"We can't change it overnight": Understanding Industry Perspectives on IoT Product Security Compliance and Certification

Prianka Mandal and Adwait Nadkarni
William & Mary
pmandal, apnadkarni@wm.edu

Abstract—**Regulators and standards bodies have recently proposed several security compliance initiatives for IoT products. These emerging standards and regulations seek to bring security assurance to IoT products by way of compliance certification. However, even certified IoT products exhibit common vulnerabilities, which suggests the presence of latent challenges in the certification ecosystem. This paper performs the first qualitative, interview-based study (n=17) with IoT practitioners to understand industry perspectives and experiences of IoT product security certification, in order to uncover the latent factors and challenges obstructing effective IoT product certification. Our reflexive thematic analysis of the interview transcripts leads to 16 key findings that uncover critical factors affecting compliance enforcement in practice. We distill these findings and our observations into 4 major themes which represent critical gaps that must be addressed for product certification to be viable for IoT.**

1. Introduction

Internet of Things (IoT) product security certification is gaining more traction after regulatory initiatives such as the US Cyber Trust Mark [1], which allow vendors to voluntarily obtain certifications for their products. The motivation for such initiatives is clear: regulators aim to motivate product vendors to incorporate basic security considerations into the development process itself, so as to bring about holistic security improvements to IoT products. Similarly, industry alliances and standards bodies have also created several popular IoT standards and criteria, e.g., the IOXT standard, managed by the IOXT alliance [2]. The standards bodies delegate the security assessment task to independent third-party certification/compliance labs, which evaluate IoT products and assign compliance certificates.

Recent work by Mandal et al. [3] shows that this traditional approach to product security compliance may not work for IoT as expected, i.e., as *even certified IoT products have common vulnerabilities* that are within the scope of the standard, and should have been detected during the certification process. This instance of compliance failure indicates the presence of latent challenges in the process of product security certification; challenges that may not be evident unless we address a key knowledge gap in our understanding of this domain: of *how IoT practitioners from industry, who are the primary stakeholders in the security certification of their products, perceive, practice, and experience compliance certification.*

Contributions: This paper presents the first qualitative, interview-based, study of the perspectives and experiences of IoT practitioners about compliance certification, particularly in the context of IoT products. We define IoT practitioners as IoT developers, engineers, project managers, contractors, security architects/engineers, and any similar stakeholder involved in the development of an IoT product, and hence, a key participant in security compliance certification as well. We conduct in-depth interviews with 17 IoT practitioners from diverse contexts, including the organization size, IoT product domain, and geographic region, guided by the following key research questions (RQs):

RQ$_1$: *How do IoT practitioners view product security?* In order to investigate perspectives on compliance certification, we first seek to understand the role that security plays during product development, and the constraints that practitioners have to deal with.

RQ$_2$: *What are the current practices in product security compliance certification for IoT devices?* We seek to understand what practitioners know about IoT-specific product security standards, as well as how they certify their IoT products in practice. For example, do practitioners use IoT-specific standards (e.g., GSMA IoT security standard [4], NIST security guidelines for IoT [5]), or do they certify IoT products using general security standards (e.g., Common Criteria [6], ISO 27017 [7])? In either case, why?

RQ$_3$: *How do IoT practitioners perceive IoT security certification?* We seek to understand how practitioners view product certification, and the guarantees they expect. What motivates them to seek certification? Do they equate certification with security? Is there a bias toward certification using third-party labs, vs self-certification?

RQ$_4$: *What challenges do practitioners face when pursuing IoT Certification? What disincentivizes them?* Our goal is to understand what practical constraints that affect the adoption and conduct of product certification. Particularly, we seek to understand problems from the business (and not technical) perspective that would hinder effective product certification.

RQ$_5$: *How do practitioners perceive liability in case of failures?* Prior work has shown that consumers will mainly hold developers liable for certification failures [3]; but what do practitioners think? Who would they hold most liable, and what practical factors affect the attribution of blame?

Our interviews (n=17) and qualitative analysis result in *16 findings* that enable us to understand IoT product compliance certification from the practitioners' perspective. Particularly, while practitioners overwhelmingly support certification for IoT products and certify IoT products using existing non-IoT-specific security standards, in practice, there is a significant reluctance in adopting IoT-specific security certification, often on account of valid reasons that tie closely with the organizational context. On the other hand, we find certain other factors that incentivize certification, but only if the process of certifying the product is robust and without error. We further distill these findings into 4 major themes that capture the challenges obstructing the widespread adoption and meaningful implementation of product security compliance certification for IoT, recommending solutions and changes where feasible.

2. Background

Domain-specific security and privacy regulations such as the the Health Insurance Portability and Accountability Act (HIPAA) [8], the Payment Card Industry Data Security Standard (PCI DSS) [9], and the California Privacy Rights Act of 2020 (CPRA) [10] enforce best practices that enable organizations to enhance the security of their products and protect user data. The fear of billions of potentially vulnerable and unregulated IoT products has prompted federal and state governments to respond with similar policy initiatives for IoT, such as the US Cyber Shield Act of 2021 [11], the California S.B. 327 on the security of connected devices [12], and the UK's new product security and telecommunications infrastructure regime [13]. These policy initiatives for secure IoT products have led to (i) an industry demand for IoT product security certification, and (ii) a surge of new IoT-specific security standards and certification programs from the public and private sectors.

The emerging IoT-specific security standards and guidelines are of diverse origins. For instance, the US Cyber Trust Mark [1] and the NIST's Core IoT Cybersecurity Capabilities Baseline (NISTIR 8259A) [5] are offered by the government, the IOXT [2] standard and the IOTAA security guidelines [14] originate with industry consortiums of IoT product vendors, whereas the GSMA IoT standard [15] is offered by an industry standards body. What these emerging IoT-specific security standards have in common, however, is that their enforcement follows the *traditional* product security certification model.

To elaborate, regulators or standards bodies license third-party evaluation facilities or *labs* to carry out the certification. Product vendors/manufacturers then hire these labs to certify individual products. During the certification process, product developers work closely with the labs to address vulnerabilities that may emerge during the certification process. For standards that also allow self-certification (e.g., the Cyber Trust Mark), audits may be carried out by third-party labs instead. That is, standards bodies such as IOXT and IOTAA develop the standard, but delegate the actual enforcement of the standard to third-party labs (e.g., Dekra [16] and Red Alert Labs [17]).

This approach disincentivizes rigorous security evaluation, as vendors may indulge in *forum shopping* [18] to select labs that offer the fastest path to certification, and because labs have no incentive to improve given that the regulators are outside of the loop of compliance certification. Particularly, our prior work [3] has found certified IoT products to have known vulnerabilities that fall within the scope of the regulation, and hence, should have been caught by the labs. This indicates the existence of unknown challenges in practice that prevent effective security certification of IoT products. As IoT developers and practitioners play a key role in the certification process, this study is motivated by the need to understand how IoT practitioners certify products at present, with or without the use of IoT-specific standards, as well as their perceptions and experiences of the same.

3. Methodology

Our study was composed of an initial survey aimed at getting a broad understanding of the problem landscape, followed by an in-depth semi-structured interview that forms the basis of our qualitative analysis. The survey helped us gain a preliminary understanding of how practitioners perceive security compliance certification for IoT products, which we then leveraged to design the interview guide. While we provide a brief overview of the survey protocol and results in Section 3.1, the rest of the paper focuses on our interview study with 17 IoT practitioners from industry.

3.1. Survey Protocols and Results

This section provides a brief overview of the survey protocol and results, which are further detailed in our online appendix [19].

Survey Protocol: Our survey consists of questions regarding participants' familiarity and experience with security compliance standards and certification for IoT products, and their opinions on specific scenarios relevant to IoT product compliance. The survey consisted of a mix of likert-based, multiple choice, questions and open-ended questions (see the online appendix [19] for the survey instrument). Our survey protocol was approved by our Institutional Review Boards (IRB). Participants were informed about the goal of the study before participating in the survey. For recruiting participants, we posted fliers on various developer forums (e.g., SmartThings community [20], Google Nest community [21], OpenHab community [22], and the Home Assistant community [23]), LinkedIn and Twitter. Further, we recruited four participants from a freelancing platform, Upwork. We received a total of 685 responses, of which we discarded 609 responses due to (i) incomplete responses, (ii) ambiguous responses, (iii) duplicate responses and (iv) multiple failed attention check questions. Finally, we obtained 76 valid responses.

Overview of Survey Results: The majority of participants (70/76 or 92.11%) agree that IoT security standards are important for the security of the product because *products with compliant safety standards are generally more trusted by consumers*. Most participants (67/76 or 88.15%) believe that compliance certification positively impacts IoT product security. The rest participants think that the certification has no impact, i.e., the product would be just as secure (or vulnerable) without it. While a majority (58/76 or 76.32%) participants agree that a vulnerability in a certified product indicates a failure of the security compliance process, only 10/76 (13.15%) participants believe that *a vulnerability in a certified product doesn't necessarily mean the whole security compliance process is a failure.* We leveraged these initial results to prioritize questions in our interview guide.

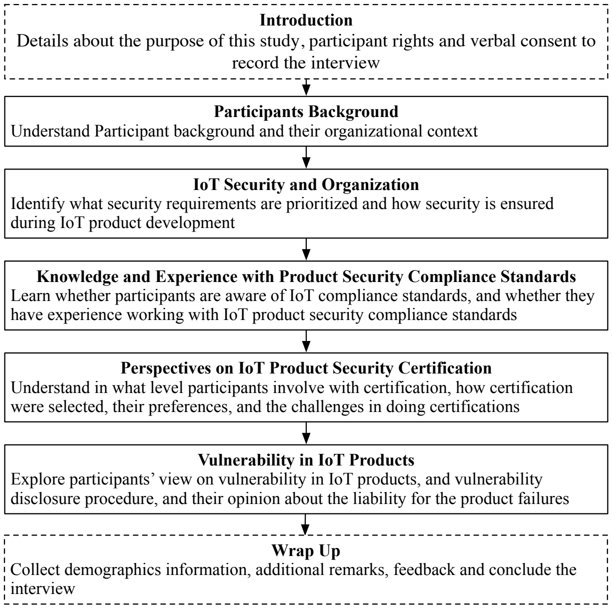
3.2. Interview Protocol

We followed a semi-structured interview approach [24] for our study. All interviews were conducted remotely between March 2024 and April 2024. This section describes our interview protocol, i.e., the recruitment process, ethical considerations and the interview process.

