NISTIR 8241

Organizational Views of NIST Cryptographic Standards and Testing and Validation Programs

Julie Haney
Mary Theofanos
Yasemin Acar
Sandra Spickard Prettyman

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8241

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8241

Organizational Views of NIST Cryptographic Standards and Testing and Validation Programs

Julie Haney
Information Technology Laboratory

Mary Theofanos
Material Measurement Laboratory

Yasemin Acar
Leibniz University Hannover

Sandra Spickard Prettyman
Culture Catalyst, LLC

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8241

December 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

Abstract

Cryptography is an essential component of modern computing. Unfortunately, implementing cryptography correctly is a non-trivial undertaking. Past research studies have supported this observation by revealing a multitude of errors and pitfalls in the cryptographic implementations of software products. However, the emphasis of these studies was on the practices of less-experienced, individual developers. Therefore, there is little understanding of the cryptographic development practices of organizations, including the benefits and challenges of using cryptographic resources such as standards specifications and libraries. To address this gap, a research team led by the National Institute of Standards and Technology (NIST) Information Technology Laboratory Visualization and Usability Group conducted a qualitative investigation into the processes and resources that organizations employ in the development and testing of cryptographic products. The study involved 21 in-depth interviews of 29 participants representing organizations that develop either a security product that uses cryptography or a non-security product that heavily relies on cryptography. This report categorizes and enumerates a subset of findings that document participant comments specific to NIST cryptographic publications and testing/validation programs, with a goal of informing future decisions of NIST and other standards bodies working in this space.

Key words

cryptography; development; standards; testing; validation

Table of Contents

List of Tables

1. Introduction

Cryptography is an essential component of modern computing. Unfortunately, implementing cryptography correctly is a non-trivial undertaking. Past research studies have supported this observation by revealing a multitude of errors and developer pitfalls in the cryptographic implementations of software products [1-5]. However, these studies focused on the practices of less-experienced, individual developers. Therefore, there was little understanding of the cryptographic development practices of organizations, including the benefits and challenges of using cryptographic resources such as standards specifications and libraries.

To address this gap, between January and September 2017, a four-person research team led by the National Institute of Standards and Technology (NIST) Information Technology Laboratory Visualization and Usability Group conducted a qualitative investigation into the processes and resources that organizations employ in the development and testing of cryptographic products. The study involved in-depth interviews of participants representing organizations that develop either a security product that uses cryptography or a non-security product that heavily relies on cryptography. The study aimed to answer the following research questions:

- What are the cryptographic development and testing practices of organizations?
- What challenges, if any, do organizations encounter while developing and testing these products?
- What cryptographic resources do these organizations use, and what are their reasons for choosing them?

This NIST Internal Report (NISTIR) is a companion to the research paper *"We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products* [6]. The paper explored one theme identified in the study (security mindsets) while describing findings related to the use, benefits, and challenges of cryptographic resources. Although descriptions of methodology and demographics are pulled from the research paper, this NISTIR is not meant to duplicate the findings and analysis previously presented. Instead, this report is more narrowly focused on enumerating (not interpreting) comments made specifically about NIST cryptographic products and testing/validation resources and programs, most frequently those associated with the Federal Information Processing Standards Publication (FIPS) 140-2 [7]. The target audience consists of those working on NIST cryptographic standards and testing/validation programs, but the results may also be useful to others outside of NIST that are developing related standards and programs. The purpose of this NISTIR is to inform the audience of the feedback and perceptions of NIST cryptographic standards and testing/validation programs from companies that develop cryptographic products. The feedback offers a lens into the organizational needs of consumers of NIST cryptographic standards and testing and validation programs and may help to inform future decisions concerning documentation and cryptographic efforts.

2. Background: NIST Cryptographic Standards and Testing/Validation Programs

Cryptographic algorithm standards are developed by consensus of community stakeholders (e.g. vendors, researchers, governments) to foster compatibility, interoperability, and

minimum levels of security. These standards can be found in formal documents from organizations such as the Internet Engineering Task Force (IETF) [8], International Organization for Standardization (ISO) [9], and NIST [10]. Likely due to the U.S. locations of most of the study organizations, the participants most often mentioned cryptographic requirements issued by NIST. As perhaps the best known government standard, the Federal Information Processing Standards Publication (FIPS) 140-2 “specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information" [7]. These requirements are mandatory for cryptographic products purchased by the U.S. Government, but also are used voluntarily outside the government.

There are two testing and validation programs associated with FIPS 140-2. The NIST Cryptographic Algorithm Validation Program (CAVP) provides guidelines that support conformance testing of FIPS-approved and other NIST-recommended cryptographic algorithms specified in special publications (SPs) [11]. CAVP is a prerequisite of the Cryptographic Module Validation Program (CMVP) which provides the validation of cryptographic modules [12]. Under these programs, vendors may submit algorithm and module implementations to any testing laboratory accredited under the National Voluntary Laboratory Accreditation Program (NVLAP) [13]. Labs perform certification testing, and NIST validates lab results.

