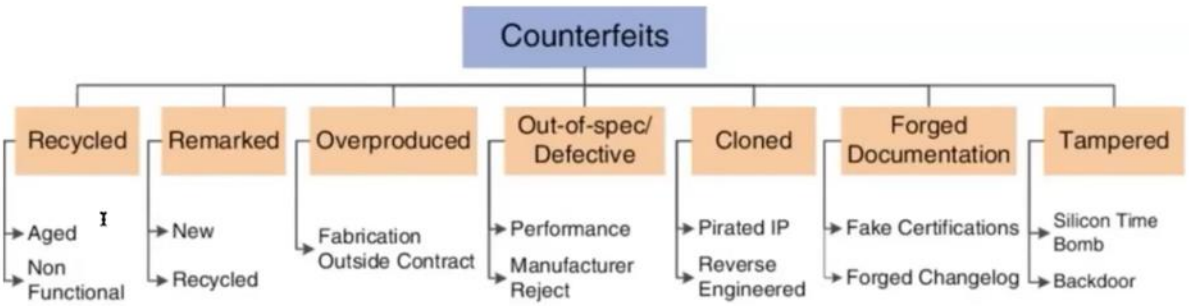


Figure 5: Typology of hardware counterfeit threats. *(Source: Guin et al., 2014)*

Countering the threats from counterfeit devices, the European Union and associated countries are working on the introduction of hardware certification schemes. For example, the ECHO Cybersecurity Certification Scheme developed by the EC, is a product-oriented cybersecurity certification scheme, supporting security requirements for sector-specific and inter-sector security requirements. According to the EU-proposed scheme: "Components are the basis for any electronic connected device. Certain security levels can only be achieved using certain certified components. A device can be characterised by its software and hardware. So, the evaluation could be performed by different stakeholders mainly because those products could have been manufactured by different entities, each one specialised on a component of the product itself." This effort is aimed at harmonising approaches to hardware security level assurance, but it will take some time to go through the legislative process and be accepted EC-wide.

6. Stakeholder Engagement and Fintech Workshop Summary

Throughout the literature review and analysis, dialogue with key stakeholders provided valuable input into the processes of the literature search and the validation of the analysis included into the final report. At the outset of the project, this included an opening conversation with one of the largest manufacturers of components for industrial connectivity. Encompassing fourteen different brands, the organisation designs, manufactures and markets a comprehensive portfolio of networking, security and connectivity technologies and products across a variety of industrial, enterprise and professional broadcast markets. This expert interview was held with the company's office in France and the guidance by the French National Agency for the Security of Information Systems (ANSSI) was identified as the core set of best practices recommended for IoT connectivity appliances in this geography. These devices are manufactured for the wider transport industry (for example, controlling bridges, railroads and traffic lights). It is worth noting that professionals solely focusing on hardware security were challenging to locate, which was one of the interview conclusions. We relied on quality interactions with key stakeholders and pursued leading professionals within the industries selected for the case studies.

Further, the automotive sector cybersecurity architects and experts in Governance, Risk and Compliance (GRC) were approached via a link with the Information Systems Audit and Controls Association. Two senior professionals from the UK/German car manufacturing alliance were interviewed. At the initial stage, we received information on the regulatory documents which formed the basis for the discussion in Section 4. In the second round, the use case draft was reviewed by experts and expanded by incorporating their feedback. Finally, the last engagement with participating stakeholders involved gathering their views on ways in which DSbD practices could be integrated in the field, which are reflected in the conclusion to this report.

Wider discussions were also held with the representatives of self-regulated sectors, such as defence. Their reflections were summarised in a series of emails, which informed conclusions about developing and adopting best practices in hardware security.

One of the key opportunities for collective stakeholder input into the regulatory analysis was the Fintech Workshop, which was held virtually via MS Teams due to the constraints of COVID-19. Leading experts in GRC working across the financial sector, technology and regulatory/trade association bodies were invited by targeted emails to attend the workshop. The invitation was also posted on LinkedIn via the Discribe Hub+ group. A total of eight participants coming from different sectors (Financial Crime, Fintech, Payment Industry, Consulting & Risk Management, BFSI, Finance, Financial Integrity Research, Payment Hub) and with roles related to cybersecurity attended the workshop.

The appendix contains details of the session plan and delivery materials for these sessions, and the discussion themes were introduced in accordance with this. Different members of the research team introduced and then facilitated different segments of the discussion, supported the synthesis of conflicting views and ensured the balanced participation of all the participants in the sessions. Other members of the research team acted as observers and note takers in the sessions that they were not leading, and did not contribute to the

discussions (so as not to distract from the input of the invited participants). The sessions were recorded and then transcribed. The resulting notes were then shared, summarised, and used for the validation and refinement of the initial findings in a plenary meeting between the members of the research team.

As the UK financial sector is highly regulated, discussions around the further introduction of regulatory frameworks have been extensive, while some elements of the conversations touched upon areas connected to emergent technologies that were outside the hardware context. An example is the theme of cryptocurrency, which is not directly relevant to the target topic, but which the participants were keen to explore. This additional theme has been added to the fintech use case in Section 5 and contextualised in terms of hardware-related regulation (or the lack of thereof).

It emerged that separating hardware/DSbD and software perspectives on regulation would be challenging as the software/hardware regulation perimeter is not clearly delineated.

As such, the material below is structured to reflect the discussion that took place, with the main sections aligning to the key themes that the workshop convenors introduced, and with the individual sub-sections then reflecting the topics raised and debated by the participants.