1. Interview Pilot: We conducted four pilot interviews with participants from our professional network: one expert in security research and three graduate students. Based on the feedback from the pilot interviews, we rephrased some questions that were not clear to participants and added details to make them easily understandable.

2. Participant Recruitment: We used multiple channels to recruit the IoT practitioners, that is, developers, program managers, engineers, consultants, and others involved in the development or security of IoT products. First, we invited participants from our preliminary survey who are willing to do the follow-up interviews, which yielded 4 participants. We also recruited 8 participants from our professional networks and using a snowball sampling approach [25]. Finally, we posted the recruitment job on Upwork [26], and recruited 5 participants whose profile matched with our study criteria. In total, we recruited 17 participants for our interview study. Our participants are from various geographic regions (e.g., Asia, North America, Australia, Europe), hold at least a bachelor's degree, have an average of 10 years of industry experience. We provide further details on our participants' organizational and security contexts in Section 4.1.

3. Ethical Considerations: Our interview study was approved by our Institutional Review Board (IRB). We informed the participants about the purpose of the interview and that the interview will be recorded and transcribed. Therefore, we emphasized that participants have the full right to terminate the interview at any point or decline to answer any questions they find uncomfortable. Participants were also informed that the information we collected through the interview will be anonymized and only the results obtained from analyzing the transcribed interviews will be disclosed. If participants willingly mentioned any private information such as product name, company name, and such identifiable information, we de-identified them, e.g., if participant mentioned any product name, we use <*product-name*> instead of the actual product name in the discussion. We made it clear to participants that the interview will take approximately an hour of their time. We compensated participants with $50 for their time.


Introduction
Details about the purpose of this study, participant rights and verbal consent to record the interview

Participants Background
Understand Participant background and their organizational context

IoT Security and Organization
Identify what security requirements are prioritized and how security is ensured during IoT product development

Knowledge and Experience with Product Security Compliance Standards
Learn whether participants are aware of IoT compliance standards, and whether they have experience working with IoT product security compliance standards

Perspectives on IoT Product Security Certification
Understand in what level participants involve with certification, how certification were selected, their preferences, and the challenges in doing certifications

Vulnerability in IoT Products
Explore participants' view on vulnerability in IoT products, and vulnerability disclosure procedure, and their opinion about the liability for the product failures

Wrap Up
Collect demographics information, additional remarks, feedback and conclude the interview

Figure 1: Overview of the interview guide.

4. Interview Process: We used a lead-interviewer approach in all the interviews to make participants comfortable. All of our interviews were conducted in English, and on Zoom. Participants were provided with the Zoom meeting link and informed consent form at least 24 hours prior to their scheduled interview. At the beginning of the interview, we briefly informed the participants about their rights during the interview, i.e., the interviewee can decline to answer any question or stop the interview at any point; however, they cannot use any external tools to answer the question, and they can retract a statement even after the interview. We also informed them that the interview would be recorded and that the recording would be destroyed after analysis. Finally, we asked for their consent once again to record the interview. On average, the duration of interview was 48 minutes.

3.3. Interview Guide

Based on our observations from the survey, we designed a semi-structured interview guide for our study, provided in Table 2 in the Appendix. Figure 1 illustrates the interview guide, organized along five sections:

Participant Background: To make the participants comfortable, we started the interview with warm-up questions about their background and organizations. Particularly, we asked participants about their roles and their work experience in the context of IoT product development. We leveraged the context acquired from this section when asking follow-up questions in the later parts of the interview.

IoT Security and Organizational Context: We asked about the development process they follow for IoT products. Further, we asked participants how they or their organization ensure security in the IoT products and how they test for security. Participants were also asked about their preference between using third-party libraries and in-house development for security-sensitive functions. We also explored what factors affect the security of IoT products.

Knowledge and Experience with Product Security Compliance Standards: The goal of this section is to understand participants' familiarity with product security compliance. Particularly, we asked participants if they had experience with product security compliance standards relevant to IoT, and if they had participated in the certification process, and in what capacity.

Perspectives on IoT Product Security Certification: We asked participants about their preference between third-party certification and self-certification. We also asked participants to provide their opinion about how certification may influence the security of the product as well as product release deadlines. We further enquired about the challenges relevant to product security certification. Finally, we asked participants to describe their responsibilities, as well as of others in their organizations, in the process of certification.

Vulnerabilities in IoT Products: We asked participants about their vulnerability or bug reporting systems, how they address the reports, and if they could provide any examples. We asked participants which stakeholder(s) they would consider to be liable if a vulnerability were to be found in a certified product.

After the main interview, we asked participants if they had additional remarks or feedback. We also asked participants whether they were willing to provide their demographic information. Finally, we informed them about the payment process, and concluded the interview.

3.4. Transcribing, Coding and Analysis

We used Whisper [27] to transcribe the interview recordings. We manually reviewed the transcripts for errors and anonymized any private or identifiable information.

We used reflexive thematic analysis with the inductive coding approach to analyze the transcripts [28]. We followed a single-coder approach for coding and analyzing the transcripts as this approach is considered a good practice for reflexive thematic analysis [28]. One of the authors got familiarized with all the transcripts, coded the transcripted data inductively to build the codebook, and identified patterns. The coder iterated through these steps to finalize the themes. During the process of coding and theme development, the coder discussed the codes and the identified themes with the team, and refined them based on the discussions. The coder did not only discuss to reach an agreement; it was considered an opportunity to clarify the observations and insights and explore alternative ways of interpreting the data, coding, and patterning that were not considered before, as is the best practice [28]. The codes and identified themes were refined based on the discussions.

Researcher subjectivity is considered an asset in reflexive thematic analysis [28]. However, it is also important to note that the coder's experience and beliefs/focus tend to influence the code book. We provide the code book in Table 3 in the Appendix, and describe the coder's positionality below:

Coder's positionality: The coder is a senior Ph.D. student with 5 years of experience in IoT security & privacy research, with an emphasis on qualitative and quantitative studies, as well as vulnerability analysis, and a dissertation focus on compliance certification in IoT. The coder also has one year of industry experience in software development, and is involved in industry collaborations centered around security and privacy. Particularly, the coder has been exposed to the technology pain points in industry and is equipped to understand the perspectives of practitioners. The coder's focus is on understanding the *security implications* of the perceptions, beliefs, and experiences of industry practitioners. They believe that security is critical for protecting consumers, and more important than plain compliance. As a result, the codebook and analysis may lean toward codes that help in the exploration of the security implications of the practitioners' perceptions and experiences, rather than codes that are purely about describing compliance for compliance's sake. This focus aligns well with the goal of the paper as well, i.e., this is a security-focused paper, which seeks to enable gains in security by uncovering participants' pain points when conducting security certification.

3.5. Limitations

As with any user study research, the responses from our participants may be influenced by biases due to self-reporting factors (e.g., over-reporting and under-reporting) and social desirability bias. To address this, we ask participants to provide examples based on their experience.

Further, as this paper reports our findings from a qualitative study, we acknowledge that the findings may not generalize across a large body of participants. However, considering the participants' diverse backgrounds in terms of their demographic regions, organization size, product domain, and organizational roles, studies like ours can be considered reliable [29].

Finally, while participants expressed opinions on liability, they may not have concrete knowledge about the relevant legal frameworks to articulate who is liable. Thus, conclusions drawn from such responses are entirely based on the participants' perspectives. Furthermore, while IoT-specific regulations are emerging, to our knowledge, there is no legal framework that articulates liability in the event of certification failures or attacks, and at present, most jurisdictions act on such issues on a case-by-case basis. Therefore, this paper discusses the liability based on the practitioners' perspectives, and does not take legal positions on liability in IoT compliance certification.

TABLE 1: Overview of the interviewed participants: their position(s), product domain(s), region, organization size and interview duration. We have abstracted certain details for preserving anonymity.

ID	Position(s)[1]	IoT Product Domain(s)[2]	Region[3]	Organization Size[4]	Duration
P01	Director	Smart Transportation	South Asia	Small	1 hr 20 min
P02	IT Department Head	Industrial IoT	North America	Large	38 min
P03	Chief Technology Officer	Industrial IoT	Southeast Asia	Small	44 min
P04[IC]	Developer	Agriculture Automation, Security system	North America	Large	51 min
P05	Chief Executive Officer	Automated Retail	South Asia	Small	43 min
P06	Developer, IoT Consultant	Security System	North America	Medium	37 min
P07	Security Analyst	Smart Home	West Asia	Medium	34 min
P08	Project Manager, Mechanical Engineer	Military IoT	South Asia	Small	41 min
P09[IC]	Senior IoT Engineer	Smart Transportation, Smart Home	South Asia	Medium	50 min
P10	Senior Software Engineer	Major Smart Home Platform	South Asia	Large	40 min
P11[SC]	Project Manager, IoT Software Developer	Smart Transportation, Healthcare	Europe	Small	46 min
P12[SC]	IoT Consultant, AWS IoT Architect	Industrial IoT	Europe	Very Small	59 min
P13[SC]	Senior Developer	Agriculture Automation, Healthcare	South Asia	Small	50 min
P14[SC]	IoT Consultant, Developer	Healthcare, Asset Tracking	South Asia	Very Small	54 min
P15	IoT Security Researcher	Smart Home	South Asia	Small	56 min
P16	Managing Director	Security System, Smart City	Australia	Small	54 min
P17[IC]	Principle Security Architect	Industrial IoT	North America	Large	41 min

[1] Positions are self-reported by the participants, [2] Product domains are selected based on the products participants have experience working on, [3] We only report the region where participants' office is located, [4] Organization size ranges from very small (1-9), small(10-99), medium(100-999) and large (1000+), [IC] **Independent Contractor** – Participants with this annotation also work as independent contractors for other IoT vendors. [SC] **Sub-contractor** – The organizations of participants with this annotation sub-contract development work from other IoT vendors.

4. Interview Results

This section describes the results from our analysis of 17 semi-structured interviews. We first discuss our participants' organizational context, and then we discuss how security is incorporated into the IoT product development life cycle. After that, we delve into the current IoT security compliance and certification practices, overall perspectives on certification, and the challenges in the certification process. Finally, we discuss the practitioners' opinions on responsibility and liability in compliance certification.

