discribe

IMAGINING SECURE DIGITAL FUTURES

December, 2021

Economic & Consumer Chain Analysis of Secure Hardware Adoption

Final Project Report

Project Team: Siraj Shaikh, Simon Parkin, Muhammad Azmat, Andrew Tomlinson, Pantelitsa Markus, Laith Altimime, Paul Jarvie & John Moor

This work details the key findings of work conducted by the Discribe Hub+ commissioned project *Economic & Consumer Chain Analysis of Secure Hardware Adoption.* You can read more about the project by visiting https://www.discribehub.org/research-2-1-1

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

Contents

1 Introduction

Hardware security advances serve to improve secure implementation of digital systems. Realising such improvements depends on several non-technical factors, and will have to acknowledge cost-benefit perspectives across the cybersecurity ecosystem.

There is little at present to indicate who the ultimate decision-makers are regarding adoption of secure hardware, given the lack of studies that reveal the decision process that governs adoption of new hardware; there are examples of existing research which indicate factors of interest around the technical features of new hardware, for instance, for new Internet-of-Things devices [1, 2, 3]. What is less well understood is *who* it is that makes decisions around the adoption of new hardware.

Regarding secure software, there is a growing field focusing on developer-centred security (e.g. [4]). In comparison, there is a dearth of material on any particular decision-maker involved in secure hardware choices. This is exemplified by papers which identify criteria for selecting hardware (e.g. ([5, 6]). Of interest is whether altogether different criteria are also involved in deciding whether to take on newly-available hardware.

Moreover, there is a paucity in the literature on group actions around hardware adoption. Collective criteria for investment in cybersecurity at an association or sector level is underexplored. Regulation and regulatory gaps are recognised (e.g., [7, 8]), however the impact of trade associations, agreements and standards upon adoption of secure hardware remain unclear. This extends to the role of the supply chain on the adoption decisions; there are sectors where the supply chain is typically multi-tiered and complex, such as the Internet-of-Things (IoT) and automotive sectors [9].

Here we focus on the decision-making processes and incentives for investment in secure hardware by decision-makers. This includes direct investment needs and indirect costs such as business disruption and adaptations to business processes. This will serve to add detail to the concept of success and failure for security technology investments, and inform what are perceived as successful decisions and the reasons as to why.

To address these questions, we conduct a qualitative study with stakeholders in the hardware community. We examine the perceived drivers and barriers to adoption of secure hardware, through the lens of various stakeholders and decision-makers of this ecosystem. We conducted an interview-based study with 25 executive decision makers, senior technical managers, product evaluators and end-users of IT hardware. Through interviews with these stakeholders, we set out to understand the benefits of secure hardware adoption, and how such benefits are measured and perceived in terms of factors such as competitive advantage, value addition, and compliance. Equally, we explore the costs of security failures as may arise out of a lack of adoption of secure hardware, and where losses may be identifiable or intangible.

The questions addressed in this study are increasingly pertinent to cybersecurity, as implementation of security controls in software alone are deemed insufficient for the threats faced by digital systems, with security now also needing to be considered at the hardware layer [10]. Secure hardware has been considered for countering the risks of hardware Trojans, piracy of intellectual property (IP), reverse engineering, side-channels, and counterfeiting [11, 12]. Secure hardware typically provides some means of encryption, authentication, or secure boot at the chip-level [13], and is important in establishing a hardware-based root of trust and protection against physical attacks, especially side-channel and fault attacks, as well to provide

support for secure software.

The rest of the paper is organised as follows: The next section presents a review of related work regarding secure hardware adoption, potential adoption drivers and barriers, and the criteria that might be considered in the adoption process. Within this we note current gaps in understanding the decision making process. We follow this with an elaboration on the ecosystem of secure hardware production and adoption (Section 3). The research methodology is detailed in Section 4, including recruitment of participants, study design, ethical governance, and our approach to analysing the interviews. This is followed by a presentation of core findings from the interviews (Section 5), across themes identified from the engagement with stakeholders. To close the paper, we summarise the outcomes of the study and examine the implications (Section 6), before concluding with directions for further research (Section 7).

2 Related Work

In this section we consider existing research which has discussed potential motivators and drivers of secure hardware adoption, or potential barriers and hindrances to its adoption. Only a few of the studies are based on primary research (e.g., [7, 14]). Few studies present empirical surveys of adoption decisions.Moreover, we could find few case studies or examples of empirical research looking into the economics and decision processes for actual deployments of (secure) hardware. We have attempted to present discussions specific to secure hardware, though in some articles the discussion overlaps between that topic, general cybersecurity, information security and general technology adoption. This section is divided into two different sections, examining potential motivators for adoption, and potential impediments to adoption.

2.1 Potential motivators for adoption

Enhanced security. Rashid et al [13] highlight the role of secure hardware in providing a root of trust, support for software security, secure implementation of cryptographic algorithms and protection against physical attacks. A point is made that hardware security is in conflict with other performance optimisations, such as low power requirements, and note that performance optimisation is the most important design task, but is also the most important cause of information leakage.

Zhoa and Lie [15] compare hardware security and software security, proposing that although hardware solutions are more costly that this may be offset by the ongoing need for software updates. Further, hardware improvements offer promise of higher immutability (resistance to unintended change), privilege (ability to observe and control the operations of another component) and resource efficiency.

Markettos et al [16] consider existing approaches to processor design to be inadequate, and that traditional system security does not fit current computer architectures. Difficulties in relying on updates to preserve security, together with the long deployment and usage lifetime of IoT devices and their expected usage in the absence of human interference, are highlighted by Sidhu et al [17]; the authors propose that relying on software security alone is not adequate, and that secure hardware can provide a firm foundation on which to build a secure infrastructure.

Regarding benefits of secure hardware, the Ponemon Institute has conducted annual surveys for several years, examining the use of encryption by companies across multiple industry sectors (as with the 2021 report [14]). The most recent drivers include protection of customer information and intellectual property, and compliance with external privacy or data security regulations and requirements (including simplifying compliance audits). Concerning the use of Hardware Security Modules (HSMs), 61% of respondents indicated that their organisation had a centralised team that provided cryptography as a service to multiple applications/teams (i.e., a private cloud model). Thirty-nine percent indicated that each individual application owner/team was responsible for their own cryptographic services.

National benefits and national security. National security benefits might also be pertinent to secure hardware adoption. Levine and Pipikaite [18] recommend that hardware security should be approached cooperatively by the private and public sectors, to *"emulate well-established mechanisms in other engineering disciplines"*, such as civil engineering, wherein *"the public sector sets standards and controls while the private sector designs, manufactures, builds and sustains."*

An OECD 2021 [19] report to inform the G7 Panel on Economic Resilience, advises that: *"...greater attention is needed to ensure a safe and trustworthy digital environment, notably with respect to digital security..."* (p 103). The report warns that: *"the economic cost of more sophisticated attacks targeting the functioning of critical activities and infrastructure in the areas of defence, health, energy, banking, communications or transport could be very substantial"* (p 34). This suggests cross-cutting security concerns across sectors.

Market demand. The role of market forces with regard to secure hardware has been considered previously; Hastings and Sethumadhavan [20] propose that although consumers generally lack sufficient knowledge to consider an economic model for secure hardware adoption, with regard to Meltdown [21] the publicity allowed those consumers to knowingly choose between a Meltdown-susceptible processor (i.e. Intel) or a Meltdown-free processor (e.g. AMD). Similarly, Robert Potter [22] (Vice President for Mandiant Security Validation) notes that *"key stakeholders are placing increased pressure on companies to demonstrate with evidence how they invest in and use security technology to protect digital assets [...] and the overall value of the company."*

Avoiding the consequences of breaches. Bojanc and Jerman-Blažič [23] outlined methods for identifying the threats and vulnerabilities of ICT systems, proposing procedures for optimal investment in security technology. Regarding the economic consequences of security breaches, the authors state that indirect losses can have a long, negative impact on the customer base, supplier partners, financial market, banks and business relationships. Such losses include damage to the reputation of the organisation, interruption of business processes, legal liabilities, loss of intellectual property and damage to customer confidence.

Reporting on Reuters on the expected potential financial liability and reputational impact of the Intel Meltdown and Spectre security vulnerabilities, Finkle and Nellis [24] regarded the incident as likely to spur cloud companies to press Intel for lower prices, and increase its chip development spending to focus on security.

2.2 Potential impediments to adoption

Technical barriers. Butun, Sari and Osterberg [5] identify obstacles to secure hardware, including needing physical access to a device to work on it (and the relative time costs of this activity), hardware typically not being as flexible as software, and scale and production constraints. However, the authors conclude that hardware-based cybersecurity attacks are mostly (or perhaps completely) thwarted by hardware-based cybersecurity solutions, rather than by software-based solutions. They report that in the absence of adequate hardware security, as in the case of Intel hardware vulnerabilities (Spectre and Meltdown), software patches cost not only direct investment to address, but also introduced a performance degradation of up to 15–20% in the software-patched processors that were being used since.