6.1. Recognition of existing 'regulation 'in hardware security

In assessing the nature of existing legislation, participants were asked to consider contemporary legislation relevant to the fintech industry, specifically related to the use, procurement and overall security of hardware, along with the motivation behind the formulation and design of these regulations and their protective qualities. In traversing these tangents, participants characterised the contemporary regulatory environment as encompassing both national level legislation and industry standards, both of which were considered to be reactive.

6.1.1. Isolating Hardware Security from Software Security Regulations

Attendees asserted that, as hardware is becoming increasingly software driven, it is difficult to distinguish between hardware and software when considering the contemporary regulatory environment. Secure chips, for example, are often driven by software developers, and remain secure through periodic software updates. In terms of regulations, secure by design assesses the security of the default state of equipment, entailing the people, process and overall technology (including hardware and software) involved in the design of a particular system. Omitting software security was likened to selling intruder alarms to a customer who has no locks, doors or windows – meaning that, however secure a given piece of hardware is, it remains vulnerable to exploitation if it is used to run vulnerability-laden software.

Cumulatively, while participants conceded that hardware security is a priority consideration when procuring hardware to run particular software, it was asserted that, as hardware becomes ever-more reliant on software, and the move towards cloud environments

continues to accelerate, any discussion of hardware security must encompass software in some capacity.

6.1.2. Legislation and Industry Standards

Discussions indicated that the contemporary cybersecurity environment within the fintech industry is not only defined by national-level legislation, but also industry standards. The key differentiator between these forms of industry regulations is that while national legislation is mandatory, industry standards, while effective for corporate marketing, are ultimately voluntary. Participants provided GDPR and the Financial Services and Markets Act (2000) (data protection and cryptocurrency respectively) as key examples of national level legislation, and pointed towards 'Secure by design 'and ISO/IEC 24643 regulations as relevant industry standards. Furthermore, participants contended that there are few regulations that relate to hardware security alone. Directly applicable legislation consists of a 'woolly' interpretation of GDPR and how compliance is achieved, along with the necessity to procure hardware that is 'secure by design' to store proprietary data or run corporate software.

6.1.3. Reactive approach

Participants contended that hardware security regulations in the fintech industry predominantly are reactive, entailing direct legislative responses to attack vectors deployed by threat actors. Reactive cybersecurity methods are not highly effective in preventing, or at least detecting and isolating known attack vectors, but fall short in addressing the inevitable emergence of new vulnerabilities and fostering secure operations in the first instance.[14] The concept of 'secure by design' was highlighted as one of the lone proactive regulatory initiatives in the fintech security domain, and perhaps the cybersecurity domain more generally.

6.2. Usage and impact of current regulation

Participants were asked to discuss their awareness of and compliance with existing regulations, which regulations they used on a day-to-day operational basis and to identify those which had the most significant impact on everyday operations. Overall, it was assessed that there is insufficient awareness of the nature and importance of cybersecurity regulations and standards in the fintech industry, and that regulations are generally utilised selectively, while customer experience and the financial bottom-line take precedence.

6.2.1. Insufficient Awareness

Despite considerable advances and investment in both the cybersecurity domain and regulatory environment, attendees contended that insufficient awareness of fast-paced technological change remains rife across the fintech industry. This, in part, stems from the failure of regulatory bodies to keep up with such changes and new development across the

[14] Sentient Digital Inc. (2020). Proactive vs Reactive Cybersecurity for your business. (Available at: https://www.entrustsolutions.com/2020/11/13/proactive-vs-reactive-cyber-security/).

cybersecurity and fintech domains. Once legislation has caught up with a specific attack vector or capability, the cybersecurity threat landscape has often moved on.

Attendees also indicated that the sheer quantity, and often contradictory nature, of international cybersecurity regulations in the fintech industry as contributing to an overall lack of awareness. Awareness of a particular granular regulation or piece of legislation is often contingent on whether relevant bodies have signed up to it, or their involvement in discussions surrounding its conception.

On the consumer side, participants highlighted the constant and sometimes incessant barrage of regulations within terms and conditions as fostering a degree of desensitisation to the terms that they are agreeing to.[15]

6.2.2. Drivers of compliance

Participants postulated that, despite the rapid growth in cyber fraud and exploitation in the fintech industry, industry compliance with hardware security regulations is ultimately driven by the principle of 'good enough' security and a rudimentary cost-benefit analysis – with regulations imposing financial penalties for non-compliance.

Attendees emphasised that compliance is not derived from an innate corporate desire to do good or protect customer data, but rather the path of least resistance and cost[16]. While benefits of a cheaper purchase are tangible (i.e. spending less money), the benefits of choosing a more secure and expensive option are comparatively intangible, characterised by the probability of a loss or breach occurring as a result of a cyber-attack, instead of a definitive and certain value. Achieving a regulatory environment not driven by cost considerations was considered as near 'blue-sky' thinking.

These cognitive heuristics manifest in the fintech industry through corporations, organisations and consumers prioritising the procurement of cheap and 'good enough' security hardware to meet minimum compliance standards, rather than prioritising security. Consequently, regulations prescribing a monetary penalty for non-compliance have achieved the greatest success. Indeed, in terms of GDPR, participants contended that organisations would adopt the path of least resistance if financial penalties were omitted. This also creates problems in constructing future regulations. Fintech corporations primarily seek to engage with economies of scale, while catering to the consumer demand for convenience over security. Future regulations must therefore balance impositions of security practice with the

---

[15] Faced with the choice of agreeing to the terms presented or sacrificing their capacity to use a given piece of software/hardware, consumers will, more often or not, agree to the terms regardless of their content, prioritising convenience over security. A Deloitte survey of 2,000 US consumers in 2017 found that 91% of people consent to terms of service without reading them, with this number rising to 97% for the 18-34 age demographic. In short, the swathes of regulations within terms and conditions have fostered numbed and unquestioning consumer compliance, and ultimately a glaring lack of awareness of what is being agreed to.