4.1. Participants and Organizations

Our 17 participants come from diverse organizational contexts, geographic regions, and roles, as shown in Table 1. To elaborate, we recruited participants from small to large companies, working in an array of roles/positions, and across several demographic regions. Furthermore, some of our participants also work as *independent contractors*. In fact, some of our participants work in organizations that *sub-contract* IoT development work for other IoT vendors, in addition to developing their own products, and as such, can also be considered as independent contractors from the IoT product vendor's perspective, as annotated in Table 1. Interviewing participants across these diverse contexts helped us understand how IoT security compliance standards are enforced in various unique circumstances.

4.2. The Role of Security in Product Development

This section characterizes how security factors into the development of IoT products, with the goal of contextualizing the later discussion on security certification.

4.2.1. The impact of the *the triangle of the project* on IoT product security. IoT product development is severely constrained by the triangle of *budget/costs*, *time*, and *scope*, i.e., as **P11** states, *"As a usual project management process, it depends on so-called 'triangle of the project'. Including budget, times and scope of work...kind of a balance between these three parameters."* These three factors determine the emphasis on security of the IoT product during development.

Participants often complained about having to adjust their product's security requirements due to limited budgets. **P8** shared an experience that exemplifies this issue: their team lacked security experts at the time of product development, and failed to adhere to any security standards or best practices, (potentially) exposing their project to security issues. After the development, their organization contracted a security consultant through their professional network, and the consultant then "handled" the security of their product post-development. From our analysis of the transcripts, we observed that this was a common trend, i.e., of budget constraints causing the lack of security expertise in the team, resulting in the IoT products rarely being *secure by design*. This trend may generalize beyond IoT products, i.e., prior work [30] has also found the lack of an adequate budget to be one of the main causes for deferring software security.

Finding 1 ($\mathcal{F}_1$) **–** Budget constraints mean the lack of security experts in development teams. This causes security issues to persist in developed IoT products, which are only addressed post-development using third-party security consultants.

When it comes to deadlines, we observe that most participants are inclined to deliver secure products, and hence, prioritize security over deadlines, e.g., by adapting internal deadlines to address security problems discovered during development. A comment from **P2** reflects this general sentiment, which is also seen in recent work [31]:

> *“...always ensuring the security of the product...we don’t cut out those problem because the deadlines are set by us to be able to meet the consumers requirements" — P2*

That said, independent/sub-contractors did not experience as much control over deadlines as first-party developers (whose organizations develop the product). Such participants recalled giving in to arbitrary deadline pressure from clients, and delivering code without addressing security concerns:

> *“Sometimes our deadline has been moved forward and it messes up with the security guarantees whereby, because I really want to give my client the best, but due to the fact that they need the product really early, I tend to finish up immediately .... sometimes it would lead me to taking shortcuts. And sometimes the whole security guarantee might be overlooked" — P4*

The primary cause of this pressure from clients is because, as **P14** states, *“most of the clients are in a hurry to get into the market."*. Some practitioners such as **P14** recall pushing back against this pressure from clients to meet deadlines if product security hangs in the balance, and instead, convincing customers of security being a valid *“reason why the task is getting delayed"*. However, this sentiment was rare among independent contractors.

Finding 2 ($\mathcal{F}_2$) **–** Most participants prioritize security over deadlines, delivering secure products by delaying internal deadlines and convincing customers. However, this trend is not seen in independent contractors, who have far less agency when it comes to adjusting deadlines, and often sacrifice security to deadline pressure from clients.

Recent work by Ami *et al.* [31] has found a similar sentiment among software developers, i.e., where software developers *prioritize security*, over deadlines. However, our results also highlight cases where practitioners sacrifice security due to non-technical requirements, e.g., when independent contractors are bound by contractual deadlines, echoing observations from past studies with software developers [32], [33].

Finally, most practitioners expressed that they try to maintain a certain minimal security baseline, often influenced by existing standards (e.g., the GSMA IoT security standard [4]). However, we observe that in locales where such standards are non-existent, and the “scope” of such minimal baseline security guarantees is unclear, practitioners may forego even basic security measures:

> *“Right now, we don’t have any encryption for this. No, but those can be used directly from the server because, in our country, we are not that much aware of our data breach, our information security...So you can say we are taking the benefits right now for this." — P1*

This clearly shows willful negligence due to the lack of enforced IoT-specific security compliance standards.

Finding 3 ($\mathcal{F}_3$) **–** Although most practitioners follow baseline security best practices, it is possible that in the absence of any enforced product security standards, practitioners forego security entirely.

4.2.2. Using third-party libraries for security-sensitive functionalities. While some participants believe that developing security-sensitive functionalities in-house is better, most participants stated that reinventing the wheel is not an efficient way to work, and *“you can’t have everything in-house"*. Furthermore, participants state that using third-party libraries can help save on budget and time during product development process while also ensuring security (assuming the library is well-tested):

> *“... from the other side, they will save a lot of budget and a lot of time. And I can say that in 99% of our projects, there were no big issues with security. At least we don’t know these issues. So the optimal way is to use somebody’s work instead of inventing the wheel each time you’re doing another project" — P11*

Participants pointed out two key factors that developers must consider while using third-party libraries for security-sensitive functionalities: (i) third-party libraries (can) have vulnerabilities (also reported in [34]), and that the developer must use (ii) the latest versions (in a bid to avoid known vulnerabilities). Moreover, participants expressed that the key concern when using third-party libraries is that of assuming responsibility for the security vulnerabilities that exist in third-party code, i.e., none of the participants in our study believed themselves to be responsible. As **P11** asserts,

> *“as soon as we are using third-party libraries, for example, or software development kits, we cannot be responsible for security of this part of the projects or implementation" — P11*

However, participants also expressed that the developers of the libraries are not held responsible in practice either, as *“[vulnerabilities in a] lot of dependencies from third party developers that never come to responsibility at all. (P11)”*

Finding 4 ($\mathcal{F}_4$) **–** Participants view the use of third party libraries and SDKs in developing IoT products as unavoidable, are aware that the libraries may have vulnerabilities, and recommend using the latest versions to avoid vulnerabilities. However, if a vulnerability is found in a library they use, participants are also firmly against assuming any responsibility for it.

This finding may reflect a more general tendency among developers even beyond the IoT domain, as prior work by Derr *et al.* as found that app developers use third party libraries with known security vulnerabilities, and demonstrate a tendency to implement fixes by updating libraries [34].

If product developers decline all responsibility, and if library-developers never assume any responsibility either (as seen from the experiences of our practitioners), the question is, *who is responsible for addressing security issues found in the third-party libraries used in IoT products?*.

4.2.3. Maintenance – vulnerability reporting and fixing the issues. Independent/sub-contractors and practitioners employed at an organization building an IoT product have different responsibilities when it comes to product maintenance after release, which affects how they address vulnerabilities in IoT products. For further clarification, participants were asked about examples of reported vulnerabilities in their product/organizational contexts. Note that the discussion is in the context of security vulnerabilities; however, most of our participants used the term "bugs" to describe vulnerabilities. Most participants who are employed in the organization building the product mentioned that they usually maintain vulnerability/bug reporting systems, and try to fix vulnerabilities that they deem as valid:

> *"...solved almost, I guess, eight to nine bugs [vulnerabilities] in the past one and a half years" — P1*

P7, whose organization does not use a bug reporting system, described the use of bounty hunters instead:

> *"We hire bug bounties whereby we introduce maybe an incentive for everyone who is willing to...check our systems for any bugs" — P7*

However, when participants work as independent contractors, their service level agreement (SLA) dictates whether and to what extent they would be be involved in vulnerability fixing. While most describe using systems such as JIRA, or using emails and log collecting mechanisms to track vulnerabilities reported by clients, this support is time-limited. That is, contractors provide such maintenance services only for a short duration pre-defined in the SLA, and as a result, are responsible for only the immediate testing of the code covered under the contract, rather than for vulnerabilities discovered through the life of the product. For example, as **P14** states, *"we keep like 10% of time as a free support. So for example, it's a one-year project. So one month free support."*

However, despite this leeway, some, like **P11**, recall providing maintenance services for vulnerability testing/fixing beyond the time required by the SLA:

> *"It really depends on the agreement and contract we signed...sometimes we like keeping our support team working in some three or six months after we finish the project" — P11*

In contrast, some others do not provide any support for addressing vulnerabilities beyond the SLA, and completely delegate the responsibility to the client:

> *"if some bugs are discovered, the customer [IoT vendors] should be equipped with tools and knowledge to solve those bugs themselves." — P12*

Finding 5 ($\mathcal{F}_5$) – Independent contractors are not required to address vulnerabilities in the code they were contracted for beyond the length of the contract, and hold the IoT vendor responsible for addressing any vulnerabilities found beyond the contract period.

Finally, after an in-depth analysis of the responses from independent contractors, we could not reach to a conclusion regarding what happens in practice when a vulnerability is found in an IoT component (developed by a contractor) that is not under any maintenance agreement.

4.3. Practices in IoT Compliance Certification

We now describe what practitioners know about IoT security compliance standards and certification, and how they certify IoT products at present.

4.3.1. Knowledge of IoT Product Compliance. While all of our practitioners were familiar with general software and product security standards, we observed that only a few were aware of IoT-specific product security standards and guidelines, such as IOXT [2], the GSMA IoT security standard [4], the NIST security guidelines for IoT [5], and the IoT Security Foundation (IoTSF) standard [35]. However, awareness of these standards does not imply practical experience. For instance, **P13** shared that they learned about IoT compliance standards via an information session in their organization a few years prior, but they *"haven't started applying any of them"*. In some cases, organizational division of responsibilities shielded developers from having to know about applying certain security standards to the very products they developed, e.g., as **P10** states,

> *"...they give us the requirements, the features, we develop it, we test it on our own, unit testing and others that we could possibly do, and then we give the release to the counterpart that is in <country-name2>, they test it, and if they found any issues, they give us back. So I think the total security part like user security or compliance, all are handled outside of <country-name1>." — P10*

The need to maintain confidentiality regarding the development of highly sensitive IoT products may contribute to this lack of experience as well. **P8** explained how their organization segments such products into minute components, and then assigns those components to individual developers without giving them any intuition regarding the other components, eventually combining them in an opaque manner, akin to a "zero-knowledge proof":

> *"...zero knowledge proof, like we have segmented our whole project into some modules smaller modules like our one intern or fresher are working only on one module so he is not aware of the other modules" — P8*

Other participants also expressed similar sentiments, that when working on large projects, developers do not have much freedom to even know about the whole, let alone influence the enforcement of a compliance standard. As **P10** states, developers are bound to follow organizational guidelines *"even if the guidelines are not perfect"*.