Poudel and Munir [25] discuss security specifications for automotive Electronic Control Unit (ECUs) and the role of secure hardware elements in automotive embedded systems. The design constraints, they note, (including resource limitation such as memory, processing, bandwidth, and applications' real-time deadlines) provide limited freedom for the designer.

Hu et al. [26], in a review of hardware security, suggest that debugging is particularly challenging at the system and architectural level. This is due to the complexity of the design and the interactions with many disparate software and hardware components.

Hoeller and Toegl [27], in a paper on the security and dependability of Trusted Platform Modules (TPMs) in cyber-physical systems, cite the difficulty of creating an external diagnosis mechanism to guarantee that the TPM is working as intended, especially for ensuring that safety-critical, cyber-physical systems conform to safety standards. They report that a key component of this difficulty stems from the need to ensure the TPM functions are separated from outside systems.

Market impediments. Market forces are considered by Hastings and Sethumadhavan [20], who claim that recent hardware security 'woes' are not because of a lack of technical solutions but, rather, because such market forces and incentives prevent those with the ability to fix problems from doing so. They draw on the economics concept of a 'Market for Lemons', arguing that customers are unwilling to pay a premium for a feature or quality they cannot identify.

Concerns around a potential Market for Lemons in hardware security are echoed by Bojanc and Jerman-Blažič [23].

Costs. Hsu [28] states that Trusted Execution Environments (TEEs) are not widely utilised in cars today, other than as HSMs for secure boot. The main reason given is that HSMs are costly and non-scalable, especially since the car-maker has to rely on suppliers to customise the interface to each ECU.

Although TPMs and TEEs for vehicles generally cost less than $1 USD for the components [29], the cost of the hardware is used as a justification to have it removed from a bill of materials for a vehicle's ECU. Jester proposes that what must also be considered is that software security is often perceived as 'free' due the fact that it is only purchased as part of the overall software package.

Burton et al [8] considered causes for failure to rectify vulnerable systems, with regards to hand-held medical and fitness devices. The main causes included economic and oper-

ational barriers associated with manufacturers, for instance that use of software patches to update devices is economically attractive, with ease of implementation and relatively low up-front investment. Further, the perception of risk and attitudes toward investment associated with particular devices or sectors can influence motivation to secure hardware, compared to areas with higher perceived risk of attack for high financial gain, for instance. Regulatory gaps are also a factor, such as with fitness devices as a largely self-regulated industry.

Vulnerabilities and volatility in the hardware supply chain. Several authors have considered the hardware supply chain itself, examining supply problems or other vulnerabilities (such as Fazzari and Narumi [30]). Yasin et al. [31] cite reverse engineering, IP piracy, overbuilding (in terms of excessive security controls), counterfeiting, and hardware Trojans. However it is unclear whether such arguments will be perceived as barriers, or as motivation for considering better integrated security and more rigorous production chains.

Ramesh [32] proposed that a reduced time to market leads to greater use of off-shore labour for chip design, development and fabrication, complicating the oversight of production, most notably in maintaining trust in the end-to-end process, as well as concerns about recycling of components and intellectual theft. Levine [12] echoes these points with regards to ensuring hardware security in a complicated, globally distributed supply chain; a semiconductor manufacturer can now have more than 16,000 suppliers spread around the world, which they remark has: *"opened many windows of opportunity"* for modification or compromise of hardware, potentially without the knowledge of the original device manufacturers or their customers.

Rekha and Nagamani [33] point out that IP protection is challenging because IP is: *"usually transparent at system level in manufacturing facility"*. Zhang and Qu [34], at the time of their writing in 2019, cite surveys as showing intellectual property (IP) infringement to high-end chips, such as cloning and reverse engineering bringing the loss of approximately $250 billion and 750,000 jobs annually.

Mudassir [35] considers the subsequent post-Covid global shortage in semiconductors. The author notes that 70% of semiconductors are manufactured by Taiwan Semiconductor (TSMC) and Samsung, and that setting up a new semiconductor foundry presents a steep curve, likely costing US$10-12 billion, and taking three years to become production ready.

3 Background: Secure Hardware Ecosystem

The secure hardware ecosystem comprises a number of players in a complex global environment, to drive the proposition of secure hardware all the way to customers and end-users. While the focus of end user representation is purposed with working towards a secure digital economy and consumer protection, the predominant motivation for the rest of the ecosystem is commercial profit. The key markets are national security with a strong public sector as key customers, and secure products and services as part of the wider digital economy.

Novel secure hardware technologies are either entering the market with the proposition to disrupt the current cybersecurity technology status quo, or growing to organically form part of an existing software and hardware stack. Dominant players working towards the former are university research groups and startups; the pursuit of the latter is mostly driven by established

giants in IT technology and digital engineering systems.

3.1 Design and manufacturing

There are entities involved in the early conception of low-level (hardware) designs and concepts to overcome security challenges, representing the cradle of novel and innovative disruptions to the digital technology stack. Over the past two decades such players (very often universities and startups, but not exclusively) have had access to many challenge-led public funding sources and venture capital investment. Examples of such players in the UK include Cambridge University, involved in the CHERI (Capability Hardware Enhanced RISC Instructions) programme [36], and Arm who are involved in computer architecture design (developing a board based on CHERI known as Morello [37]).

Driving up the value chain, such designs and concepts are realised by manufacturers [38], including semiconductor fabrication labs and foundries, working towards integrated chips (ICs) and microcontroller units (MCUs). The global semiconductor supply chain is dominated by a handful of large players [39] including, for example, Taiwan Semiconductor Manufacturing Company, Limited (TSMC) and Korea-based Samsung, with further relatively smaller but high value-add manufacturers, such as the US-based Microchip Technology Inc. building Trusted Platform Modules (TPMs) and hardware-based cryptographic accelerators.

3.2 Systems integration

Integrating a complex product in this ecosystem is a substantial challenge, such that a modern automotive platform, for example, comprises a few tens of thousands of parts, assembled as a collection of bespoke and proprietary components, subsystems and systems, under hierarchies of feature sets, and functional and non-functional requirements. This is increasingly reflective of products and systems in healthcare, rail, aerospace and aviation, telecommunications, and mass consumer electronic products.

Tiered hierarchies of suppliers and integrators work towards Original Equipment Manufacturers (OEMs) who offer the ultimate branded value to the market. In the case of the automotive sector [40], as an example of a mature supply chain, a Tier-3 supplier may offer digital displays and plastics, on to a Tier-2 supplier who assembles some functional units (to play radio and music), who then offer it up to a Tier-1 integrator which builds a fully-functional fit-ready infotainment head unit (HU). Tier-1s would then deal with OEMs directly to allow for these HUs to be fitted into the final systems, that is, vehicles.

3.3 Consulting, evaluation and certification

The integration and engineering process is governed by a full spectrum of age-old traditions to explicit rules, involving historical trade secrets, industrial norms and practices, as well as trends and fashions associated with modern products. Oversight mechanisms also prevail, such as best practices and code of conducts, national and international standards, and legislation and regulation governing to address aspects of liability, insurance, consumer protection and na-

tional policy imperatives. There are as such a wide array of ecosystem stakeholders serving to guide, advise, enforce, regulate and certify according to relevant sets of rules and principles.

Continuing the automotive industry example [41], an HU is likely to be assembled in compliance with standards for digital interfaces and technologies, such as those for Bluetooth, WiFi, USB, CD/DVD and Digital Audio Broadcasting (DAB) Radio, following protocols set by the electronics and IT industry. Once the HU is delivered to an OEM, an independent safety and security assessor, such as HORIBA MIRA LTD. in the UK, would typically certify the integration of a HU into the electrical/electronic (E/E) architecture of a vehicle, according to international functional safety standards. Finally, national certification bodies, such as the Vehicle Certification Agency (VCA) in the UK, would conduct the final type approval testing and certification of the vehicle, with the integrated HU, to ensure the functional architecture is in compliance with relevant standards.

3.4 End users

End users in this ecosystem are essentially consumers of systems (such as automotive vehicles or healthcare products) or operators who provide some (digital or infrastructure) service directly dependent on such a system (such as a rail operator). Representation of such end user communities is often through campaign groups (for societal interests such as privacy, digital rights and consumer protection), and not-for-profit entities and trade bodies (championing industry interests in policy and working towards better stakeholder management). One such example is the IoT Security Foundation (IoTSF)[1] in the UK, who host the *Consumer IoT Security Special Interest Group (SIG)* with a mission to "improve the status of cybersecurity for consumers" with guides and training webinars. Government departments, working for regulation, and digital infrastructure and access, may also play an active role in this space, where the UK's Department for Digital, Culture, Media & Sport (DCMS) is one example, having worked to ensure consumer products and smart IoT devices are more secure, with security built in from the start as part of their *Secure By Design* initiative[2].