[16] In accordance with prospect theory – when individuals are contemplating purchasing a product or level of service, they are highly susceptible to cognitive biases, with decisions driven by risk and loss-avoidance rather than rationality.

enduring necessity for fintech companies to meet consumer demand for ease-of-use and convenience.

6.3. Suitability and sufficiency of existing regulation

Attendees were asked to consider whether existing regulations were sufficient in terms of their content, coverage and overall utility, whilst also indicating whether any regulations are outdated or not fit for purpose. Participants found existing regulations to be often contradictory and lacking in agility, resulting in a lack of overall awareness of the holistic regulatory landscape and legislation that is not fit for purpose (within the context of the participants' experience).

6.3.1. Contradictory Regulations

In assessing the suitability of existing regulations, participants reiterated the pervasive contradictions across standards and legislation. The financial services and fintech industry are so large that if a new piece of legislation is released not all companies have to sign up to it, leaving room for unaddressed vulnerabilities. Moreover, regulations are also often unique to national contexts, consisting of a microcosm of nuanced socio- and geo-political factors. Together, this formulates a regulatory environment saturated with a plethora of standards and regulations with inconsistent subscription and fragmented into national socio-political microcosms.

Those from a regulatory body background mentioned that tangible consequences of this environment include the capacity for financial dispute resolution services, including the Financial Ombudsman Service, to draw upon swathes of granular, and sometimes obscure, legislation on behalf of a corporation or customer to resolve a case, which a defendant or other relevant parties may not have had any knowledge of prior to entering into an agreement.

6.3.2. Insufficient Regulatory Agility

Hardware security regulations in the fintech industry are often outdated, as the regulatory environment cannot keep up with the pace of hardware innovation and development.

The rapid technological development in the digital and technology industry is both a blessing and a curse. Whilst enduring innovation provides a consistent stream of convenience-inducing technologies for consumers, regulatory bodies are currently being outpaced by a significant margin. As the enactment of new legislation requires consensus across a wide variety of regulatory bodies, technology simply moves at a far greater pace than regulations can be enacted. Though not directly related to hardware, an observation was made that currently there is no specific law for cryptocurrency in the UK, which means that the Financial Services and Markets Act (2000) and other e-money regulations from 2011 are the only pathways that exist to regulate the market. Resultantly, legislation is frequently outdated and consequently not fit for purpose.

Industry standards, unburdened to a degree with the bureaucratic processes endemic to legislative regulations, are far more agile. While standards are by no means keeping pace with technological innovation, they provide a richer picture of the fundamental industry direction of travel and are able to react far quicker to the changing cybersecurity landscape. As voluntary agreements, however, industry standards lack the tangible punitive incentive provided by national and international legislation.

6.4. Moving forward

In this concluding section, attendees were invited to discuss ways in which the regulatory environment can be improved, and whether the solution resided with the enactment of stronger and more severe regulations. Participants highlighted the harmonisation of standards and regulations with enhanced monitoring as a possible way in which the hardware security regulatory landscape could be improved, and critiqued the effectiveness of enhancing the severity of regulations as a means to improve overall compliance and security.

6.4.1. Harmonisation of Standards and Regulations

A common trope in discussions was the necessity for the overall harmonisation of hardware security standards across industry sectors. Formulating holistic approaches to cybersecurity in the fintech domain is immensely complex whilst each nation constructs their own regulations. Nation-states often have their own data protection regulations which, while sharing much of the regulatory content with GDPR (around 80% in some cases), are distinguished by often granular nuances, influenced by differing national socio-political contexts. This makes cross-compatibility extremely difficult.

Participants highlighted harmonisation as essential to tackling emerging threats to secure operations in the fintech industry.[17] Participants considered wider cooperation in raising the minimum encryption requirements for systems in the fintech sector as the most effective approach in enhancing resilience and combatting this threat.

Attendees, however, questioned whether the global harmonisation of regulations was realistic or utopian. Conceptualisations of cybersecurity are wholly derived from the unique geopolitical and social contexts that are associated with the contemporary socio-political environment in each given nation, which are often ideologically incompatible with each other. Indeed, the inability to formulate a harmonised vaccine policy during the COVID-19 pandemic, characterised instead by self-interest and vaccine hoarding,[18] suggests that a coordinated and consistent approach to hardware security may be unlikely.[19]

---

[17] Quantum computers, for example, can rapidly crack existing industry standard EMV encryption standards. If threat actors are able to develop quantum computing capabilities, most likely at the nation-state level, this risks the confidentiality, integrity and availability of the global financial system.

[18] World Health Organisation (WHO) (2021). WHO Director-General's opening remarks at the 148th session of the Executive Board. (Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-148th-session-of-the-executive-board).

[19] For example, western nations may be concerned about Chinese hardware brands for fear of backdoors put in by the Chinese government, whereas Chinese companies may similarly suspect American hardware for fear of backdoors put in by the NSA.