Finding 6 ($\mathcal{F}_6$) – There may be a significant knowledge gap among developers when it comes to the practical application of IoT-specific product security standards, owing to slow adoption by organizations and the opaque segmentation of product development tasks.

4.3.2. Current Practices in IoT Product Security Certification. That participants have little practical experience with IoT security compliance standards does not imply that the IoT products do not undergo security certification at all. In fact, most participants stated that their IoT products do undergo security certification, but the certification is of the *general* kind, i.e., security standards and certifications that apply to any software or hardware product, and not specific to IoT (e.g., ISO 27017 [7], UL certification [36], and CE mark [37]).

Most participants stated that they opt to certify their products when they want to export them to a country that requires a specific certification. However, the lack of a regulatory requirement may also disincentivize the need to seek security certification, e.g., **P1** states that *"...in <country-name>, there is no currently, there is no such certification right now."* Similarly, **P9** also states that they only *"have maintained some ISO certificate which is mandatory for the manufacturing"*. Further, participants from organizations in their early stages of growth (e.g., **P9**) generally avoided product security certifications, even if it meant limiting their markets, given the additional time and budget the certification process entails.

Participants who work as independent contractors consider certification as outside their scope of work, and as their client's responsibility. This stand is particularly motivated by the tendency to distance themselves from any liability from security issues in the product, as **P12** aptly states,

> *"they [client] followed the certification by themselves because they already were established the manufacturer in the market. They know all the required certifications. Basically, they know what they are doing from the legal perspective." — P12*

Finally, one of our participants was not only familiar with IoT-specific security certifications, but had also applied a popular standard, IOXT [2], to their own products:

> *"...we usually contact that the ioXt to look into most of the things we do in our company to make sure that everything is done accordingly..." — P6*

Finding 7 ($\mathcal{F}_7$) – IoT products generally undergo security certification using existing (non-IoT-specific) product security standards. However, several factors disincentivize certification, such as the lack of regulatory requirements, organization size, and in the case of contractors, the lack of ownership in (and hence liability from) the product.

4.4. Perceptions of IoT Product Certification

After learning about current practices of compliance enforcement and certification, we aimed to understand participants' perspectives on the IoT security certification.

4.4.1. Certification implies *Trust*. Regardless of their current adoption of IoT-specific product security standards, all participants believe that IoT security certification is essential for security assurance.

> *"I think it is good in terms of, you know, making your product certified so that it gives assurance to your end client or end customer, right? That our product is certified. So it gives a kind of a trust base to your product " — P14*

Particularly, most participants were keen on certifying security/privacy-critical IoT products, i.e., as **P15** states,

> *"I'm more concerned about the medical devices here. If the security vulnerabilities are coming on the medical device and the medical device are connected to the internet. The patient data is very sensitive and i'm very much concerned about that. So definitely those devices to be certified..." — P15*

There is also a perception among practitioners that if the IoT product is certified, customers would be more likely to trust it and prefer it over non-certified products:

> *"as they're being concerned about the security they are willing to purchase the product which is certified and avoid the product which is non-certified right so it is always a good practice to have" — P8*

Similarly, participants also mentioned that consumers will be willing to spend more on a certified IoT product, especially if the product handles sensitive information.

> *"If it is a solution for some very high sensitive data, then customer will choose the higher cost product with the certification" — P16*

This perception among practitioners (i.e., of consumer-preference for certified products) aligns with prior work that shows that security labels for IoT devices can influence consumers' purchase decisions [38], [39] and that consumers are willing to spend more for secure IoT products [40].

Finding 8 ($\mathcal{F}_8$) – Practitioners are overwhelmingly in support of adopting IoT-specific security standards, and view certification as important for security assurance, especially for security-critical IoT products. Practitioners also believe that certification makes products attractive to consumers, which echoes findings from recent work.

4.4.2. Certification does not imply security. While participants agreed that security certification for IoT products is necessary, they believe that the processes involved are not accurate. **P12**'s comment summarizes this sentiment:

> *"...the way that certification process is actually implemented, is not always perfect. It's sometimes far from being perfect." — P12*

Particularly, participants recalled from experience that certification may not always lead to security, and overly focusing on fulfilling certification criteria sometimes causes them to overlook certain security issues.

> *“let’s say you have 20 criteria to follow up so sometimes what happens that if you are on too much time crunch...so you just complete the two 20 criteria, and you deliver them the product, and they inspect the 20 criteria and send us through. But those 20 criteria are not all the measurements that should be taken so there is always a flaw" — P3*

In fact, **P11** stated that focusing on unnecessary security compliance requirements actually distracted developers from the security of the product (i.e., finding and addressing vulnerabilities in the product), which may make the product less, and not more secure.

> *“in the practice, it may even reduce the level of security in some times just because it’s bring more work for the developer for the project planning and development and maybe give some less focus on the main topics but concentrate developer’s target on the certification itself." — P11*

Prior work on organizational/IT security compliance (i.e., as opposed to our context of *product* security certification) has observed similar perspectives among practitioners [41], [42], which may indicate a systemic problem with the overarching compliance certification approach in industry.

Finding 9 ($\mathcal{F}_9$) **–** In practice, compliance certification may not always improve product security, with practitioners often blaming inaccurate or cumbersome compliance requirements that distract from the task of actually addressing vulnerabilities in the product.

4.4.3. Preference between third-party certification by certification labs vs self-certification. When asked about their preference between certification by third-party labs and self-certification, most participants expressed support for an independent third-party certifying their product. Participants felt that self-certification would be biased, and moreover, that dedicated certification labs with the facilities to properly assess the product would be better, i.e., as **P1** states, to ensure that *“...a certain level of quality is being maintained."*

However, the few participants who supported self-certification argued that biases could be eliminated through cross-team testing, i.e., as **P3** describes,

> *“we have a cross-team like one team validates each other results so that way if there is any fault it will be [addressed] by other teams" — P3*

Moreover, biases and conflicts cannot be overruled even with third-party testing, particularly given how labs and standards bodies can also be affiliated with (competing) product vendors. **P2** shared a bitter experience of product security certification involving a third party lab that was affiliated with a competitor (not directly, but to an extent that the evaluation would be biased against **P2**’s product):

> *“...the third party is a company that is a kind of a competitor with us. So, the certification process was done based on bias .... disrupt the progress of the projects, and we tried to survive the disaster that caused the company." — P2*

Such experiences and imperfections in the ecosystem and processes may dissuade practitioners from seeking certification for their products using third-party labs. Instead, a few of our practitioners argued that self-certification would be beneficial to them in terms of increasing consumer trust in their brand, as it shows that the organization had *“gone to the extent of certifying the product"*.

Finding 10 ($\mathcal{F}_{10}$) **–** Practitioners generally support certification by an independent third-party lab citing biases in self-certification and the lack of adequate security testing in-house. However, third-party testing may incur its own biases stemming from conflicts of interest.

Finally, participants also asserted that third-party certification should not cause organizations to rule out internal security testing, i.e., that it is best to test the product in-house lab before going for third-party certification, which is better for security and also cost efficient, i.e., as **P14** states, *“you can do on your in-house lab so that you can go outside on a third party lab to obtain for the certificate and that will reduce the time and also the efforts because the third party labs going to charge you and it also going to delay you."*

4.5. Challenges in IoT Product Certification

Participants pointed out several challenges such as cost, time, and lack of expertise and resources that affect the proper adoption of product security certification. Some of these challenges are identical to those participants face when ensuring the security of their products ($\mathcal{F}_1$).

4.5.1. Keeping up with certifications is costly. Certification does not incur a one-time cost, but instead, practitioners often have to spend significant additional sums to maintain the certification, and to obtain re-certification for newer versions of their product, e.g., as **P1** states when asked about certification costs, *“sometimes there are some third party companies who can charge more than you imagine for a certification"*.

Cost is one of the biggest challenges that IoT practitioners face when considering product security certification. Participants from small/medium sized organizations (often called “small and medium enterprises” or SMEs) described how given their funding constraints, certification is unaffordable, e.g., as **P1** states, *“...whatever the fund we are getting, that is not even feasible for one or two months of running the operation."*

Moreover, participants describe how negotiating with various labs to bring down the costs can actually impact the quality of the security testing received, with cheaper labs also providing a faster path to certification with minimal testing, i.e., as **P15** describes,

> *“Usually what will happen, suppose if any companies doing the certification for 60,000 <local currency>, any other company (gets it done) for 50,000 <local currency>...I think that will definitely impact on the device security part" — P15*

Vendors may seek such labs that are cheap and/or provide an easy path to certification, in a phenomenon known as “forum shopping” [18], as we discuss in Section 5.

Alternately, fulfilling certification requirements in-house entails knowledgeable staff and proper facilities for security testing, which is challenging for SMEs, i.e., as **P7** states:

> *“Some of the challenges is lack of knowledgeable security experts who can do the certification. You’ll find that to get a really qualified person, you have to be willing to pay a lot. And for a company, we have not gone to that extent, having the ability to certify our own products." — P7*

SMEs with limited budgets do not have the flexibility to address these issues. Not only do they lack in-house security expertise, as discussed in $\mathcal{F}_1$, but they also the lack proper know-how regarding IoT certification (as also discussed in $\mathcal{F}_6$), which poses a significant challenge, i.e., as **P4** states,

> *“some IoT manufacturers may lack awareness or understanding for the importance and also the benefits of certification process for ensuring product quality, security, and compliance." — P4*

Finding 11 ($\mathcal{F}_{11}$) – Budget constraints and the continuous costs associated with certification severely restrict practitioners from SMEs from seeking security certification for their IoT products. Participants also offer that selecting labs based on cost may backfire, i.e., may enable cheap certification at the cost of security guarantees.