4 Methodology

Our aims are to investigate decision factors in the adoption of secure hardware, across a range of relevant stakeholders. We pursue these aims directly, through semi-structured interviews with 25 senior technical staff and company executives drawn from the hardware ecosystem. The study necessitated several considerations and commitments, as outlined in this section.

4.1 Scope of secure hardware

For the purposes of this study, and the basis for our participant recruitment, the scope of secure hardware [13] includes concepts and technologies that fall under physical, structural and behavioural domains of hardware abstraction layers. This covers enhanced hard-

[1] https://www.iotsecurityfoundation.org/

[2] https://www.gov.uk/government/collections/secure-by-design

ware Instruction-Set Architectures (ISAs), Trusted Platform Modules (TPM), Hardware Security Modules (HSMs), Trusted Execution Environments (TEE), Physical Uncloneable Functions (PUF), Random Number Generators (RNGs), System-on-Chip (SoC) analytics, physical quantum computers, and tamper-resistance and proofing.

The above scoping definition was consistently used to support identification of professionals as candidate participants for our interview study, with the hardware classifications acting as reference points for the semi-structured discussions. Having clear definitions of terminology in studies of security and privacy technologies is a key aspect of being able to understand the perspectives of participants [42].

4.2 Participant recruitment

To enable direct access to relevant industrial communities, two trade associations acted as partners to recruit interviewees from cross-sector stakeholders:

- **SEMI**[3], which is the globally leading semiconductor association, representing electronics design and manufacturing supply chain stakeholders. It has a strong reach across a number of sectors including manufacturing, automotive and mobility, healthcare technologies, and AI.

- **TechWorksUK**[4], which is the UK industry association serving as a national hub for technology, particularly automotive electronics (AESIN), IoT security (IoTSF), electronics manufacturing and systems (NMI), and power electronics.

Combined across the two bodies, this represented a membership of several tens of thousands professionals. While the interview invitations went through the two bodies, the actual recruitment was not limited to their membership, as a number of venues and forums used to promote the study attracted non-members equally. All interviewees were qualified on the basis of their involvement in decisions pertinent to secure hardware adoption, deployment, development, and procurement. The qualification was achieved through both trade body representatives and pre-interviews (in some cases to reaffirm alignment with the scope of the study) conducted by the authors.

As mentioned above, establishing shared points of reference for the interviews was critical. Understanding participants' background relative to the subject of study is also important for later making sense of the outcomes [43]. Some additional qualification for participation was then established at the start of each interview, to arrive at broad alignment on the notion of secure hardware. Of note is that most participants described secure hardware by the functionality typically offered by secure hardware modules, such as encryption, root of trust or a trusted execution environment. Some of the participants cited specific instances, including HSMs, TPMs, and consumer product examples of these, for example *"Trusted platform modules, either for a desktop laptop environment, or premium servers"* (P12), or *"a kind of system on a chip, or a part of a chip that is hardened to stop people getting information out of it, so TPMs, HSMs, that kind of class. But also the devices you find in your phone."* (P25).

[3] https://www.semi.org/

[4] https://www.techworks.org.uk/

4.3 Ecosystem representation and interviewee profile

We strived for an effective representation drawn from stakeholders across the ecosystem. Participants are professionals working at organisations ranging from large multinationals to small early-stage startups (both represented in approximately equal measure) and across the ecosystem. We consider the participants as representing distinct stakeholder categories, as below, and include an indication of the operational context and sectoral focus for each category.

- **Design and Manufacturing [P1,P5,P6,P10,P11,P13,P14,P16,P17,P24,P25]**: The biggest group of participants, the sample includes a mix of small and large organisations, including some very early-stage startups. The range of business maturity was also reflected in the diversity of views on value propositions offered by secure hardware technologies, which for this group ranged over telecommunications, consumer electronics, automotive, Unmanned Aerial Vehicles (UAVs), and manufacturing systems.

- **Systems Integration [P7,P12,P15,P22]**: With the exception of one niche player, the rest of this group comprised of major global Tier-1 integrators and OEMs operating in automotive, transport, instrumentation and sensor technologies, and control systems. One of the organisations is one of the world's leading systems integrator operating across almost engineering and technology sectors enabling a range of mass consumer products to critical infrastructure.

- **Consulting, Evaluation and Certification [P3,P4,P8,P18,P21,P23]**: This was the most diverse group, including a commercial research centre associated with a university, alongside national certification bodies and technical evaluators and assessors. Activities cover a wide variety of sectors across consumer devices in health, electronics, mobile phones and enterprise devices, alongside more complex engineering sectors including automotive, maritime, manufacturing and energy systems.

- **End Users [P2,P9,P19,P20]**: Two of the organisations represented industrial and consumer end user communities, with one deeply involved in Industrial IoT (IIoT) deployment and operations. Again, experience represented a broad range of sectors.

The study aimed to ensure a fair representation of diversity in the individuals sampled for interviews, ensuring age, disability, race, gender, religion, and sexual identity were all protected attributes.

While the majority of participants were located in the UK, some were based across Europe and US. Participant job roles were across C-Level executives (including CEOs, CTOs and Chief Engineers), and others designated in senior capacity (such as Project Manager, Technical Lead/Manager, and Senior Consultant).

Understanding current events around a study of security and privacy technologies is important, for putting participant responses in context [42]. Of note then is that the interviews took place between early April 2021 and late July 2021; this time period overlapped with two significant disruptions affecting the activities of the interviewees and their industries:

- The **COVID-19** pandemic affecting a number of businesses in terms of staff availability due to furloughs, change in business strategy due to market shifts, and workplace culture due to increased home-working and digital dependence, and;

- The ongoing global **chip shortage**, observed as having begun in 2020. While somewhat related to the previous disruption due to an increased demand in digital devices and PCs, the cause of this can also be attributed to the *concentration problem* of chip manufacturing [35], in that well over two-thirds of global chip supply is associated with only two semiconductor manufacturers, namely TSMC and Samsung.

Both of the above arose in several interviews, as security of supply [44], trust in the supply chain and access to physical engineering and manufacturing sites overlapped with some of the discussions.

4.4 Ethical governance and data management

The study was approved by the Ethics Committee at both Coventry University and TU Delft prior to participant recruitment. Interview accuracy and anonymity was ensured through a predefined interview protocol. All interviews were conducted using an institutional Zoom account, with each participant interviewed individually (except in two instances where two of the participants from the same organisation joined the call together, as for P5/P6 and P19/P20).

Interviews were audio-recorded and subsequently transcribed, and an anonymisation check conducted to remove any personally identifiable or company identifiable information which may have entered into conversation. Two interviewers were present at each interview, thereby facilitating the monitoring of fair practice, while also allowing the second interviewer opportunity to delve into any information that the first interviewer might have missed. Copies of the anonymised transcripts were approved by the participants before being released to the team for subsequent analysis.

In accordance with the ethical approvals, all data collected during the interviews was processed and stored in accordance with General Data Protection Regulation (GDPR) obligations, with Coventry University serving as the Data Controller. As such, all information collected on the participants was kept strictly confidential, and interview data referred to by a unique participant number. All audio recordings were destroyed once they were transcribed, and stored securely.

4.5 Study design

The study was designed to be conducted through an open-ended, semi-structured, on-line interview to gather opinions, experiences and ideas concerning the topic under investigation. The interviews were scheduled for one hour, with a few running up to 1.5 hours. While following the semi-structured format, there were just under a dozen core questions in the script to allow for key perspectives to be gathered; Table 1 details the questions in the script, with the first and last questions serving as opening and closing prompts respectively. The design of the interview question set was informed by existing research, as summarised in Section 2. The semi-structured nature of the interviews meant that topics were not necessarily visited in sequence as in the table.

Table 1: Core questions asked during the semi-structured interviews. Each question formed the focus for a deeper discussion with the participant.

Interview Questions	**Scope and context**
1) We'd like to know what the term "secure hardware" means to you.	Opening question to determine the participant's understanding of secure hardware.
2) Is this aspect of secure hardware something that you are concerned with in your job or role?	Participant is asked to elaborate on decisions they are engaged in.
3) Does secure hardware have a role in any systems you are currently involved with?	The role(s) of secure hardware, reasons for its consideration, and the roles and processes in the adoption process are subsequently discussed.
4) What do you see as being the main benefits of secure hardware adoption?	Participants are asked what benefits they perceive in a secure hardware approach. Participants are encouraged to discuss all benefits that might have been achieved or envisaged, including also economic and governance aspects.
5) How do you feel the benefits are perceived? Are they measured or calculated?	Discussion to uncover any methods, measurements and processes for determining or quantifying the potential benefits.
6) What do you feel are the costs or detrimental impacts of security failures arising out of a lack of secure hardware?	Here the participants are prompted to discuss costs that may be identifiable or otherwise intangible.
7) Do you feel there are any value gains likely from software add-ons and developer platforms on top of enhanced security of hardware?	Participants are asked whether any other value gains have been observed.
8) What do you feel might offset (or diminish) such value through various stages of the use case lifecycle, including at development and operational stages?	Uncover any value offsets from secure hardware, including subsequent upstream practices. Here, if not already mentioned, participants will also be asked whether the processes of integration and firmware upgrades lead to any notable problems, insecure integration, or misconfigurations.
9) What do you feel would be the main challenges or obstacles to adopting secure hardware for products?	Participants are asked whether they have encountered any challenges and obstacles concerning the adoption of secure hardware.
10) Do you feel the secure hardware supply chain itself currently presents any obstacles or barriers?	Examine aspects of the secure hardware supply chain and associated stakeholders and processes.
11) Is there anything that has not been discussed that you think is important for deciding whether to implement secure hardware in a product?	Closing question that gives the participant the opportunity to discuss topics not already covered which they believe are important, or review aspects they feel need more discussion. This also serves as a debrief for participants.