This fragmentation was illustrated using blockchain technology as an example. In cryptocurrency, blockchains obscure the origins of transactions, and the general movement of currency. While this enhanced privacy and anonymity may be beneficial on the individual level, it may also facilitate anonymous fraud and tax evasion, which becomes increasingly problematic as cryptocurrency is adopted more widely. In tackling this issue, certain countries may prioritise anonymity in the blockchain, whilst others may prioritise the ability to trace transactions to prevent fraud and tax evasion. These approaches are incompatible and may inhibit initiatives to achieve a harmonised regulatory solution.

6.4.2. Enhanced Monitoring of Transactions

There was consensus that greater monitoring and recording of individual transactions in real time would enhance the effectiveness of existing legislation. If the entire transaction process can be digitalised in real time and transactions traced to their origin, the capacity for threat actors to carry out fraudulent activities and other financial crimes, including terrorist financing, would be severely hampered. In an inversion of overall industry trends – this would require technology to catch up with existing regulations.

It was noted, however, that this system only functions effectively with collective buy-in. Universal compliance is immensely difficult to achieve across 8 billion people and 300 million companies. If financial institutions lack sufficient Know Your Customer (KYC) policies,[20] for example, the capacity to track threat actors conducting financial fraud or other financial crime is compromised. Moreover, in an integrated financial system, trust is paramount, and without universal guarantees that money received in transactions is legitimate in nature and origin, then trust breaks down and the system collapses.

6.4.3. Enhanced Regulatory Agility

Attendees also highlighted that, akin to software, a consistent or periodic amendment to legislation is required in order to maintain hardware security resilience. A consistent updating of legislation would also encompass adding layers to an organisation's defensive posture, facilitating Defence in Depth.

This can only be achieved if legislation maintains pace with technological innovation and attack vectors employed by threat actors. Further, participants suggested that this had greater probability of success if channelled through voluntary compliance with industry standards grounded in empirical research.

[20] Know Your Customer, sometimes defined as Know Your Client, is the mandatory process of identifying and verifying the client's identity when opening an account and periodically over time. In other words, banks must make sure their clients are who they claim to be, and can refuse to open an account or halt a business relationship if the client fails to meet minimum KYC requirements. Source: Thales, "Know Your Customer in Banking." (Available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/issuance/id-verification/know-your-customer).

6.4.4. Is more severe legislation realistic?

Participants questioned the degree to which enhancing the severity of legislation, for example in the form of expanding and enhancing monetary fines for non-compliance, would enhance the overall hardware security regulatory landscape. It was asserted that regulation will always be necessary to establish the lowest common denominator to which the industry must comply with, as compliance will never stem from corporate morality.

Moreover, existing empirical research indicates that the banking sector has carried forward overheads for investment in both hardware and software controls and assurances in the cybersecurity domain directed towards addressing cybersecurity and posture.

6.5. Recommendations and Conclusions

Overall, participants identified a security regulatory environment in dire need of change and innovation. Hardware security, inherently intertwined with software security, is defined by both national and international legislation and industry standards, and is predominantly reactive in nature. Moreover, this regulatory environment is characterised by insufficient awareness and is driven by rudimentary assessments of cost and the path of least resistance. Its effectiveness is also hindered by contradictory regulations and the sub-standard agility of regulatory bodies in responding to emerging threats and industry trends. To reform hardware security regulations, attendees advocated for the harmonisation of standards and regulations, enhanced monitoring of transactions and expanding transactional monitoring capabilities, albeit conceding that some of these aspirations may be utopian. These recommendations and conclusions by no means offer a panacea for rectifying the innate wrongs of the hardware security regulatory environment, and instead form a summation of a sample of industry perspectives on how the regulatory environment can be improved.

7. Discussion and Conclusions

The project has determined that regulation in this context is difficult to specifically identify and can exist in many forms. Notably, some of these forms do not have a formal regulator and are instead driven by what the industry itself judges to be good practice.

While there are sector-specific regulations to be considered, it is notable that related awareness did not emerge strongly from the stakeholders' interactions.

In both the workshop and wider discussions, it proved hard to separate discussion of hardware and software regulation. The delineation that exists within academia between hardware security and systems security was not typically followed by the participants. For example, GDPR is not seen as a regulation relevant to hardware security, whereas any vulnerability in the hardware or the hardware supply chain that leads to the leakage of personal data is almost certainly insecure in a more general context. To have industry adopt hardware security regulations it may be helpful to clearly define hardware as a separate layer of abstraction for the purposes of regulating it.

This raises the question of how to move things forward and ensure both wider awareness and uptake. Discussion during the wider industry consultation led to an observation from one of the contributors regarding the approach by which previous standards have managed to achieve uptake. Looking at the ISO 9000 quality standard as a case in point, it was noted that the Ministry of Defence (MOD) was a key influencer over wider uptake as one of the first organisations to set a requirement for compliance. While adoption of the standard led to push back from affected suppliers, it was ultimately realised that meeting the standard was the only means to get an MOD contract, and this in turn had a knock-on impact throughout the supply chain.