Prior work has also identified similar challenges with SMEs at large. Particularly, Wolf *et al.*’s study with Chief Information Security Officers (CISOs) with small business experience found that using proper security guidance is costly for small businesses, as there is a hidden cost for effectively implementing the security guidance [43].

4.5.2. Time to certify vs. the competitive IoT market.

Practitioners noted that while certification labs require a long period of time to test and certify products, including time for revisions and fixing vulnerabilities, IoT vendors are also under serious market pressure to release their products before their competitors. The main challenge here is that if the product fails during certification, then the development team needs to fix the discovered vulnerabilities and again redo the certification, which requires additional time and may hamper the product’s release deadline. **P14** shared an experience that exemplifies this issue:

> *“... it was 10 days long process. First attempt that we failed, we failed on the first day itself. They put our device and it failed ... by this experience, we get to know that, okay, this has to be planned earlier and this has to be included when you commit anything to your end customer as well" — P14*

The situation is even more critical if the product is already in the market, and if updates are delayed due to certification, i.e., as **P10** states, *“it (time) is very much a vital element as you are working on a product that is already in the market.... it will bounce back very heavily if things doesn’t go right."*

Participants noted that projects may get stalled or even shut down if things go wrong during certification:

> *“So if there are some issues discovered on those steps, depending on how severe those issues are, that might require you to change a small fraction of the whole solution or maybe you need to redesign everything inside out...it can even put the whole project at risk because you already invested a lot of time and money to develop something. And if that something is not meeting the standards, sometimes it requires to start from scratch almost. And in those cases, these stakeholders might run out of time or money, but time, most of the time. And in that case, they will just cancel the whole initiative." — P12*

Such unpredictable failures may play a key role in disincentivizing IoT vendors from product security certification.

Participants added that one way to address this unpredictability would be to integrate security considerations into the development process itself, so vendors have the time to plan ahead. As **P11** states,

> *“It should be planned prior to development start because it definitely will impact the deadlines" — P11*

Finding 12 ($\mathcal{F}_{12}$) – Time constraints and the unpredictable outcomes of certification disincentivize practitioners from seeking product security certification. Practitioners propose integrating compliance and security requirements early in to their development process, so as to prevent surprises during certification, and adapt their deadlines accordingly.

4.5.3. Reputation and profits come before security.

Our participants noted that the impact of certification on their reputation plays a major role in their incentive to obtain certification for their products. That is, if the product is certified, practitioners expect a boost in their reputation, increased consumer trust in their product, the ability to demand an increased price, and hence, profit. As **P5** states,

> *“obviously if there is a standard certification we will be able to demand a bit higher price from our customers" — P5*

However, if certification *fails*, i.e., if a vulnerability is discovered in a certified product that is already in the market and deployed with consumers, it can hamper both the reputation and profits. For instance, **P15**, who has previously worked with a certification lab that performs security assessment and penetration testing for IoT devices and provides certifications, states that companies are discouraged from certification precisely because of this, i.e., because *“if any security vulnerability come now in the market...it’s more like a reputation so...the company don’t want to take any risks on their reputation."*

Finding 13 ($\mathcal{F}_{13}$) **–** Product certification may bring additional profits to vendors through increased brand reputation, but also poses a risk that disincentivizes vendors from seeking it: if vulnerabilities are found in certified products, then the damage to the brand may be just as significant.

4.6. Responsibility and Liability

This section describes the participants' opinions on who they consider (i) *responsible for the process of security certification*, and who they would hold (ii) *liable for compliance failures*, i.e., for vulnerabilities in certified products. Note that we did not ask participants about their knowledge of their region's legal framework of liability while asking the questions related to liability; instead, we asked their perspectives on liability, and the findings should be interpreted in that context, as previously stated in Section 3.5.

4.6.1. Responsibility for the process of security certification. We asked participants who they think is responsible, *within their organizations* for fulfilling certification requirements properly in the event their organization would want to go for IoT product security certification. Participants responded both based on past experience and on how product security certifications are generally carried out in their current organizations. Most participants stated that their quality assurance (QA) and/or compliance teams would be assigned the responsibility, but multiple other roles would also be involved during the process, such as project managers, developers, security experts, the CTO, and in some instances, even the CEO. According to **P14**,

> *"I get involved in terms of defining the security plan, that this is what we need to do. Then the development team needs to be involved to implement those security (requirements), and then the QA need to be involved to verify the security (requirements)." — P14*

Some participants expressed a strong preference for having a dedicated person/team assigned to product security certification, but also recognized the budgetary and time-related constraints that prevented this, e.g., as **P11** states,

> *"...we should have a specific person in the team with responsibility of security (compliance)... But in reality, we are a relatively small team. We cannot afford to have a separate person only for these purposes. So we combine this role with project manager usually. Project manager is responsible for questions of security compliance and of course he is involving other team members." — P11*

P08 noted the need for a legal practitioner to be involved in the process, stating that *"some individuals from law background and practicing and advocates we who actually help us to determine the legal issues"*.

Finding 14 ($\mathcal{F}_{14}$) **–** Practitioners assign the responsibility for the process of product security compliance certification on QA or compliance teams, if available, but also note that every participant of the project should also be involved in the certification process, including developers, project managers, CTOs, the CEO, and even legal teams in case issues of liability arise.

When discussing overall responsibility for the correct implementation of the compliance certification process, most participants held the certification labs and developers as equally responsible. As **P13** states,

> *"The certification authority would be the one finally certifying that it is compliant so I'm assuming the final test is handled by them but my final call is with them because that's the authority we are trusting to make sure that it is compliant...to make the test pass, we'll have to make sure that the (development) team has to keep the compliance in mind when designing the firmware or software" — P13*

From the P13's comment, we can observe that not only participants think certification labs are responsible, they put a level of trust on them as they *"know the guidelines and know the certificates inside out (P12)"*. That it, the certification lab is the one entity who can make sure that the product fulfills all the criteria for certification. Several participants exhibit similar trust in certification labs, particularly because they are intimately aware of regulatory standards for IoT, e.g., as **P6** states,

> *"I think I trust them so much for the effort they usually do in a particular product to make sure that product is being certified and if it gets to their stage to make sure that it is linked to state and federal standards of IoT." — P6*

Finding 15 ($\mathcal{F}_{15}$) **–** Practitioners hold certification labs and product developers equally responsible for ensuring correct compliance certification, while also placing significant trust on certification labs.

4.6.2. Liability for compliance failures. If a vulnerability is discovered in a certified product, most practitioners stated that they would hold the certification labs liable, i.e.,

> *"Because if they (certification labs) had really done their job well in the certifying process, maybe they should have noticed the bug before the system is introduced into the consumers." — P7*

A few participants believe that product developers should also shoulder some blame for the vulnerability, although *after* the compliance lab, i.e., as **P10** states,

> *"The certification team, firstly, they have certified and things got wrong...logical that they have to be responsible for what they did, and eventually it comes down to developer because of that - they have developed, they have tested, like UATM tested, but there may have some new form that they did not." — P10*

However, a majority of the participants argued against assigning any blame to developers, as they believe the developers to have done their due diligence by conducting the compliance certification in good faith. That is, as **P9** states, *"this is not only the company's fault because the company always wants to release the good product"*, and that the main issue is the carelessness of certification labs. Participants often implied that they would blame everything on the last entity to sign off on the product's security (i.e., the certification lab) for all legal purposes, i.e., as **P13** states, *"a person who finally signs off as everything will be the scapegoat"*. A comment from **P1** summarizes the participants' strong preference for assigning a majority of the blame to the certification labs:

> *"...the certifying body is the main entity to assure the claim of the innovators. So if (I) say, if (as a) third party, you have certified this, I have sold this and any accident has happened. Not only I should be punished, that certifying body (should also be punished) for carelessness because it is their responsibility..." — P1*

Finally, some participants believe that no one is liable for the vulnerabilities discovered in certified products because, as **P13** states, when *"technology gets better, people crack things better"*. A comment from **P12** explains this view:

> *"But if some potential security issue is discovered after the certification process, then it's hard to blame anyone. Because basically, according to your best knowledge at every stage, so during the design development certification, we met all the requirements. And if something is discovered after that process, then basically there is nothing you can do about it." — P12*

Finding 16 ($\mathcal{F}_{16}$) – Practitioners mostly assign blame to certification labs for vulnerabilities in certified products, to the extent of holding them legally liable as entities who are the last to sign off on the product's security.

5. Discussion

Compliance and security may not always be equivalent. In fact, we find that overemphasis on compliance may distract practitioners from real security issues and may do more harm than good ($\mathcal{F}_9$). That said, product security compliance requirements may still be a net positive, as they motivate practitioners to think about security early in the development process, if only to avoid surprises, delays, and losses later during certification ($\mathcal{F}_{12}$). Recent regulatory initiatives for improving IoT product security such as the US Cyber Trust Mark program [1] rely on a similar view, of using compliance certification to motivate practitioners to build IoT products that are secure by design, even if for the incentive of passing certification with minimal effort.

However, despite the general support for compliance certification among practitioners ($\mathcal{F}_8$), we find that the awareness of IoT-specific security standards is limited ($\mathcal{F}_6$), and while practitioners do use general product security standards to certify IoT products, they are hesitant in deciding to certify ($\mathcal{F}_7$). Further, while all our findings are relevant to ongoing IoT product security certification and prior experiences of participants in certifying IoT products, only a few (namely $\mathcal{F}_3$, $\mathcal{F}_6$, and $\mathcal{F}_8$) relate to *IoT-specific security standards*.

Given these observations, we distill the findings into *four* key themes that capture the systemic challenges preventing the widespread adoption and practical implementation of IoT product security standards.

5.1. Time to Certify vs. the Budget

A common sentiment observed throughout this study is that practitioners are reluctant to pursue security certification because the process can cost them unpredictable delays in the release of their products ($\mathcal{F}_{12}$). For instance, some participants had to wait for months for the certification lab to assess and re-assess their products. In some cases, entire projects were re-designed from scratch or shelved altogether due to issues discovered during certification. Hence, participants perceived compliance certification as a hindrance that would put their products at a competitive disadvantage.