4.6 Data analysis

Once interviews were transcribed and anonymised transcripts produced, one author conducted reflexive thematic analysis [45] to identify themes within the interviews. Thematic codes were created and consolidated into a codebook, which was reviewed by all authors at intervals and adjusted, towards producing a final codebook. At the close of the analysis process, seventy-two codes had been produced based on content in the interviews, which were used to tag themes across the participant transcripts to identify cross-cutting topics of interest.

Themes were grouped into the following categories: **Business Decisions** identified descriptions of processes and roles involved in the relevant decisions made by companies. This included codes tagging discussion of: cost-benefit evaluation, identification of market opportunities, supply chain issues such as chip provision, indirect incentives to the business, externalities, measurement of efficiency, and the roles and position of the decision-maker (including internal stakeholders); **Adoption Decisions** including discussion of aspects deemed by the participant to be drivers or barriers to adoption, such as risk reduction, security assurance, compliance, cost, and resources; **Adoption Criteria** describing system requirements or external factors regarding the choice of solution, such as deployment requirements, environmental constraints and system constraints; **Activities** ranging across system development or implementation, such as requirements analysis, system development, testing, integration, certification and deployment; **Technologies** where participants had mentioned specific hardware, software, firmware or platforms.

5 Findings

Here we describe the prominent themes which emerged across the topics identified from the analysis of interviews (Section 4.6).

5.1 Perceived drivers

Several participants (P12, P13, P25) discussed the influence of market forces such as supply and demand and associated commercial pressures as driving security implementation. One participant (P12) felt that *"big commercial organisations like Samsung"* were more likely to be *"moving with market forces"*, though they also felt that this was of comparable relevance to other very different sectors such as the military, since they would in turn get the *"fallout from what's widely used in the civilian domain"*.

Marketing and PR benefits of being an early adopter were also stated by one participant, who felt it important that their company could say they were *"going above and beyond what the rest of the industry is doing "* (P25). P25 also countered the view of consumer demand driving adoption. Citing parallels with the sale of IoT devices on Amazon, where *"the ones that are most popular are the cheapest ones with the lowest sort of security properties"* , they stated: *"I think the market has chosen and decided they don't care about security, even though they might say they do. They care more about price when push comes to shove"* (P25). In all, these statements point to different drivers being applicable for different stakeholders and not only their economic drivers, but also potentially their organisational identity and goals.

Moving from internal to external drivers, commonly cited as drivers for secure hardware, and cybersecurity in general, were compliance, standards and regulation. These were raised by every participant in one way or another. At the extreme were views that compliance was the only significant driver for secure hardware adoption, as echoed by a range of participants: *"people don't tend to do things [in cybersecurity] unless they are actually required to, either by a supply chain requirement or via governmental certification"* (P12); *"That's easy, if we go back to HSMs, the answer is compliance, regulatory obligation. And you can almost trace the sales from when various regulatory things were introduced, and that led to adoption of hardware"* (P17); *"the business says, "as long as I'm compliant with regulations, I should be safe, or I should be secure"* (P10).

These last excerpts illustrate that compliance and regulatory needs can motivate change, but also define a clear minimum standard to be met. In this way, compliance was seen as impactful across industries and sectors. This was reported for the financial sector, for instance, where *"the fines for non compliance, for not just cybersecurity but for everything, are enormous"* (P24), and the automotive, defence, and national infrastructure sectors: *unless it's compliance related, it's a nice to have.* (P2);

The role of compliance and standards was also framed in a collaborative way, by P25: *"I think that the way to solve this is really through policy. It's the industry getting together, governments getting together and saying here are a set of standards, here are a set of kite marks or, you know, kind of quality marks to put on things"* (P25). P12 illustrated how definitions of expectations in regulation can promote movement in markets:

It comes down to regulation and market requirements. So if for instance it was [a public sector] procurement and they were going to replace all the laptops [...], and they came out said "Look they're gonna have to have a TPM 2.0 chip on", you know damn sure all the manufacturers make sure there's a TPM chip on those computers. (P12)

This was echoed by P20:

I would kind of expect most private sector organisations, unless they were particularly security focused, just generally wouldn't be putting an awful lot of thought into it i.e. secure hardware. Generally the regulation side of things is probably doing the primary pushing for critical national infrastructure cybersecurity. I don't think it's something that they would ever adopt out of choice. (P20)

In the automotive industry UNECE Regulation 155, ISO 21434 and GDPR were cited as important – see Table 2. UNECE Regulation 155 was noted as being a requirement to sell cars in some markets (P15), but as also being a driver as it was seen as stipulating the adoption of a cybersecurity management process (P18) and countermeasures to be in place (P7). Also cited as *"really driving people"* (P25) was ISO 21434 (as also summarised in Table 2). The role of GDPR was also cited as a likely push for automotive secure hardware since OEM revenue models are shifting towards service provision, implying processing more client data which needs to be kept private (P2).

The motivation of a compliance framework in making software development houses and hardware manufacturers consider their security assessments was noted by one participant, since for these companies it was also *"important for them to have the delivery time, you know, to have the product fast in the market"* (P4).

For the public sector, the importance of being able to refer to standards as part of the procurement process was highlighted, since it typically relied on the specification of requirements

Table 2: Below is a list of standards, regulations and best practices sources that the interview participants made critical reference to, when arguing motivation and alignment for their products and services. Our descriptions below include key aspects of these sources in reference to secure hardware concepts and technologies.

Standards and Best Practices	**Description**
UN Regulation No. 155 (Cyber security and cyber security management system)	Arising out of the United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations, launched in 2021 this global regulation is exclusively for road vehicles in the automotive industry and serves to address four key areas including managing cybersecurity risks, design measures to mitigate risks, threat detection, and over-the-air software updates. As such, secure hardware controls and design enhancements are relevant to all four of the areas covered.
ISO/SAE 21434:2021 (Road vehicles: Cybersecurity engineering)	Enforced in 2021, this is a global standard exclusively relevant to road vehicle engineering in the automotive industry. It prescribes a framework for threat and risk assessment, and helps to work towards risk management and engineering requirements. Secure hardware are critical in enforcing controls and measures for reducing risk both to security and safety of the vehicles.
GDPR (General Data Protection Regulation (EU) 2016/679)	Enforced in 2018, this is a European Union regulation on data protection addressing controls on privacy, data sharing, processing and retention. Applicable to enterprise class systems, and extending to physical devices where data is collected, stored, processed and communicated. The relevance here is largely in terms of hardware controls that may help achieve compliance with enforcement and audit requirements.
Common Criteria (Common Criteria for IT Security Evaluation (CC))	With its roots in several US and European standards, this is one of the leading widely known security evaluation frameworks, with a particular focus on operating systems, access control systems, databases, and key management systems certified to varying levels of assurance where each level guarantees certain security attributes. Current secure hardware products are particularly notable for access control and key management.
IoTSF (IoT Security Foundation)	Founded in 2015, IoTSF is a UK-based non-profit aiming to promote best practice for IoT security. It is concerned with championing consumer rights, but equally guidance for industry including supply chain organisations. Notable for its guidance on security assurance, vulnerability disclosure, and design and architectures.
GSMA (Global System for Mobile Communications Association)	Founded in 1995, this is an industry organisation presenting most of the world's mobile network operators and associated organisations in the telecommunication sector. Serving as a trusted platform, it serves threat intelligence sharing and best practice adoption to address fraud and security for mobile handsets, network carriers, and manufacturers.

that *"tend to be cast in terms of known quantities, which are standards based"* (P13).

Having an industry standard for onboarding (certifying) devices, or having agreed best practices from consortia such as IoTSF and GSMA, were seen by one participant as necessary to prevent a plethora of individual solutions that would *"become too difficult to manage and too costly"* (P6).