There is certainly no guarantee that cybersecurity will be a sufficient basis to prompt a market response. This is illustrated by another MOD-related example from the same era – namely the VIPER microprocessor back in 1987. VIPER was specifically designed for use in safety-critical systems, and was claimed to be the first commercial microprocessor design to have been proven to work (MacKenzie, 1991). However, it ultimately failed due to a lack of market demand. Looking at a modern-day security example, albeit from a non-hardware perspective, we can cite the relatively slow progress of the Cyber Essentials scheme.[21] Despite having been around for over 7 years, the level of awareness about it remains relatively low, with the Cybersecurity Breaches Survey 2021 suggesting that only 14% of UK businesses are aware of it (DCMS, 2021). While this proportion rises to 45% and 50% in medium and large organisations, this is still only reaching half of them, and if this is reflecting *awareness* then the level of *compliance* is likely to be significantly less. This is despite Cyber Essentials Certification being a requirement if organisations wish to bid for government contracts involving the handling of sensitive and personal data or relating to the provision of certain

[21] See https://www.ncsc.gov.uk/cyberessentials/overview

technical products and services, which in turn suggests that the scope of the compliance obligation is not yet broad enough to make a significant difference in the wider community.[22]

The above leads to potential lessons in terms of driving the adoption of DSbD, which represents a level beyond that normally expressed in standards and guidance. Unfortunately, factors such as current awareness and the nature of market forces clearly mean that success will depend upon more than it being a 'good thing to do.' The market – in terms of both technology manufacturers and adopters – will require evidence and incentives for persuasion. Having strong regulation prescribing DSbD could be such an incentive.

The Industrial Strategy Challenge Fund has recently issued a call for business-led demonstrators of DSbD, with the intention of delivering products or services in which capability enabled hardware is shown to provide a more secure solution.[23] However, while this will clearly be useful as part of an overall evidence base in support of DSbD, the challenge is not just to have exemplars to show that it works and succeeds at the technical level. Wider adoption will depend upon it working more easily or more profitably, or it being encouraged by a different means.

Given the context of this review, it is relevant to consider the implications of the findings for the practical DSbD initiative that Discribe is supporting, with the CHERI architecture and Morello demonstrator. The CHERI architecture aims to increase security by design, by having a more secure chip architecture (Woodruff et al. 2014). The use of capabilities in CHERI allows for compartmentalisation, limiting the effect of security vulnerabilities. Morello provides a prototype implementation, demonstrating the feasibility of this architectural approach.[24] Based on our findings, it is clear that awareness of hardware security is fuzzy in at least parts of the industry, and it is therefore likely that the security benefits of such capability hardware may not be a sufficient incentive by itself. At the same time, the potential benefits of using CHERI for crucial components in the financial and automotive sector are clear – in both contexts there are critical operations that may run alongside more open (and vulnerable) processes. As regulation can provide an incentive for adoption, it would appear desirable to have some form of regulation prescribing the use of technology like CHERI for critical components. Such regulation can come through legislation, standardisation or other forms of self-regulation.

Returning to the feedback from our participants, it was observed that an effective approach in other contexts has been to take a targeted approach of:

- Finding a domain that really needs to address a particular risk;
- Identifying the route(s) this domain uses to 'regulate';
- Identifying a key user group/organisation that leads in the domain, where a potential solution would offer them market advantage;

---

[22] There are practical aspects to consider, insofar as if Cyber Essentials compliance *was* to become a statutory requirement, it would raise significant questions about the ability of many businesses to meet the level as a result of costs and lack of skills.

[23] See https://apply-for-innovation-funding.service.gov.uk/competition/865/overview#summary for details of the call for expressions of interest, which ran from March-May 2021.

[24] See https://developer.arm.com/architectures/cpu-architecture/a-profile/morello

- Identifying key guides/standards (requirements) in the domain that should be enhanced or augmented, and which could be traceable to the solution(s);
- Pursuing the user group/organisation route to regulation to support the enhancement of the guides/standards.

For our purposes, the 'solution' element could be capability enabled hardware as a specific technology, or DSbD as an underlying approach. In either case, however, the process is easier said than done, but adopting a strategic approach clearly has more prospect of success than simply relying upon an expectation of 'build it and they will come.'

Of the specific sectors examined in this study, the automotive context would seem most immediately likely to provide a suitable domain. Not only is there already significant use of embedded technologies within vehicles, but the current transition to CAVs has the potential to offer a timely opportunity to spotlight security concerns and to drive the adoption of DSbD-based approaches.

8. References

Baumgarten, A., Steffen, M., Clausman, M. and Zambreno, J. 2011. *A Case Study in Hardware Trojan Design and Implementation. International Journal of Information Security*, 10(1), pp.1-14.

Bartock, M., Souppaya, M., Savino, R., Knoll, T., Shetty, U., Cherfaoui, M., Yeluri, R., Malhotra, A. and Scarfone, K. 2021. *Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases*. Draft NISTIR 8320. May 2021. https://doi.org/10.6028/NIST.IR.8320-draft

Boyens, J., Paulsen, C., Moorthy, R. and Bartol, N. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. NIST Special Publication 800-161. April 2015. http://dx.doi.org/10.6028/NIST.SP.800-161

California Legislature. 2018. SB-327 Information privacy: connected devices. Senate Bill No. 327. Chapter 886. 28 September 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Common Criteria. 2017. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1, Revision 5, April 2017. https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Crisanto, J. C., J. Ehrentraud, and M. Fabian. 2021. "Big Techs in Finance: Regulatory Approaches and Policy Options." FSI Briefs 12 (March).