However, participants also proposed a solution that would make compliance certification practical for their products: *preparing for it in advance*, both in terms of (i) hiring security and compliance experts on product teams, and (ii) incorporating security considerations (and certification guidelines) early into the product's development. This would prevent surprises at the time of certification, and help teams predict and manage delays. However, our participants also stated that this preparation, composed of additional expertise/manpower and advance allocation of resources demands a significant increases in their operating budgets ($\mathcal{F}_{11}$). That is, there exists a natural trade-off between the *time to certify* and the *organizational costs/budget allocated for security*, which can mean the difference between a smooth certification and a constant struggle to retrofit security. This trade-off puts practitioners between two equally difficult choices, and explains why they would hesitate to certify their products in locales where certification is optional ($\mathcal{F}_7$).

5.2. No Path to Certification for Small Enterprises: An Invitation to *Forum Shopping*

This trade-off between the time to certify and the operating budget affects the IoT industry as a whole, but it most severely impacts small and medium scale enterprises (SMEs), who do not have the operating budgets to involve additional security experts during development. To elaborate, at present, there are two ways in which an IoT product is certified: *(i)* certification by a licensed third-party lab, and *(ii)* self-certification by the developer/vendor. Popular IoT standards such as IOXT [2] allow vendors to choose either for flexibility. Based on our findings, we observe that both of these ways may be inaccessible to SMEs.

As discussed previously in Section 4.5, hiring a certification lab incurs continuous costs, as the lab not only charges for certifying a specific version of a product, but also for support to address the found vulnerabilities, and additional charges for certifying every updated version. Our participants from SMEs perceive these costs charged by compliance labs as exorbitant (i.e.,*"more than you can imagine"* as **P1** puts it), and unaffordable given their project budget ($\mathcal{F}_{11}$). These costs are not unknown to regulators and standards bodies, and motivate initiatives such as the US Cyber Trust Mark to allow self-certification, so that even SMEs who cannot pay for labs would be able to get their products certified.

However, we observe that *SMEs do not have the in-house security and compliance expertise* required for self-certification, as that entails budget for additional, specialized, personnel ($\mathcal{F}_1$, $\mathcal{F}_{11}$). That is, both the current ways to certify incur costs that our participants from SMEs deem significantly beyond their reach: whether it is contracting third-party certification labs, or hiring dedicated in-house security experts for self-certification.

If initiatives such as the US Cyber Trust Mark become mandatory, that would force SMEs to pursue a third and highly undesirable alternative: *forum shopping* [18]. That is, under the present compliance enforcement model, labs have no incentive to perform their best at detecting vulnerabilities in products, as they are not licensed on their performance, but on purely procedural features (e.g., the availability of test facilities, personnel). Thus, nothing prevents SMEs from seeking labs that would be both cheap, and offer a quick route to certification with lightweight checks, an activity known as forum shopping (as discussed in Section 4.5.1, $\mathcal{F}_{11}$). Prior work has demonstrated that certified IoT products indeed have common vulnerabilities [3], which indicates that vendors may already be shopping for labs based on attributes other than security (e.g., time to certify, cost).

To summarize, both self- and third-party certification are currently out of reach of SMEs, given the lack of budget for dedicated security experts in-house, and the costs associated with compliance labs. Unless we want market forces to take over and forum shopping to prevail, it is imperative for regulators, researchers, and practitioners to make (1) product security standards and regulations accessible to the average developer at SMEs, and (2) develop usable and accessible tools for analyzing products along precise security criteria, leveraging decades of security research on helping developers write secure code [44], [45], [46], [47], [48], [49].

5.3. Liability is Unclear in the Event of Failures

If compliance certification has to carry any real weight, there must be well-defined consequences for certification failures, i.e., for vulnerabilities discovered in certified products. However, defining such consequences is infeasible without first understanding *who to hold liable* in case such failures occur. Firmly establishing liability would require a sound legal analysis of the IoT compliance standards as well as contracts among labs, IoT developers, and standards bodies, which is beyond the scope of this work. Instead, we offer relevant observations from our analysis, both related to how practitioners perceive liability, as well as the complexities of IoT product development, which illustrate the practical constraints and confounding factors that may prevent a straightforward framework for assigning liability in IoT compliance certification.

We observe that practitioners place immense trust in certification labs ($\mathcal{F}_{15}$), and hence, would also blame them for failures ($\mathcal{F}_{16}$). Note that this does not mean that practitioners want to shirk responsibility; rather, they consider themselves as responsible as the labs for participating in the compliance certification process in good faith ($\mathcal{F}_{15}$), sometimes showing the willingness to involve entire teams including the organizational leadership in the process ($\mathcal{F}_{14}$). However, participants hold labs liable because the labs are expected to have the necessary security expertise (that developers may lack) and the ability to perform extensive security testing as per the certification criteria, and because the labs are the last to "sign-off" on the product. That is, practitioners hold developers responsible for developing and participating in the certification process in good faith, but hold the labs responsible for security assurance, and hence, liable when that assurance does not hold. Interestingly, this notion of liability is in conflict with what consumers believe, as prior work demonstrates that consumers would hold the product developers as most liable, since developers are the ones who introduce the vulnerabilities in the first place [3].

Even if we hold developers liable as consumers would want to, assigning blame for vulnerabilities may not be as straightforward. For instance, we observe that independent contractors contribute to IoT products, but are neither required to maintain their contributions or fix vulnerabilities beyond the short contract period, nor to participate in the compliance certification process ($\mathcal{F}_5$). The question is, who do we hold liable for vulnerabilities in such code? That is, can we hold developers liable because the code is eventually a part of their product and hence their responsibility, akin to external library? Developers oppose this view, and reject any responsibility for vulnerabilities in external libraries ($\mathcal{F}_4$).

Alternately, we could blame the independent contractor for vulnerabilities in their code. However, we also observe that unlike first-party developers who can push back against deadlines to prioritize security, independent contractors have little agency in this respect, and have to release their code, even if vulnerable, by the deadline ($\mathcal{F}_2$). To summarize, even if developers were to be considered liable, the presence of third-party code and independent contractors makes it hard to concretely assign liability to a specific party.

5.4. Industry lacks Confidence in IoT-specific Product Security Standards

Practitioners generally view product security standards and compliance in a positive light, not only because they enable security assurance for sensitive IoT products, but also because certification may improve their reputation among consumers [3], [38], [39], and allow them to command higher prices ($\mathcal{F}_8$). However, they are hesitant toward adopting IoT security standards and undergoing certification, due to concerns about the impact of compliance failures on their reputation ($\mathcal{F}_3$). Particularly, we observe that even for IoT products, practitioners adopt general security compliance standards (e.g., UL certification [36], CE Marking [37]), and avoid IoT-specific compliance certification standards (e.g., IOXT [2], IOTSF [35]) ($\mathcal{F}_7$). These findings indicate a lack of confidence in IoT-specific standards, in comparison with general product security standards.

This contrast in how practitioners treat general and IoT-specific security standards is also observed in how developers and IoT vendors advertise them. For instance, prior work has observed that even when IoT vendors obtain IoT-specific security certifications such as IOXT, they do not advertise these certifications on their websites [3]. In contrast, vendors openly advertise general security certifications obtained for IoT products (e.g., LG's press release regarding and its Common Criteria certification for its SmartTV platform [50]).

One explanation for this behavior is that developers have grown accustomed to and are more aware of the older, general, product-security standards, relative to their limited awareness of IoT-specific standards ($\mathcal{F}_6$). That is, the industry has confidence in the general standards because they are time-tested, and also because developers are trained to work with them. Another explanation is that developers could be discouraged by the fragmentation in the IoT security standards and the general lack of stability, with several competing standards available worldwide. Regardless, as IoT security standards converge, it is imperative on the standards bodies, and in the case of initiatives such as the US Cyber Trust Mark, on the regulators, to actively work toward gaining the IoT industry's confidence.

Based on the observations in this work, we recommend three key directions to improve the perception and adoption of IoT security compliance standards: (i) *educating developers* about the standards, and providing the necessary tooling and accessible explanations to make the standards easy for the average developer to interpret and use, (ii) *strengthening compliance enforcement* by closely monitoring and regulating the labs licensed to certify products, through random audits that test the labs' performance at detecting vulnerabilities using existing techniques [51], thereby reducing the possibility of failure, and finally, (iii) developing a clear, legally enforceable framework for assigning liability in the case of compliance failures, so as to disincentivize harmful behaviors such as forum shopping, and promote sustained improvement in the state of IoT security.

6. Related Work

Prior work has studied compliance security standards for organizational security [41], [42], [43], [52]. For instance, Stevens *et al.* evaluated three compliance standards that are treated as a checklist in the organization and found several security issues in those compliance standards, confirmed by experts [41]. Further, Stevens *et al.*'s study with security professionals explored how organizations perceive compliance flaws in organizational IT security and adopt complementary measures to mitigate the security gaps [42]. Although the focus of our work is on IoT product certification, unlike the IT/organizational compliance focus in prior work, some of our findings align with those of prior work, particularly in the context of compliance requirements being inaccurate ($\mathcal{F}_9$) and the budget and time form a challenge in addressing them ($\mathcal{F}_1$, $\mathcal{F}_{11}$-$\mathcal{F}_{12}$). This may indicate that the challenges in IoT product compliance certification that we observe may be more systemic in nature, and impact the overarching compliance model.

Researchers also focus on examining compliance standards for product security [3], [53]. For instance, Rahaman *et al.* examined PCI scanners with PCI DSS-related vulnerabilities and found an alarming gap between the PCI DSS standard and its real-world enforcement in the payment card industry [53]. Furthermore, Mandal *et al.*'s work focused on IoT product security, showing that certified IoT apps have vulnerabilities within the scope of the certification standards [3]. This work also analyzed the IoT security standards and identified problems that affect the appropriate enforcement of security compliance standards (e.g., several criteria definitions in the standards are too "broad", which allows subjective interpretation of standards). Moreover, Mandal et al. also surveyed users, and obtained key insights on user perceptions on compliance enforcement. Our work on understanding how IoT practitioners practice and perceive product security compliance complements this prior work.