In spite of the frequency of mention by participants, and the citing of regulations and standards deemed to be influential, the impact in encouraging secure hardware adoption specifically was questioned by one participant: *"I don't think the regulations are at this point in time, specific enough that it would suggest a particular solution one way or the other. certainly a good driver for cybersecurity in general. But, nothing hardware specific at this point."* (P20). Moreover not all participants felt that it was the only driver. Also cited were reducing the risk of reputational damage (P11) (P24) and revenue protection (P5), as well as IP protection, for example in providing end-to-end encryption for a 3D printing company (P6), or preventing software exfiltration by employees and unauthorised users (P20). The presence of multiple driver factors was summed up by one participant, P6:

"Compliance is [...] not the only driver, and I wouldn't say if there wasn't compliance, they wouldn't bother. People do care about their reputation, they do care about their IP. [...] if you're dealing with a medical robot manufacturer, it's critical that they carry out the right operation on the right person [and] that any data associated around the records of that person is only accessed by the right consultant, or nurse or whoever. [...] Revenue protection is important as well. So there's multiple factors." (P6)

Technical benefits were also offered, such as facilitating secure over the air updates (P10), and demonstrating that elements are isolated for safety test reassurance (23).

A few specific use cases were cited as examples of drivers. Emissions legislation was noted to be forcing the OEMs to ensure the secure preservation of in-vehicle data and the non-tampering of systems by third-party companies (P2). Preserving the user experience of automotive infotainment interfaces through the prevention of aftermarket tampering and updates by third parties (P10) was also cited.

The adoption of secure hardware was discussed by some as being a natural progression to security requirements, with managers likely to become more convinced following the rise in attacks such as Jailbreak, which revealed hardware vulnerabilities (P4). In the automotive field, the 2014/2015 attacks demonstrated by Miller and Valasek [46] were cited as being influential in raising industry awareness regarding security, *"everyone realised at that point, oh, there are real attack vectors against real vehicles out there today. And I think since then the industry has really kind of turned around"* (P25), and *" there wasn't only immeasurable loss in the idea of sales and things like that, but it also affected the industry as a whole as you started seeing proliferation of security"* (P8). These comments reflect how progression in hardware involves not only technological advancements, but also a capacity to respond in the 'arms race' against attacks.

5.2 Impact of sector and company characteristics

Drivers and motivators for hardware security investment were felt by some participants to be likely to differ according to company factors such as size, maturity or position in the business chain. For example, Tier One suppliers in the automotive supply chain were seen as being

driven by requirements stipulated by the OEMs Original Equipment Manufacturer (P15), who in turn were driven by regulation. This was summed up by participant P21: *"At the moment the current version of the UNECE regulations state that it's the OEMs that have to comply with that. [...] the OEMs are kind of pushing those requirements down into the supply chain"* (P21).

In the automotive field, one participant noted the importance of functional safety, though felt there was currently less focus on security (P15). In the operational technology sector (i.e. monitoring and control physical processes, devices, and infrastructure), the adoption of secure hardware was seen as a long way off by one participant due to *"The lifetime of those systems [being] an incredibly long time"*, and further, that *"There's a certain element of, if it ain't broke, don't fix it. A lot of businesses have been running 24/7 since sometime in the 70s. And therefore, they're kind of pushed to make any changes."* (P20).

Not requiring secure hardware chips in sufficient volume for the order to be attractive to suppliers was cited by one participant: *"the military market is small, high value, but it just hasn't got the sheer size. Although we [might have an order that we see as] a big order, it was actually a tiny order compared to, for example, some of the handsets that were being produced, sold worldwide"* (P13). Another recalled *"when they only licensed an ARM TEE chip to chip users in the millions. So if you and I had an idea for a good app that we could use it for, it was locked out because the business plan wouldn't let it happen"* (P17).

Some participants felt that the maturity of the business impacted the desire to adopt secure hardware. For example, one participant pitched the adoption of secure hardware to an established multinational consumer goods manufacturer to facilitate secure remote monitoring, and found them *"so concerned about brand reputation [they] immediately bought in to the idea of having a secure hardware product "* whereas the participant found that SMEs *"don't really fully recognise the value of their brand"* (P1). It was also noted that for companies at the research and development phase, security was less likely to be a consideration *"Because at the R&D phase you're interested in proof of concept, and you're interested in building something, demonstrating something"* (P13). It is noteworthy, however, that such perceptions were expressed about other companies, rather than the participants' own, moreover, one participant from an SME stated that cyber security was one of the pillars on which their company's reputation was based; the other two pillars being performance and flexibility (P25).

5.3 Hardware versus software

A number of participants pitched secure hardware adoption in terms of a choice between hardware and software solutions. Hardware was seen as providing enhanced security *"since it sits below the software, it's transparent, so its somewhat isolated from the arms race between the software developers and the hackers"* (P7); providing a means to *"avoid some of the vulnerabilities that you have with software only solutions, the basic problem with anything that is in software is that you can hack into it. And you can change the variables in that software"* (P11); or that *"being able to carry out the cryptographic functionality on hardware does give you the added benefit of being able to implement more robust functionality on the hardware"* (P16). Secure hardware was also seen as offering a *"pre-configured solution that can, obviously, be more straightforward to implement"* (P8) and *"very easy to deploy onto an end user, they don't need to configure anything"* (P16).

However, one participant from a Design and Manufacture SME stated that not being able

to change the hardware *"can be a real problem for the integrating into much larger systems from an operational point of view, disruption point of view. Imagine having to plug a card into every server in a data centre, it's unlikely to happen with existing data centres that are at high capacity. Whereas perhaps a software patch is much easier to do"* (P24).

Another participant, also from a Design and Manufacture SME, still preferred software security solutions for mass market deployments since it offered flexibility in meeting user requirements: *"We tend to find that, for most mass market solutions, we still favour a software-based approach [...].", and "when you look at the majority of the organisations and the day to day data that they handle, the threat just isn't high enough to warrant a hardware solution. [...] the number one point for us is the agility that software offers [...] in terms of changing to user requirements and being able to patch and update the solution very quickly."* (P16)

The challenge of meaningfully comparing software solutions and secure hardware was noted by one of the SME participants in the Design and Manufacture sector: *"I think people find it hard to quantify the advantages of a hardware versus a software based security solution. [...] clients are doing a cost benefit analysis, because a hardware is always going to be more expensive than software solutions, and they are trying to balance that additional cost against some additional benefits. But being able to quantify those benefits, I think is what are the key challenges."* (P11)

5.4 Cost, complexity and lack of expertise - perceived barriers

Cost, complexity and lack of expertise were frequently cited by participants as disadvantages of secure hardware and key barriers to its adoption (e.g., P6, P4, P8). Secure hardware was described by P6 as *"a cost, more effort, more work, but a necessary evil"* (P6). The complexity of getting things to work and connect from different vendors was described as a *"horrible, massive, monumental task. Almost 99.9% of the customers when it comes to security? The first question they ask is how complicated it is to get into"* (P10). Costs were cited as the hardware itself, changes to the design process and switching to the new solution (P11), time to deliver and additional costs to the system through secure hardware adoption (P8).

A few participants offered the perception that secure hardware solutions would be more costly than software solutions, for example: *"It's always going to be more expensive, putting a hardware security solution in place, compared to a software solution"* (P11). Higher salaries of developers with security expertise were also cited as a challenge for the automotive industry OEMs (P21). Return on investment was noted as *"dubious"*, being an *"uncertainty, unquantifiable"* (P17).

The speed at which an application or product with secure hardware in it could be developed and deployed was seen by one participant as being especially problematical for small businesses, since *"they would probably argue that security hardware will be out of date in a year [when] a software solution they could upgrade over the internet, for example"* (P24).

However, costs were not always universally considered as being more for secure hardware. For the automotive sector, one participant noted the costs of testing for safety and demonstrating that systems would not interfere:

"The automotive domain is relatively cost sensitive, especially since we are talking about high value, high volume. So if you add 10 cents to an ECU Electronic Control Unit you think that a modern vehicle has around 100 ECUs. This adds up, but still it's cheaper to go for a

hardware based solution, especially if you have to change anything, then this is also easier." (P23)

5.5 Integration

Integration was raised by some participants as a challenge for adoption. For one participant, the challenge was learning new APIs, which whilst *"not necessarily difficult was another thing you got to learn. It's another API, you got to learn and figure out how we're going to implement"* (P12). Moreover, P12 saw the lack of understanding and visibility of APIs as restricting the optimal use of secure hardware features, as reasons why: *"a lot of ARM chipsets have got trusted enclave, trusted execution process in the chipset that aren't actually particularly well used"*.

For one participant in the design and manufacturing field, an important part of getting secure hardware adopted stemmed from working with the adopting client, to offer *"turnkey solutions"* [as 'ready-to-go' solutions] comprising *"the hardware security product with keys and secret assets and passwords, everything pre-programmed in the factory"* (P1). These solutions were seen as facilitating rapid adoption and scalability, and overcoming the *"typically neglected"* problem at the early stages of development of a secure product; that programming happened in advance in a manufacturer's secure facilities also added further security assurances.

Knowledge about the integration of secure hardware modules or functionality was seen as important. For example, *"just because one module is plausibly secure, doesn't mean I can use it alongside another one in a secure way. That's a research issue [...], that virtually no one I think, in the outside world understands"* (P17).