DCMS. 2021. *Cybersecurity Breaches Survey 2021: Statistical Release*. Department for Digital, Culture, Media & Sport. 24 March 2021. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

Diamond, T., Grayson, N., Paulsen, C., Polk, T., Regenscheid, A., Souppaya, M. and Brown, C. 2020. *Validating the Integrity of Computing Devices: Supply Chain Assurance*. National Institute of Standards and Technology and The National Cybersecurity Center of Excellence. March 2020. https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/tpm-sca-project-description-final.pdf

Dun & Bradstreet. 2019. *Compliance And Procurement Sentiment Report*, July 2019. https://www.dnb.com/content/dam/english/business-trends/DNB_Compliance_and_Procurement_Sentiment_Index_Report.pdf

EBA. 2018. *Regulation and Policy – Single Rulebook*. European Banking Authority. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2%23:~:text=Regulatory%2520Technical%2520Standards%2520on%2520strong%2520customer%2520authentication%2520and,security%2520of%2520payment%2520services%2520across%2520the%2520European%2520Union

ECSO. 2016. *European Cybersecurity Industry Proposal for a contractual Pubic-Private-Partnership*. European Cybersecurity Organisation, June 2016. http://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf

Ehrentraud, J., Garcia Ocampo, D., Garzoni, L. and Piccolo, M. 2020. *Policy Responses to Fintech: A Cross-Country Overview*. FSI Insights on policy implementation No 23, January 2020, Financial Stability Institute. https://www.bis.org/fsi/publ/insights23.pdf

Eliot, D and Santos, A (2011) *Estimating the Costs of Financial Regulation*. Monetary and Capital Markets Department, International Monetary Fund (IMF). pp 1- 42. Available at: https://www.bis.org/events/bokbisimf2012/session4_estimating.pdf

Emami-Naeini, P., Agarwal, Y. and Cranor, L.F. 2021. *Specification for CMU IoT Security and Security Label (CISPL 1.0)*, 17 January 2021. https://www.iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf

ENISA. 2017. *Hardware Threat Landscape and Good Practice Guide*. European Union Agency for Cybersecurity. 8 February 2017. https://www.enisa.europa.eu/publications/hardware-threat-landscape

ENISA. 2020. *Cybersecurity Certification: Candidate EUCC Scheme*. 2 July 2020. https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

Escrypt. 2020. "UNECE WP.29 and ISO/SAE 21434: Automotive cybersecurity faces new challenges," 8 June 2020. https://www.escrypt.com/en/news-events/unece-wp29_iso-sae-21434

Escrypt and KPMG. 2020. *Cybersecurity full speed ahead: How digitalization and automation are presenting automotive manufacturers and suppliers with new security challenges*. Whitepaper. https://www.escrypt.com/sites/default/files/2020-02/200225_ESCRYPT_KPMG_Whitepaper-WP29_EN_0.pdf

EVITA. 2011. "Presentation Slides from the Final EVITA Workshop on Security of Automotive On-Board Networks." Deliverable D1.2.5.2, E-safety vehicle intrusion protected applications (EVITA) project. 23 November 2011. https://evita-project.org/Publications/EVITAD1.2.5.2.pdf

EY. 2019. *Global FinTech Adoption Index 2019*. EYG no. 002455-19Gbl. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf

Fagan, M., Megas, K.N., Scarfone, K. and Smith, M. 2020a. *Foundational Cybersecurity Activities for IoT Device Manufacturers*. NISTIR 8259. National Institute of Standards and Technology, May 2020. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf

Fagan, M., Megas, K.N., Scarfone, K. and Smith, M. 2020b. *IoT Device Cybersecurity Capability Core Baseline*. NISTIR 8259A. National Institute of Standards and Technology, May 2020. https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259a.pdf

Fagan, M., Marron, J., Brady, K., Cuthill, B., Megas, K. and Herold, R. 2020c. *IoT Non-Technical Supporting Capability Core Baseline*. NISTIR 8259B. National Institute of Standards and Technology, December 2020. https://csrc.nist.gov/publications/detail/nistir/8259b/draft

Fagan, M., Marron, J., Brady, K., Cuthill, B., Megas, K. and Herold, R. 2020d. *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline*. NISTIR 8259C. National Institute of Standards and Technology, December 2020. https://csrc.nist.gov/publications/detail/nistir/8259c/draft

Fagan, M., Marron, J., Brady, K., Cuthill, B., Megas, K. and Herold, R. 2020e. *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government*. NISTIR 8259D. National Institute of Standards and Technology, December 2020. https://csrc.nist.gov/publications/detail/nistir/8259d/draft

Fazzari, S. and Narumi, R. 2019. "New and Old Challenges for Trusted and Assured Microelectronics," Defense Technical Information Center, 25 March 2019. https://apps.dtic.mil/sti/citations/AD1076110

Federal Office for Information Security. 2007. *Guidelines for Developer Documentation according to Common Criteria Version 3.1*, Version 1.0. Bundesamt für Sicherheit in der Informationstechnik. https://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf

FSB. 2017. *Financial stability implications from FinTech: Supervisory and regulatory issues that merit authorities 'attention*, Financial Stability Board, 27 June 2017. https://www.fsb.org/wp-content/uploads/R270617.pdf

GLI. 2020. "Fintech 2020 United Kingdom," Global Legal Insights, https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/united-kingdom

Guin, U., Dimase, D. and Tehranipoor, M. 2014.*A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment*. Journal of Electronic Testing: Theory and Applications. 30. 25-40. https://doi.org/10.1007/s10836-013-5428-2

Hamsini, S. and Kathiresh, M. 2021. "Automotive Safety Systems." In: Kathiresh M., Neelaveni R. (eds) Automotive Embedded Systems. EAI/Springer Innovations in Communication and Computing. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-59897-6_1

Hastings, A. and Sethumadhavan, S. 2020. "WaC: A New Doctrine for Hardware Security," *Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security (ASHES'20).* Association for Computing Machinery, New York, USA, pp127–136. DOI: https://doi.org/10.1145/3411504.3421217

HM Government. 2017. *Principles of Cybersecurity for Connected and Automated Vehicles*. 6 August 2017. https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

HM Treasury. 2017. *Regulatory Innovation Plan*. April 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/606953/HM_Treasury_Regulatory_Innovation_Plan.pdf