Similar to IoT security certifications, prior work has championed cybersecurity labels or trust marks [1], [54], [55], [56] for security or privacy-sensitive IoT products. Researchers have also emphasized the effectiveness of security labels in delivering the informative and educational value of security compliance/certification [38], [39], [57], [58]. For example, Emami-Naeini *et al.* proposed that *privacy and security labels for IoT* are important factors for IoT consumers to be informed and to be able to make purchase decisions [38]. We observe that practitioners' perspectives align with prior work in this regard ($\mathcal{F}_8$).

Finally, the Apple Store [59] and Google Play [60] have mandated app developers to submit privacy nutrition labels for their apps. A study by Li *et al.* delved into the challenges app developers face in creating privacy labels for the Apple Store [61]. The study revealed that developers often encounter recurring errors and misunderstandings, primarily due to knowledge gaps and the inherent complexity of the task. Our research reveals a significant knowledge gap among IoT developers regarding IoT compliance standards as well ($\mathcal{F}_6$). Unlike app developers who are mandated to create nutrition labels for their apps, IoT practitioners often lack the necessary knowledge and incentive to acquire it, and instead, may use general product security certification standards to certify their IoT products.

7. Conclusion

This paper describes a qualitative study based on 17 in-depth interviews with IoT practitioners from diverse security and organizational contexts. A thematic analysis of the interview transcripts results in 16 critical findings that illustrate the latent aspects that affect product certification in practice. Particularly, while we observe that IoT-specific security standards may not be well known or commonly used at present, this does not mean that IoT product certification is not occurring in industry. Instead, we find that most practitioners have certified IoT products, if only with general security standards. Moreover, time and budget constraints impose significant resource demands on enterprises, making product certification hard for small and medium scale enterprises, and motivating them to pursue the easiest path to certification at the cost of security. These findings lead us to a natural takeaway, that the present trend of adopting the traditional compliance certification model for IoT, as seen in emerging policy initiatives, will simply carry over the very challenges that hamper general product compliance to the IoT domain, and may not yield the desired security benefits.

Acknowledgments

The authors would like to thank the shepherd, the anonymous reviewers and Amit Seal Ami for their constructive feedback on the paper. The authors have been supported in part by the NSF-2237012 and NSF-2132281 grants. Any opinions, findings, and conclusions expressed herein are the authors' and do not reflect those of the sponsors.

References

[1] "Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices," https://www.fcc.gov/cybersecurity-certification-mark, last accessed on June 2024.

[2] ioXt Alliance, "ioXt: The Global Standard for IoT Security," https://www.ioxtalliance.org/, 2021.

[3] P. Mandal, A. S. Ami, V. Olaiya, S. H. Razmjo, and A. Nadkarni, ""Belt and suspenders" or "just red tape"?: Investigating Early Artifacts and User Perceptions of IoT App Security Certification," in *33rd USENIX Security Symposium*, 2024. *To Appear*.

[4] "GSMA IoT Security Guidelines Endpoint Ecosystem Version 2.2 29 February 2020," https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf, last accessed on January 17, 2023.

[5] "NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline," https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259A.pdf, last accessed on January 31, 2023.

[6] "Common Criteria," https://commoncriteriaportal.org/index.cfm, Accessed June 2024.

[7] "ISO/IEC 27017," https://www.iso.org/standard/43757.html, Accessed June 2024.

[8] "Health Insurance Portability and Accountability Act," https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[9] "The Payment Card Industry Data Security Standard," https://www.pcisecuritystandards.org/.

[10] C. S. Legislature, "California Privacy Rights Act of 2020 ("CPRA")," https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5, 2020.

[11] United States Senate, "S.965 - cyber shield act of 2021," https://www.congress.gov/bill/117th-congress/senate-bill/965, 2021.

[12] California Legislature, "Sb-327 information privacy: connected devices." https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327, 2020.

[13] Viscount Camrose, "The uk product security and telecommunications infrastructure (product security) regime," https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime, 2024.

[14] "IoTAA Security Guideline V1.2 November 2017." https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf, last accessed on February 05, 2023.

[15] GSMA, "GSMA | IoT Security Assessment | Internet of Things," https://www.gsma.com/iot/iot-security-assessment/, Accessed July 2021.

[16] "DEKRA - Cybersecurity Testing and Certification," https://www.dekra.com/en/cyber-security-b2b/, Accessed September 2024.

[17] "Red Alert Labs," https://www.redalertlabs.com/.

[18] J. Lerner and J. Tirole, "A model of forum shopping," *American economic review*, vol. 96, no. 4, pp. 1091–1113, 2006.

[19] Prianka Mandal and Adwait Nadkarni, "Online appendix for "We can't change it overnight": Understanding Industry Perspectives on IoT Product Security Compliance and Certification ," https://github.com/Secure-Platforms-Lab-W-M/IoT-product-security-certification-study/, 2024.

[20] "SmartThings Community," https://community.smartthings.com/, Accessed June 2024.

[21] "Google Nest Community," https://www.googlenestcommunity.com/, Accessed June 2024.

[22] "OpenHab Community," https://community.openhab.org/, Accessed June 2024.

[23] "Home Assistant Community," https://community.home-assistant.io/, Accessed June 2024.

[24] W. C. Adams, "Conducting Semi-Structured Interviews," in *Handbook of Practical Program Evaluation*, K. E. Newcomer, H. P. Hatry, and J. S. Wholey, Eds. John Wiley & Sons, Inc., 2015, pp. 492–505. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1002/9781119171386.ch19

[25] L. A. Goodman, "Snowball Sampling," *The Annals of Mathematical Statistics*, vol. 32, no. 1, pp. 148–170, 1961.

[26] "Upwork," https://www.upwork.com/.

[27] "Introducing Whisper," https://openai.com/index/whisper/.

[28] V. Braun and V. Clarke, *Thematic Analysis: A Practical Guide*. SAGE Publications, 2021. [Online]. Available: https://books.google.com/books?id=eMArEAAAQBAJ

[29] H. Dorussen, H. Lenz, and S. Blavoukos, "Assessing the reliability and validity of expert interviews," *European Union Politics*, vol. 6, no. 3, pp. 315–337, 2005.

[30] H. Assal and S. Chiasson, "'think secure from the beginning': A survey with software developers," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, ser. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 1–13. [Online]. Available: https://doi.org/10.1145/3290605.3300519

[31] A. Ami, K. Moran, D. Poshyvanyk, and A. Nadkarni, ""False negative - that one is going to kill you" - Understanding Industry Perspectives of Static Analysis based Security Testing," in *2024 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2024, pp. 23–23.

[32] S. C. Sundaramurthy, J. McHugh, X. Ou, M. Wesch, A. G. Bardas, and S. R. Rajagopalan, "Turning contradictions into innovations or: How we learned to stop whining and improve security operations," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 237–251. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/sundaramurthy

[33] A. Tuladhar, D. Lende, J. Ligatti, and X. Ou, "An analysis of the role of situated learning in starting a security culture in a software company," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug. 2021, pp. 617–632. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/tuladhar

[34] E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes, "Keep me updated: An empirical study of third-party library updatability on android," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 2187–2200.

[35] "IoTSF IoT Security Assurance Framework Release 3.0 Nov 2021." https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/IoTSF-IoT-Security-Assurance-Framework-Release-3.0-Nov-2021-1.pdf, last accessed on February 05, 2023.

[36] "UL Solutions - Product Certification," https://www.ul.com/services/certification/product-certification, Accessed June 2024.

[37] "CE Marking," https://single-market-economy.ec.europa.eu/single-market/ce-marking_en, Accessed June 2024.

[38] P. Emami-Naeini, Y. Agarwal, L. Faith Cranor, and H. Hibshi, "Ask the Experts: What Should Be on an IoT Privacy and Security Label?" in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 447–464.

[39] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2013, pp. 3393–3402.

[40] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "Are consumers willing to pay for security and privacy of iot devices?"

[41] R. Stevens, J. Dykstra, W. K. Everette, J. Chapman, G. Bladow, A. Farmer, K. Halliday, and M. L. Mazurek, "Compliance Cautions: Investigating Security Issues Associated with US Digital-Security Standards." in *In the Proceedings of the Network and Distributed Systems Symposium (NDSS)*, 2020.

[42] R. Stevens, F. B. Kokulu, A. Doupé, and M. L. Mazurek, "Above and beyond: Organizational efforts to complement us digital security compliance mandates," in *In the Proceedings of the Network and Distributed Systems Symposium (NDSS)*, 2022.

[43] F. Wolf, A. J. Aviv, and R. Kuber, "Security obstacles and motivations for small businesses from a {CISO's} perspective," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 1199–1216.

[44] M. Gutfleisch, J. H. Klemmer, N. Busch, Y. Acar, M. A. Sasse, and S. Fahl, "How does usable security (not) end up in software products? results from a qualitative interview study," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 893–910.

[45] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky, "You get where you're looking for: The impact of information sources on code security," in *2016 IEEE Symposium on Security and Privacy (SP)*, 2016, pp. 289–305.

[46] H. Perl, S. Dechand, M. Smith, D. Arp, F. Yamaguchi, K. Rieck, S. Fahl, and Y. Acar, "Vccfinder: Finding potential vulnerabilities in open-source projects to assist code audits," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 426–437. [Online]. Available: https://doi.org/10.1145/2810103.2813604

[47] D. C. Nguyen, D. Wermke, Y. Acar, M. Backes, C. Weir, and S. Fahl, "A stitch in time: Supporting android developers in writing secure code," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 1065–1077. [Online]. Available: https://doi.org/10.1145/3133956.3133977

[48] Y. Acar, C. Stransky, D. Wermke, C. Weir, M. L. Mazurek, and S. Fahl, "Developers need support, too: A survey of security advice for software developers," in *2017 IEEE Cybersecurity Development (SecDev)*, 2017, pp. 22–26.

[49] P. L. Gorski, L. L. Iacono, D. Wermke, C. Stransky, S. Möller, Y. Acar, and S. Fahl, "Developers deserve security warnings, too: On the effect of integrated security advice on cryptographic API misuse," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 265–281. [Online]. Available: https://www.usenix.org/conference/soups2018/presentation/gorski

[50] "LG WebOS 3.5 Smart TV Platform Earns Common Criteria Certification for Security Excellence," https://www.lgcorp.com/media/release/7247, Accessed June 2024.