An example of uncertainty that was noted in the automotive industry concerned roles and responsibilities for integration and API development to use the secure hardware: *"Who will provide this interaction interface between the HSM and software running on the ECU Electronic Control Unit? We had a conflict between the Autosar AUTomotive Open System ARchitecture HSM library and custom built one, so this is already there. And the problem is, all of these are still in the starting phase."* (P23).

5.6 Communicating benefits

Measuring benefits from secure hardware, or indeed enhanced computer security in general, seemed challenging, or reported to be typically not attempted (P23), but was occurring in places. This challenge was articulated by several participants:

"The challenge is to be able to communicate the value proposition, not the technological advantage, to people at board level. We try to quantify it from a cost perspective, engineering time, perspective, complexity perspective." (P10)

Further, P24 noted the difficulties in articulating security benefits:

"Measuring benefits can often be really difficult in my experience. Certainly performance stuff is a bit easier to measure. You can talk about number of CPU cycles that are freed up. In terms of quantifying a security benefit somehow? It depends. Normally, I would say, it's hard to do that, to say that because my protocol is running in a secure box rather than on an open server, somehow this is more secure." (P24)

P4 related these challenges to a lack of methods for establishing costs:

"In my view, there is no methodology, scientific methodology that can quantify the cost of a breach, before the breach happens. Even when the breach happens, even then there isn't a reliable scientific methodology that can quantify this. We don't have historic data of what happened when a breach happened on an IoT device, on a pipe for oil, for example." (P4)

Measuring benefits was also reported by one participant as being *"ad hoc"*, done *"partly through research projects that we're doing where we always try to throw in a work package where we're doing a little bit of analysis of the solution and try to come up with some quantitative measures for how how we improve the security"* (P11). Cited as hindrances to measuring benefits were the lack of historic data about actual breaches (P4), and a lack of support from neutral bodies (including academic community) that could examine a range of solutions.

Where benefits were measured, or were being contemplated, candidates for measurement included data throughput and reliability, reductions in downtime, compliance with regulations such as GDPR (P8), and cost and complexity (P10). One participant (P25) reported trying to measure security using threat modelling and risk assessment, although these had not been run prior to the adoption of the secure hardware, so were not used to gauge benefits. Technical criteria such as cost and performance are mentioned elsewhere (e.g., [1]), where here our participants also related business requirements as expectations for hardware.

5.7 Skills gap

A skills gap was discussed by some of the participants, and cited as a cause not only of lack of adoption of secure hardware, but also of failure to leverage the full potential of secure hardware. For example: *"Today there is a lack of awareness of any of those kinds of systems. And so as a result, I just don't see them as being leveraged probably as much as they should be"* (P22).

This skills gap was seen as applying generally across sectors (P16, P17, P22, P25), for small companies (P12), industrial sectors (P20), national infrastructure (P19), in-vehicle electrical engineering teams (P21). For one of the participants, a challenge was for users to understand the differences between HSMs: *"One of the issues is obviously there are lots of different types of HSMs around and they might all be certified to a particular level. And it's such a complex area, I think the user often finds it difficult to understand, you know, the differences if I'm honest"* (P14). Regarding the awareness associated with hardware security, Ramesh [32] cites awareness and skills, noting in particular that the defence industries have a large priority for hardware protection but comparably low research funding available for hardware security.

Some participants discussed a gap between the client demand for some functionality, such as connectivity, and considering the security implications. For example: *"the simple equation that many of my clients did was something like, 'Okay, I need this hardware to be connected.' The problem is that they typically completely omit the security bit from the equation"* (P1).

One participant reported that many manufacturers of heating, lighting, air conditioning, burglar alarm and fire alarm systems they had spoken to said that security was something they left to the network people (P9). Similarly, with regard to in-vehicle components, it was expressed that security was sometimes seen as pertaining just to network gateways or external facing interface components, even though it could be that another component *"gets exploited to become a vulnerability [...] I think getting people to understand that we have to look at each component to consider its security relevance [such as electrical or network-accessible features], and*

it goes far beyond just the external facing ones, is a really important point" (P3).

It was also noted that developers would try to implement their own security solutions with insufficient knowledge: *"We've seen developers who try to implement really simple things for security, and they may even not know exactly what security is all about." They "literally invent the encryption algorithm, which is completely bad practice from the security point of view"* (P1). Other work has noted that software developers may experience a 'knowledge deficit' regarding secure development [47], and need support to access underlying security-related features [48].

There were suggestions elsewhere that secure hardware knowledge was improving, for instance P6 said they *"now speak to more people that have security architects or security teams, attributed to an IoT project or device, as well as the corporate security team who's handling the support and the operations once things get go into production. So there is definitely a bigger appetite to look at security"*. Even so, that participant qualified that *"I am still shocked, and we do get surprised sometimes by security as an afterthought"* (P6). That security is being considered as an afterthought is an ongoing narrative in the community, beyond secure hardware [49].

P8 saw improvements being driven from outside of technical professions: *Now you've got the sales people and the marketing people driving it too, and you get more investment into it, you're starting to see a transition to safety becoming a more marketable feature* (P8).

The resistance of some developers to change, especially where secure hardware might be perceived as replacing their skills: *"some don't want this because they feel like it's not necessary, because they've already designed such a wonderfully robust system, that it's not necessary"* (P8).

5.8 Who are the decision makers?

One interviewee noted the importance of procurement and standards in adoption decisions, at a general level for high-risk environments:

"Inevitably, somebody has to write an equipment specification of the system specification derived from requirements. So the requirements tend to be cast in terms of known quantities, which are standards based. So I think the thing that will determine whether these things get incorporated is if there are standards for them [...] that can be adequately pointed to." (P13)

No dominant chain of decision making was uncovered. For example, one secure adoption project was instigated by the Chief Technology Officer (CTO) and head of security (P20). The board and senior management were often seen as the key influencers for pushing security (P17), though not necessarily pushing specific implementations, such as secure hardware:

"Generally cybersecurity has been taken up at the board level. So this is what we're hearing in the past couple of years, you know that the board now cares about security in general. And, for instance, they keep hearing ransomware in the news, and they are worried about their data [being] hacked and leaked, and stuff like this. When you talk about a product or when you talk about the hardware, that's a little bit more technical, I would say." (P10)

P10 noted also that once a decision to act on security has been made at a high level, *"then technical people basically got in touch. Clearly was decided at the top"* (P10).

This relates to management of security within organisations in general, where senior security managers report fielding concerns from executive managers, at times when they have read

a news story about a competitor organisation experiencing a security incident such as a data breach [50].

Whilst the board was important, the role of other stakeholders was also acknowledged:

"The pressure comes from the board. Now the product owner, the engineer that is responsible for the product to be developed, usually cares about security. They care because if the product owner doesn't care, and something happens, someone attacks the product when it's on the market, then it's [their] head on the block." (P4)

P14 framed this from a different perspective, stating that what mattered was *"identifying the problem owner. And the problem owner isn't always the one that has the budget [...] but feels the pain"* (P14).

Also, the need to influence other stakeholders, such as procurement staff (P11), who *"don't actually understand the importance of security when they are procuring, all they're interested in is the price"* (P9), and technical staff, where it was also stated: *"The drivers are set out by the board that organisations need to improve the security. But the key people to convince will be the technical people. Because when it comes to security, it's very much a specialist area, you need to convince the people who have that expertise within the company."* (P11)

In this sense, technical experts are at the intersection between hardware features and adoption decisions, as an intermediary between both areas, making the argument on behalf of the offering and relating it to the business. The need to tailor the message of what the hardware is capable of to the needs of different stakeholders is echoed by P1:

"Depending on the stakeholder in a company, you need to tailor the security message in a different way. So when you talk to the CEO of the company, [they do not] care about the security peripheral, but [they understand] the brand, reputation angle. But when it comes to the firmware engineer, you need to provide very solid pieces of collateral to let [them] understand how to implement in a AES encryption routine, or how to use the ECC acceleration engine, or how to secure the key." (P1)

6 Discussion and Recommendations

To return to our overarching research question, through engagement with our participants we uncovered various aspects of the decision-making process around adoption of secure hardware. Across sectors, the most consistent form of motivating factor for adoption was seen as compliance, standards, and regulation; this only differed insofar as whether it was seen as a primary driving force. The role of legal and regulatory frameworks in driving change in security – and potentially being the one, primary driver - has also been seen for security in companies [7]. What also emerged from our interviews was that standards were seen either as dictating conditions to strive for, or acting to state conditions to be seen as meeting as a baseline requirement for operating within a market.