HM Treasury. 2018. *The Financial Services and Markets Act 2000 (Amendment) (EU Exit) Regulations 2019: explanatory information*. 21 December 2018. https://www.gov.uk/government/publications/draft-financial-services-and-markets-act-2000-amendment-eu-exit-regulations-2019/the-financial-services-and-markets-act-2000-amendment-eu-exit-regulations-2019-explanatory-information

Hoque, T., Slpsk, P. and Bhunia, S. 2020. "Trust Issues in COTS: The Challenges and Emerging Solution," *Proceedings of the 2020 on Great Lakes Symposium on VLSI (GLSVLSI '20)*. Association for Computing Machinery, New York, USA, pp211–216. DOI: https://doi.org/10.1145/3386263.3407654

Intel and McAfee.2015. *Automotive Security Best Practices: Recommendations for security and privacy in the era of the next-generation car*. White Paper. https://www.infopoint-security.de/medien/wp-automotive-security.pdf

IoT Security Foundation. 2020. *IoT Cybersecurity: Regulation Ready*. https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Cybersecurity-Regulation-Ready-White-Paper-Full-Version.pdf

ISO. 2013. *Information Technology — Security Techniques — Code of Practice for Information Security controls*. International Standard ISO/IEC 27002:2013. Second edition 2013-10-01

Levine, E.V. 2021. *The Die Is Cast*, Communications of the ACM, 64(1), pp56-60.

MacKenzie, D. 1991. *The Fangs of the VIPER*, Nature, vol. 352, 8 August 1991. pp467-468.

Mackenzie, A. 2015. *The Fintech Revolution*, London Business School Review. 26(3), pp50-53.

Marty, K. 2021. "UNECE WP.29 / R155 –How Cybersecurity will impact the automotive market as of June 2022," CertX AG, 1 April 2021. https://certx.com/automotive/unece-wp-29-r155-how-cyber-security-will-impact-the-automotiva-market-as-of-june-2022/

McAfee. 2017. *Automotive Security Best Practices.* https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf

Microsoft. 2021. *Security Signals*. Hypothesis Group / Microsoft. March 2021. https://www.microsoft.com/en-us/secured-corepc

MSTIC. 2019. "Corporate IoT – A Path to Intrusion," Microsoft Threat Intelligence Center. 5 August 2019. https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

Mulligan, D.K. and Schneider. F.B. 2011. "Doctrine for Cybersecurity," *Daedalus*, (140)4, pp70–92.

NCSC. 2018. "Supply Chain Security Guidance," National Cybersecurity Centre, Version 1.0, 16 November 2018. https://www.ncsc.gov.uk/collection/supply-chain-security

NCSC. 2020. "Supplier Assurance Questions," National Cybersecurity Centre, Version 1.0, 17 December 2020. https://www.ncsc.gov.uk/guidance/supplier-assurance-questions

Okazaki, S., and Mendez, F. 2013. *Exploring Convenience in Mobile Commerce: Moderating Effects of Gender*, Computers in Human Behavior. 29(3), pp1234-1242.

Restoy, F. (2021) *Fintech Regulation: How to Achieve a Level Playing Field.* Bank of International Settlements. Financial Stability Institute. No 17, February 2019, pp. 1-21. Available at: https://www.bis.org/fsi/fsipapers17.pdf

Ryu, H.S. 2018. "Understanding a Benefit and Risk Framework of Fintech Adoption: Comparison Of Early Adopters And Late Adopters," in Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS), January 2018.

Sheehan, B., Murray, F., Mullins, M., Ryan, C. 2019. Connected and autonomous vehicles: A cyber-risk classification framework, Transportation Research Part A: Policy and Practice. 124 pp523-536.

SOGIS. 2010. *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*. Version 3.0. SOGIS Management Committee, 8 January 2010. https://www.sogis.eu/documents/mra/20100107-sogis-v3.pdf

SOGIS. 2011. *SOGIS IT-Technical Domains*. Version 0.93. SOG-IS Recognition Agreement Management Committee, February 2011. https://www.sogis.eu/documents/mra/SOGIS-IT-Technical-Domains-v0.93.pdf

Soja, R. 2014. Automotive Security: From Standards to Implementation. Freescale White Paper.

Stumpf, F. 2018. "Automotive Security from the Inside Out." https://www.etas.com/data/RealTimes_2019/rt_2019_1_58_en.pdf

UNECE. 2020. UN Regulations on Cybersecurity and Software Updates to Pave the Way for Mass Roll Out of Connected Vehicles. https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll

UNECE. 2021. WP29 World Forum for Harmonization of Vehicle Regulations (WP.29). https://unece.org/transport/vehicle-regulations/wp29-world-forum-harmonization-vehicle-regulations-wp29

Weston, D. 2021. "Windows 11 enables security by design from the chip to the cloud," Microsoft Security Blog, 25 June 2021. https://www.microsoft.com/security/blog/2021/06/25/windows-11-enables-security-by-design-from-the-chip-to-the-cloud/

Williams, C. 2016. "Today the Web was Broken by Countless Hacked Devices – Your 60-Second Summary," The Register, 21 October 2016. https://www.theregister.com/2016/10/21/dyn_dns_ddos_explained/

Wood, D. 2020. "What Your Company Needs to Know About Hardware Supply Chain Security," DARK Reading, 27 February 2020. https://www.darkreading.com/endpoint/what-your-company-needs-to-know-about-hardware-supply-chain-security-/a/d-id/1337084

Woodruff, J., Watson, R.N.M., Chisnall, D., Moore, S.W., Anderson, J., Davis, B., Laurie, B., Neumann, P.G., Norton, R., Roe, M. 2014. "The CHERI capability model: Revisiting RISC in an age of risk" https://www.cl.cam.ac.uk/research/security/ctsrd/pdfs/201406-isca2014-cheri.pdf

Appendix – Workshop materials

This appendix provides details of the materials used to support the workshop activities, namely the plan that investigators used for structuring the session and the slides that were used to support its subsequent delivery.