[51] A. S. Ami, N. Cooper, K. Kafle, K. Moran, D. Poshyvanyk, and A. Nadkarni, "Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques," in *IEEE Symposium on Security and Privacy (S&P)*, Apr. 2022.

[52] R. Stevens, J. Dykstra, W. K. Everette, and M. L. Mazurek, "It lurks within: a look at the unexpected security implications of compliance programs," vol. 18, no. 6. IEEE, 2020, pp. 51–58.

[53] S. Rahaman, G. Wang, and D. Yao, "Security certification in payment card industry: Testbeds, measurements, and recommendations," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 481–498.

[54] "Cybersecurity Labelling Scheme (CLS)," https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cybersecurity-labelling-scheme.

[55] "Evidencing the cost of the uk government's proposed regulatory interventions for consumer IoT," https://assets.publishing.service.gov.uk/media/5f0da46ed3bf7f03aa74a79d/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products_-_technical_report.pdf.

[56] T. W. House, "The President's Executive Order (EO) 14028 on Improving the Nation's Cybersecurity," https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, May 2021.

[57] P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices," *IEEE Security & Privacy*, vol. 20, no. 2, pp. 31–39, Mar. 2022.

[58] T. Li, K. Reiman, Y. Agarwal, L. F. Cranor, and J. I. Hong, "Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels," in *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA: ACM, Apr. 2022, pp. 1–24.

[59] "The Privacy Nutrition Labels - Apple Store," https://www.apple.com/privacy/labels/.

[60] "A unified view of app safety in Google Play," https://blog.google/products/google-play/data-safety/.

[61] T. Li, K. Reiman, Y. Agarwal, L. F. Cranor, and J. I. Hong, "Understanding challenges for developers to create accurate privacy nutrition labels," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–24.

Appendix A. Interview Questions and Codebook

TABLE 2: The Semi-structured Interview Questions.

Section 1: Background
To get started, can you tell us about yourself,
What is your title and role at the company?
How long have you been in this role?
What is your company size?
Where is the headquarters of your organization?
How would you describe your target client for your product?
Which type of IoT product are you working on currently?
Section 2: IoT Security and Organization
Can you tell us more about the team you work with?
How would you describe the IoT product development process you follow?
How do you ensure the security of your product?
When you develop a product, do your client provide any specific security guidelines?
Can you tell us about product security-specific functions/components? That is, how does the team deal with product security at present?
How do you test your products? That is, Do you write test cases specifically for testing security-related requirements? Can you give us an example?
Do you remember being constrained by any factors, such as Deadline/Time, Requested Features, Dependencies, or others, when programming that may have affected/compromised security guarantees?
What are the consequences if the security requirements in your IoT products are not met? Do you recall any consequences from the past, whether to your product/team/company or any other in your knowledge?
Do you think your organization's existing coding standards, security compliance requirements, have any influence on the security of your products? Can you give us an example?
For your products, do you develop security features or use any third-party libraries? Have you implemented security features through in-house development instead of relying on third-party libraries? Why?
Between using third-party libraries for security-sensitive functionalities and implementing security-specific features on your own, which one do you prefer?
Section 3: Knowledge and Experience with Product Security Compliance Standards
What IoT Compliance Standards/IoT Certification requirements are you familiar with or aware of?
Do your clients ask you to follow any compliance standards?
Regarding policies and regulations, are you influenced by the headquarters? If so, how?
Do you have any working experience with any of the certifications while developing a product?
There are many organizations who certify their IoT products, what is your opinion about that? How do you see that?
If a developer in your team is expected to be involved with the certification process but is not familiar with it or does not have the prerequisite knowledge, how do you address it?
Section 4: Perspectives on IoT Product Security Certification
Are you familiar with Security & Privacy label or Mark? Does your company maintain any security & privacy label/mark for your IoT products?
Which role or roles would you expect to get involved in fulfilling certification requirements properly? For example, the QA team, developer, security expert, etc. And why?
Who should be responsible for the correct enforcement of IoT compliance standards/certification?(e.g., developers, certification lab, standard body). Why?
How is a particular certification standard chosen at your organization?
Between self-certification or third-party certification, which one your company would prefer to certify the product? Which one would you prefer? Why?
What are the potential challenges if IoT certification is introduced for your products? (what about the benefits?)
What are the challenges that work against adopting the IoT certification processes?
Does the compliance certification have any influence on the IoT product development, both in terms of security and just how easy it is to develop?
Does compliance certification have any influence when it comes to meeting product release deadlines?
Section 5: Vulnerability in IoT products
Does your company have vulnerability reporting program? (bug reporting program) (bug bounty program) What happens when someone submits a vulnerability report? Can you walk us through the process when it is accepted and not accepted? Can you give some examples based on your experience?
What happens if a vulnerability is found after you deliver a product?
If a vulnerability within the scope of the certification standard is found in a certified product, who would be liable for that?
Section 6: Wrap up
Is there anything else you would like to share/add to this conversation?
Is there anyone else you know who may provide us with valuable insight related to certified IoT products and/or certification standards?

TABLE 3: The codebook developed during our qualitative analysis. This codebook contains primary and secondary-level codings, as well as a description and an example for each code.

Code	Description	Example Quotes
Participants	Information related to participants such as industry experience, position and demographic information	I am the founder of this company and acting as a CEO
Organizations	Information related to participants' organizations such as company size, product type and location	the size of my company is 1,000 to 1,500 employees
IoT Product Development	Information related to IoT product development lifecycle	—
Development process	In-depth information about product development process.	Follow a software development life cycle, which comes from design, development, verification and deployment.
Challenges face during product development	Discussion of challenges that they usually face during product development	we don't have a sufficient human resource who can design these.
Developing security features in-house vs using third-party	Discussion of the preference of using in-house developed security features vs using third-party and the reasoning	The preference is, of course, to have everything in house, but you cannot always have everything in house
Product Testing	Information related to what how the product is tested and what process is followed	based on the features that we define the specification, we define the test cases.
Product Security	Information related to how they maintain the product security	—
Security requirements	General information related to the security requirements or guidelines that comes from client or customers	I don't think they do not understand this but some of them are asking about the security protocol
Security practices	Information related to what they practice in terms of product security	For the communication protocol, we do follow HTTPS and MQTT.
Challenges	Description of challenges faced to ensure security	we are lacking of the enough resources who are well aware of the security concepts from the IoT device
Security standard & guidelines	Description of security standards and guidelines they follow	we follow already the security compliance requirements in any company.
Security vs Deadlines	Discussion of priorities between security vs deadlines	we have to compromise some factors because of constraint deadlines and market rush
Compliance Standards Knowledge	Information related to participants knowledge on IoT security compliance (specific and general)	—
Familiarity with general security standards	Statements on the familiarity with general security standards and their usage	they check the OWSP vulnerabilities and all and do something
Familiarity with IoT specific security standards	Statements on the familiarity with IoT-specific security standards and their usage	I know about the NIST framework related to the iot standards
Learning process	Discussion on how to get familiar with the concepts	So if we don't know something, so we organize this Tiger team, provide them with all the requirements' information.
IoT Product Certification	Information on familiarity with IoT product certification	—
Familiarity with certification	Statements on the familiarity with certification	CE certification, we were requested but we've never done it
Experience with certification	Statements on the experience with certification if any	I have experience with UL certified product.
Necessity & Benefits	Discussion on why certification is necessary and what makes or works against companies to go for certification	I want to sell my device in the European Union, I do need to take the CE certification
Perspectives on Certification Process	Detailed discussion of participants perspective on certification process	—
Third party certification vs self certification	Discussion on the preference between third party certification and self certification, and their reasoning	Both are important. So, before going to third party, it is best to test it within your in-lab.
Responsible entity	Discussion on which is responsible for fulfilling the certification requirements and why they are responsible	that's definitely the development team cause that needs to decide what kind of security is appropriate for this product
Responsible person inside the company	Discussion on the person within an organization which is responsible for fulfilling the certification requirements and why they are responsible	there is also a compliance team that ensures that all the security standards are met
Challenges	Discussion on the challenges that work against adopting certification	clients gonna drop this part because of the times constraint and the budget constraints.
Influence on product security	Statements about how certification influence product security	it's additional security requirements meaning more secure system.
Influence on product release	Statements about how certification influence product release date	this has to be planned earlier and this has to be included when you commit anything
market perspectives	Discussion on how certification influence customers and market perspectives	They (customers) just want to use the product, and they want to be sure that the product is secure
Security and privacy Mark	Information on participants' familiarity with security and privacy mark	I know that there was an initiative, US based initiative some time ago
Vulnerability Reporting	Information on product maintenance, vulnerability reporting and fixing.	—
Service level agreement	Information about agreement on whether to solve the bug. This is especially for independent contractors.	we have a service level agreement
bug bounty program	Statements on whether they use bug bounty problem	we make use of bug bounty hunters.
Handing & fixing	Information on the process of how they handle and fix vulnerabilities	we had some weekly meetings about the problems and the bug we found
Liability for failures	Information on participants' perspectives on who is liable for vulnerable certified product	—
Nobody	Statements on why nobody is liable	if some potential security issue is discovered after the certification process, then it's hard to blame anyone.
Certification Lab	Statements on why certification lab is liable	The certification team, firstly, they have certified and things got wrong
Development team/company	Statements on why development team/company is liable	eventually it comes down to developer because of that, they have developed, they have tested
Others	Statements on why a particular entity is liable	per our company's policy, this will be liable to the chief compliance officer

Appendix B. Meta-Review

The following meta-review was prepared by the program committee for the 2025 IEEE Symposium on Security and Privacy (S&P) as part of the review process as detailed in the call for papers.

B.1. Summary

This paper presents a mixed-method study, where n=76 IoT practitioners from around the world were surveyed and n=17 interviewed. It investigates the impact that (new) IoT regulations have on the practitioners' work with IoT. The paper describes the challenges facing developers implementing security in IoT and developer perceptions of the certification process, e.g., that budget constraints prevent certification processes.

B.2. Scientific Contributions

- Provides a Valuable Step Forward in an Established Field

B.3. Reasons for Acceptance

1) The paper provides a valuable step forward in an established field. IoT certifications are an upcoming trend and a step towards reducing the IoT attack surface. This study provides insights into the obstacles experienced by different practitioners around the world with those certification processes. Those insights might help to adapt the processes accordingly.