Market forces were also seen as driving adoption of new and secure hardware when it emerges, to serve as a differentiator from competitors; this then brings into question the value proposition for those organisations in a sector which are not intent on being first adopters, and certainly that market position is a factor in how product developers will act to incorporate new hardware. Other drivers can be usefully framed in terms similar to the 'costs of cybercrime' [51], differentiating between direct, indirect, and defence costs. Investment in improved hardware

is a clear defence cost to realise protection of revenue and IP, to also offset the perceived risk of potential reputational damage, and to reduce concern about publicised attacks which have been seen to affect similar organisations. However, our participants were divided as to whether a defence cost to hardware improved or added complications to the process of maintaining defences, such as how it may enable secure updates remotely or over-the-air, but otherwise may complicate improvements to security by requiring direct access to products in order to upgrade the hardware.

Our participants nonetheless articulated that secure hardware can have a range of direct, indirect, and defence *benefits*, and that these may be perceived internally according to the strategy or narrative of the business. These benefits may also be externally visible, seen by peers and customers to convey governance efforts, assurances, and ultimately act as market signals (for instance, that a product is 'secure' without requiring the observer to understand the technical details of how this is achieved).

This is to say also, that where there are indirect benefits of secure hardware, the connection of defence benefits – the technical improvements provided by the hardware – must then be articulated in business terms, to support reasoned and informed decision-making. What must also be considered is that it is not sufficient to regard the business as an indistinct decision-maker; often in discussion of adoption of improved security solutions, there is discussion of the decision to adopt but also a 'missing decision-maker'. Our participants have articulated that different stakeholders within a business or community of practice have differing imperatives, but also differing frames of reference for the benefits of hardware. These can range from direct technical improvements to expectations as to how a security solution will address a business need (or indeed, a particular threat that the business is concerned about). Decisions about hardware are about more than hardware, and general improvements to security may not be sufficient if specific concerns are not also addressed.

Secure hardware was not always seen by our participants as the preferred solution to addressing efforts to improve system security. Some participants saw it as less flexible and more challenging to deploy compared to software solutions in some circumstances. Software solutions were seen as more favourable in some situations, being potentially cheaper and easier to deploy, though hardware was then easier to package as a single, complete solution; ongoing oversight of software was itself seen as a cost, one then requiring dedicated expertise to manage.

Depending on who is addressed with the proposal of newer, secure hardware, the *argument* for adopting the hardware must account for the challenge in the "determinability of costs" [52]. Measuring benefits from hardware adoption was deemed challenging by our participants, who also noted a lack of sufficiently reliable methods for establishing evidence upon which to make the decision for adoption. As a value proposition to adopters, an informed decision must be made, beyond the narrative that secure hardware will generally improve security – the improvements must match with, and be articulated according to, business needs. Indeed, *"the challenge is to be able to communicate the value proposition, not the technological advantage"* (P10). In a similar vein, a 'symmetry of ignorance' has previously been identified for secure development practices [53], where the expertise to avoid pitfalls is distributed between many stakeholders in an environment. Our participants identified many stakeholders in the chain of secure hardware, and we observed a similar 'symmetry', where business leaders would not know technical details, and hardware proposals would not directly relate to business needs.

Developers and technical experts within organisations would be somewhere in the middle, realising improvements to their own goals, and having some expectation of being able to articulate these benefits in terms of higher business needs. This nonetheless demonstrates the interconnectedness of stakeholders in the joint creation of value in IT ecosystems [54].

As well as the discussion of individual stakeholders in secure hardware adoption, there are also challenges at a collective level. The concentration problem in chip production can mean that small-scale efforts to explore adoption of secure hardware cannot even begin; it may be seen as too inefficient by actors in the supply chain to entertain a variety of needs from a similarly diverse range of customers. Similarly, it is laudable that various governments and associations are developing and articulating expectations for device security (such as in the UK [55] and US [56] for consumer IoT). However, it is arguably not sufficient in a global hardware market to have potentially divergent standards. If, as our participants alluded to, actors in the development and procurement of secure hardware will increasingly look to standards and regulations to indicate what is expected to demonstrate secure systems, any divergence in standards at a global level may become a potential exacerbating issue until a unified standard emerges (or clear equivalence is signalled).

Our participants noted a range of costs to hardware adoption; direct costs of adoption arguably include not only the costs to acquire the technology, but also to integrate it into active systems and devices and have it be made useful. The costs for developers to learn how to leverage new hardware were also cited; the need for usable APIs [4], especially to be able to access hardware primitives, have been noted elsewhere [48], representing a convergence of efforts to improve the security of organisations through both hardware and software.

6.1 Limitations

Our study is based on twenty-five interviews with senior company staff across sectors and countries. Though limited in number, participants were selected through their membership of trade organisations concerned with hardware and electronics, thus ensuring familiarity with technical implementations. The exploratory, semi-structured nature of the interviews allowed for a broad examination of the subject matter, which was necessary given the lack of prior studies connecting hardware concerns with the perspectives of those more familiar with the decisions around adoption of hardware.

There is a potential bias in that many participants appeared to discuss action needed by other stakeholders, or by a larger and less distinct collective such as whole sectors. The discussion of interactions noted between different kinds of stakeholder, and where each stakeholder group has a role in the drivers for change, are nonetheless valuable, when brought together in sum through our analysis. Future work will then engage with more organisations concerned with directly adopting secure and/or new hardware, to complement the perspectives we have detailed here of perhaps more independent groups of stakeholders in the ecosystem.

6.2 Recommendations

- **Find opportunities for unified standards and common needs.** Compliance and standards were seen by our participants as a main driver for adoption of secure hardware,

and development of standards ought to persist given that they are not yet mature. The activity of developing standards may also benefit from finding commonalities across emerging hardware standards, where secure hardware may find its way into various contexts (healthcare, IoT, etc.). Stakeholders and product developers in the supply chain may not be flexible enough to align with multiple divergent standards.

- **Support the decision-maker in making adoption decisions.** Regarding the determinability of costs and benefits, it is not sufficient to focus on a small set of costs as the drawbacks and benefits go beyond hardware. This relates also to the need to elicit decision-maker preferences, to align the advantages of adopting new secure hardware with the needs of the adopting party. One approach is to tailor sensemaking scenarios to frame security concerns alongside other business imperatives [57], in this case by engaging technical and/or senior decision-makers.

- **Articulate switching costs and leverage existing skills.** It would aid the adoption of new hardware, to find overlaps between existing and new skills in the development of solutions on top of the hardware, as developers also need to have sufficient support to leverage the features of new hardware. It is necessary to understand the gap between existing knowledge and what is needed to best use emerging hardware. Developers will have switching costs of their own in moving from one, perhaps more familiar hardware platform, to another. Such efforts can leverage lessons from developer-centred security, where targeting support for developers in order to address 'knowledge deficits' is an ongoing challenge [47].

7 Conclusion and Future Work

Hardware security and decisions to adopt secure hardware involve complex, multi-stakeholder ecosystems. Through interviews with twenty five professionals in the area of hardware development and procurement, we have identified a range of perceived costs and drawbacks, as well as aspects where there is uncertainty and a perceived need for targeted support to realise more secure technology platforms and devices.

These go beyond the technology itself to relate to economic and other business decisions, such as skill availability and time to market. Efforts to pitch cybersecurity were often seen by our participants as difficult and delicate, with a common view that awareness of security options and secure hardware in particular, was lacking. The need to pitch appropriately to the target audience (for example board level versus technical) was also noted – the need to support awareness and understanding of needs goes in both directions.

Future work will engage with stakeholders in organisations adopting hardware, building case studies in a vertical manner. This would involve the decision-makers responsible for determining whether to adopt new hardware in systems and products, as well as those involved in engineering and implementation, and their assessments of how to integrate new solutions into existing systems. This would build a picture that relates the value proposition for the business to the efforts to align new hardware with existing technology to realise that value.

References

[1] Mike O Ojo, Stefano Giordano, Gregorio Procissi, and Ilias N Seitanidis. A review of low-end, middle-end, and high-end IoT devices. *IEEE Access*, 6:70528–70554, 2018.

[2] Ramesh Krishnamoorthy, Kalimuthu Krishnan, Bharatiraja Chokkalingam, Sanjeevikumar Padmanaban, Zbigniew Leonowicz, Jens Bo Holm-Nielsen, and Massimo Mitolo. Systematic Approach for State-of-the-Art Architectures and System-on-Chip Selection for Heterogeneous IoT Applications. *IEEE Access*, 9:25594–25622, 2021.

[3] M Tariq Banday. A study of current trends in the design of processors for the internet of things. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*, pages 1–10, 2018.

[4] Mohammad Tahaei and Kami Vaniea. A survey on developer-centred security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 129–138. IEEE, 2019.

[5] Ismail Butun, Alparslan Sari, and Patrik Österberg. Hardware security of fog end-devices for the internet of things. *Sensors (Switzerland)*, 20(20):1–28, 2020.

[6] Jatinder Singh, Jennifer Cobbe, Do Le Quoc, and Zahra Tarkhani. Enclaves in the Clouds. *Communications of the ACM*, 64(5):42–51, may 2021.

[7] Eva Weishäupl, Emrah Yasasin, and Guido Schryen. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers and Security*, 77:807–823, 2018.