8.1. Session Plan

Activity	Indicative timing

Introduction and scene-setting
 	
● Welcome and participant introductions
● The DSbD programme and the Discribe Hub (*very* briefly)
● The focus of our project
● The focus of the session and reminder of the Chatham House rule
● What we mean by regulation in the context of hardware security. We can break down relevant regulation into two main categories:
  ○ Regulation that provides restrictions or requirements on the sector in question (i.e. the regulation is relevant, because the sector needs to follow it)
  ○ Regulation that provides restrictions on the organisations that supply hardware to the sector (i.e. the regulation is relevant, because the sector relies on the hardware being compliant)
	15 mins

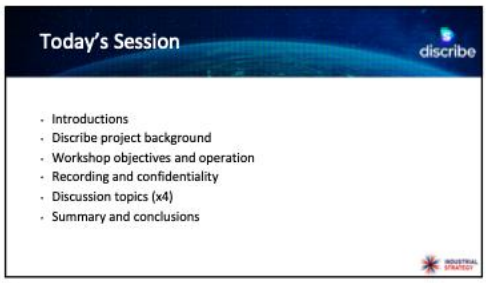
Discussion theme 1 – Recognition of regulations
 	
● What forms of regulation do the participants feel already exist that are relevant to this topic in terms of:
  ○ General regulations
  ○ Regulation specific to their sector
● What threats do you think the regulation in question is motivated by? Does it offer some protection against these threats?
	15 mins

Discussion theme 2 – Usage and impact of current regulation ● Is there sufficient awareness and use of existing regulation? ● Which regulations do you heavily rely on in everyday operations? ● Which regulations that you need to follow have the most impact on your everyday operations? (What are the most relevant operations?)	25 mins

Break	5 mins
Discussion theme 3 – Suitability and sufficiency of existing regulation • Are existing forms of regulation sufficient and appropriate in terms of content/coverage? • Do you think XYZ is a useful regulation? Would your organisation follow it if it weren't a regulation? • Are any regulations outdated (either no longer necessary, or have become ineffective over time)?	25 mins
Discussion theme 4 – Moving forward • What would be desirable to change in the future? • Is there a need for more or stronger regulation?	25 mins
Conclusions and next steps • A convenor-led summary of the key points (plus inviting participants to add any that they felt were missed in the summary) • A brief outline of the plans for how the findings will be used • Thanking the participants and drawing attention to the Discribe website as a place to watch for future developments	10 mins

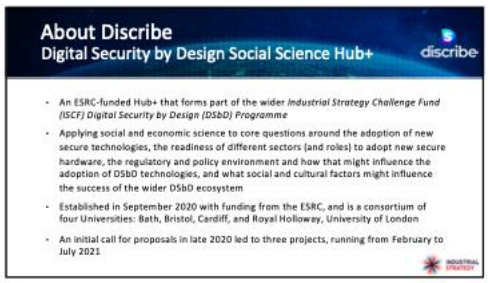
8.2. Workshop slides

1



2

3



4

5

6

7

8

During the session

- A shared Google Doc is available for you to record thoughts during the session

  https://tinyurl.com/u67txr3s

- Resulting notes will be anonymous, but feel free to use an identifier to signify your responses as coming from the same person

9

Recording and confidentiality

- We would like to record the session in order to enable reference back to the discussion
  - No comments will be identifiably attributed in later reporting
  - Recordings will not be retained beyond the relevant period for the work of the project
- The session is running under the 'Chatham House rule'
  - i.e. you can share the information you receive, but do not reveal the identity of *who* said it

10

'Regulating' the workshop discussion

- Feel free to be on or off camera, as you prefer, but please mute mics when not speaking
- In order to avoid talking over each other, please use the raise hand feature in Teams to indicate that you wish to speak
  - the moderator will watch out for raised hands and their order
- Can we please avoid the chat function, as it tends to distract the main discussion
  - If you have additional points that you wish to add, then please capture them in the Google Doc

11

Topic 1
Existing 'regulation' in hardware security

- What forms of regulation do you feel already exist that are relevant in terms of:
  - General regulations
  - Regulation specific to your sector
- What threats do you think the regulation in question is motivated by? Does it offer some protection against these?

12

Topic 2
Usage and impact of current regulation

- Is there sufficient awareness and use of existing regulation?
- Which regulations do you heavily rely on in everyday operations?
- Which regulations that you need to follow have the most *impact* on your everyday operations? (What are the most relevant/affected operations?)

13

5-minute break ☺

14

Topic 3
Suitability and sufficiency of existing regulation

- Are existing forms of regulation sufficient and appropriate in terms of content/coverage?
- Do you think existing regulations are useful?
  - Are there any instances that your think your organisation wouldn't follow if it weren't a regulation?
  - Are any regulations outdated (either no longer necessary, or became ineffective over time)?

15

Topic 4
Moving Forward

- What would be desirable to change in the future?
- Is there a need for more or stronger regulation?

16

Conclusions

- Summary of key points
- Final extra thoughts?

17

Thank you

https://www.discribehub.org

18