[8] Saheli Datta Burton, Leonie Maria Tanczer, Srinidhi Vasudevan, Stephen Hailes, and Madeline Carr. The UK Code of Practice for Consumer IoT Security: 'where we are and what next'. Technical report, The PETRAS National Centre of Excellence for IoT Systems Cybersecurity, 2021.

[9] Omera Khan and Daniel A. Sepúlveda Estay. Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, 5:6–12, 04/2015 2015.

[10] Ioan Tudosa, Francesco Picariello, Eulalia Balestrieri, Luca De Vito, and Francesco Lamonaca. Hardware Security in IoT era: The Role of Measurements and Instrumentation. *2019 IEEE International Workshop on Metrology for Industry 4.0 and IoT, MetroInd 4.0 and IoT 2019 - Proceedings*, (i):285–290, 2019.

[11] M Rostami, F Koushanfar, J Rajendran, and R Karri. Hardware security: Threat models and metrics. In *2013 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 819–823, 2013.

[12] Edlyn V Levine. The Die is Cast: Hardware Security is Not Assured. *Queue*, 18(4):95–109, 2020.

[13] Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, and Andrew Martin. The Cyber Security Body of Knowledge (CyBoK) 1.0. Technical report, The National Cyber Security Centre, 2019.

[14] Ponemon Institute LLC. 2021 Global Encryption Trends Study. Technical report, Ponemon Institute LLC, 2021.

[15] Lianying Zhao and David Lie. Is Hardware More Secure Than Software? *IEEE Security & Privacy*, 18(5), 2020.

[16] A. T. Markettos, R. N.M. Watson, S. W. Moore, P. Sewell, and P. G. Neumann. Inside risks through computer architecture, Darkly. *Communications of the ACM*, 62(6):25–27, 2019.

[17] Simranjeet Sidhu, Bassam J. Mohd, and Thaier Hayajneh. Hardware security in IoT devices with emphasis on hardware trojans. *Journal of Sensor and Actuator Networks*, 8(3), 2019.

[18] Edlyn V Levine and Algirde Pipikaite. Hardware is a cybersecurity risk. Here's what we need to know, 2019.

[19] Organisation for Economic Co-operation and Development (OECD). Fostering economic resilience in a world of open and integrated markets: risks, vulnerabilities and areas for policy action. Technical report, Organisation for Economic Co-operation and Development, 2021.

[20] Adam Hastings and Simha Sethumadhavan. A New Doctrine for Hardware Security. *ASHES 2020 - Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security*, pages 127–136, 2020.

[21] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Mike Hamburg. Meltdown. *CoRR*, abs/1801.01207, 2018.

[22] Robert Potter. CFOs Can Prove the Value of Cybersecurity Investments: Here's How, November 2020. Forbes.

[23] Rok Bojanc and Borka Jerman-Blažič. An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5):413–422, 2008.

[24] Jim Finkle and Stephen Nellis. Intel shares fall as investors worry about costs of chip flaw, 2018. Reuters.

[25] Bikash Poudel and Arslan Munir. Design and Evaluation of a Reconfigurable ECU Architecture for Secure and Dependable Automotive CPS. *IEEE Transactions on Dependable and Secure Computing*, 18(1):235–252, 2021.

[26] Wei Hu, Chip-Hong Chang, Anirban Sengupta, Swarup Bhunia, Ryan Kastner, and Hai Li. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(6):1010–1038, jun 2021.

[27] A Hoeller and R Toegl. Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability. In *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 136–144, 2018.

[28] Katherine Hsu. Trusted Execution Environments (TEEs) in Connected Cars, 2019. All About Circuits.

[29] Joby Jester. Think the hardware in your car is secure? You might be surprised at our findings..., 2020. Irdeto Insights.

[30] Saverio Fazzari and Robert Narumi. New and Old Challenges for Trusted and Assured Microelectronics. Technical report, Booz Allen Hamilton, Arlington, 2019.

[31] Muhammad Yasin, Bodhisatwa Mazumdar, Jeyavijayan Rajendran, and Ozgur Sinanoglu. Hardware Security and Trust: Logic Locking as a Design-for-Trust Solution. In *The IoT Physical Layer*, number November 2018, pages 353–373. Springer International Publishing, Cham, 2019.

[32] T Ramesh. Security and trust - new challenges to computing today in cyberspace. In *2014 7th International Conference on Contemporary Computing, IC3 2014*, pages 1–6. Institute of Electrical and Electronics Engineers Inc., 2014.

[33] S S Rekha and A N Nagamani. Hardware Security-present and Future Trends. In *ACM International Conference Proceeding Series*, pages 24–29. Association for Computing Machinery, 2019.

[34] J Zhang and G Qu. Recent Attacks and Defenses on FPGA-based Systems. *ACM Transactions on Reconfigurable Technology and Systems*, 12(3), 2019.

[35] Hamza Mudassir. How the world ran out of semiconductors, mar 2021. The Conversation.

[36] Jonathan Woodruff, Robert N.M. Watson, David Chisnall, Simon W. Moore, Jonathan Anderson, Brooks Davis, Ben Laurie, Peter G. Neumann, Robert Norton, and Michael Roe. The cheri capability model: Revisiting risc in an age of risk. In *Proceeding of the 41st Annual International Symposium on Computer Architecuture*, ISCA '14, page 457–468. IEEE Press, 2014.

[37] Robert N. M. Watson, Jonathan Woodruff, Alexandre Joannou, Simon W. Moore, Peter Sewell, and Arm Limited. DSbD CHERI and Morello Capability Essential IP (Version 1). Technical Report UCAM-CL-TR-953, University of Cambridge, Computer Laboratory, December 2020.

[38] Hwaiyu Geng and PE CMfgE. *Semiconductor manufacturing handbook*. McGraw-Hill Education, 2018.

[39] Robert Unseld. Bravely marching in the wrong direction, 2021.

[40] Richard Stone and Jeffrey Ball. *Automotive engineering fundamentals*. SAE, 2004.

[41] Christopher Robinson-Mallett. Coordinating security and safety engineering processes in automotive electronics development. In *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, CISR '14, page 45–48, New York, NY, USA, 2014. Association for Computing Machinery.

[42] Kat Krol, Jonathan M Spring, Simon Parkin, and M Angela Sasse. Towards robust experimental design for user studies in security and privacy. In *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2016)*, pages 21–31, 2016.

[43] Anne Adams and Anna L Cox. *Questionnaires, in-depth interviews and focus groups*. Cambridge University Press, 2008.

[44] Jeffrey Voas, Nir Kshetri, and Joanna F. Defranco. Scarcity and Global Insecurity: The Semiconductor Shortage. *IT Professional*, 23(5):78–82, 2021.

[45] Virginia Braun and Victoria Clarke. One size fits all? what counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, pages 1–25, 2020.

[46] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015(S 91), 2015.

[47] Irum Rauf, Marian Petre, Thein Tun, Tamara Lopez, Paul Lunn, Dirk Van der Linden, John Towse, Helen Sharp, Mark Levine, Awais Rashid, et al. The case for adaptive security interventions. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, 31(1):1–52, 2021.

[48] Partha Das Chowdhury, Joseph Hallett, Nikhil Patnaik, Mohammad Tahaei, and Awais Rashid. Developers are neither enemies nor users: They are collaborators. In *IEEE Secure Development Conference 2021*, 2021.

[49] Joobin Choobineh, Gurpreet Dhillon, Michael R Grimaila, and Jackie Rees. Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, 20(1):57, 2007.

[50] Tyler Moore, Scott Dynes, and Frederick R Chang. Identifying how firms manage cybersecurity investment. *The 2016 Workshop on the Economics of Information Security (WEIS 2016)*, 32, 2016.

[51] Ross Anderson, Chris Barton, Rainer Bölme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. Measuring the changing cost of cybercrime. *The 2019 Workshop on the Economics of Information Security (WEIS 2019)*, 2019.

[52] Matthias Brecht and Thomas Nowey. A closer look at information security costs. In *The economics of information security and privacy*, pages 3–24. Springer, 2013.

[53] Olgierd Pieczul, Simon Foley, and Mary Ellen Zurko. Developer-centered security and the symmetry of ignorance. In *Proceedings of the 2017 New Security Paradigms Workshop*, pages 46–56, 2017.

[54] Johannes M Bauer and Michel JG Van Eeten. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10-11):706–719, 2009.

[55] UK Department for Digital, Culture, Media & Sport (DCMS). Code of practice for consumer IoT security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security, 2018.

[56] Michael Fagan, Mary Yang, Allen Tan, Lora Randolph, and Karen Scarfone. Security review of consumer home Internet of Things (IoT) products. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf, 2019.

[57] Simon Parkin, Kristen Kuhn, and Siraj Ahmed Shaikh. Scenario-driven assessment of cyber risk perception at the security executive level. *The Workshop on Usable Security and Privacy (USEC) '21*, 2021.