3. Study Methodology

The research team conducted in-depth interviews of individuals working in organizations that develop products that use cryptography. The study was approved by the NIST institutional review board. Prior to the interviews, participants were informed of the purpose of the study and how their data would be used and protected. Interview data were collected and recorded without personal identifiers and not linked back to the participants or organizations. Interviews were assigned an identifier (e.g., C08) used for all associated data in the study. The majority of this Methodology section is taken from the previously mentioned research paper [6].

3.1. Recruitment

To enable the exploration of different perspectives within the cryptographic product space, the sampling frame consisted of individuals who had organizational experience designing, developing, or testing products that use cryptography or who were knowledgeable about and had played a key role in these activities (e.g., managers of teams that performed these tasks). The research team utilized a combination of purposeful and convenience sampling strategies, which are widely employed in exploratory qualitative research [14]. Purposeful sampling was used to select organizations of different sizes and to select participants from those organizations who had knowledge and experience within this specialized topic area. This was combined with convenience sampling, where participants were sought based on their willingness to participate in the study and their ease of accessibility by the researchers.

Nine organizations were recruited from prior researcher contacts. Additional organizations were recruited from among vendors at the RSA conference [15], a large industry Information

Technology (IT) security conference that also hosts an exhibition floor with security-focused vendors. A list of 54 potential organizations was compiled after in-person researcher contact on the exhibition floor. After the conference, the research team identified organizations that provided organizational diversity for the sample and that were accessible by the researchers. Seventeen of these organizations were invited to participate in the study via email. Eleven organizations agreed to participate. One additional organization was recruited based on the recommendation of a participant.

The high acceptance rate among solicited organizations is potentially due to the research being conducted by NIST. Many organizations were openly enthusiastic about the opportunity to provide NIST with feedback about their organizations' successes and challenges with cryptographic standards and testing/validation.

3.2. Data Collection

Data was collected via semi-structured interviews. Interviews were conducted by two of the researchers and ranged from 30 to 64 minutes, lasting an average of 44 minutes. The 21 interviews had 1-3 participants per interview, and a total of 29 participants. Five organizations opted to have more than one participant in the interview: three organizations had three participants, and two organizations had two participants. Face-to-face interviews were conducted if feasible. Otherwise, participants were given the choice of a phone or video conference interview. Five interviews were conducted face-to-face, ten by phone, and six via video. Interviews were audio recorded and transcribed by a third-party transcription service.

After the first nine interviews, the research team performed a preliminary analysis and chose to make minor revisions to the interview protocol in accordance with the qualitative research practice of theoretical sampling. Theoretical sampling involves adjusting data collection while the study is in-progress to better explore themes as they arise [16]. Following rigorous, commonly accepted qualitative research methods, the researchers continued interviewing until they reached theoretical saturation, the point at which no new themes or ideas emerged from the data [17].

The interviews began with demographic questions about the organization (e.g., size, products) and the individual participants (e.g., role within the organization, professional background). Subsequently, participants were asked to describe their organizations' development and testing practices and associated challenges for their cryptographic products. Questions then transitioned into exploring the cryptographic resources used by the organizations and how the participants thought those resources might be improved, if at all. The complete interview protocol is included in the appendix.

3.3. Data Analysis

The research team utilized both deductive and inductive coding practices. Coding is an analytical process in which data are categorized to facilitate analysis. In the case of interview data, snippets of text are labeled based on their main topic or idea, with these labels being called "codes." Snippets may consist of a phrase, sentence, or multiple sentences. For example, the snippet "I've used standards from three-letter organizations. I use NIST. I've

used ANSI. I've used ISO" was assigned the code "Standards." Related codes were later grouped into higher-level categories, called axial codes. For example, the codes "Standards," "Certifications," and "Industry/Third-party Resources" were clustered into an overarching "Resources" code.

Initially the team constructed an *a priori* list of codes based on the research questions and literature in the field to provide direction in the analysis. As the researchers performed multiple rounds of coding, they also discovered emergent codes in the data. This iterative, recursive process helped identify additional codes and categories until saturation was reached [18].

Five interviews (almost 24%) were first coded individually, then discussed as a group to develop a codebook. After coding of this initial subset of data, the remaining 16 interviews were coded by two coders each. Once each pair completed their coding, they discussed the data to address areas of divergence about their use and application of the codes and come to a final coding determination. New codes that were identified during these discussions were added to the codebook, with previously coded interviews then re-examined to account for additions.

During the coding phase, the team also engaged in writing analytic memos to capture thoughts about emerging themes [16]. For example, one memo captured thoughts on cryptography complexity. Once coding was complete, the research team reorganized and reassembled data, discussed patterns and categories, drew models, discussed relationships in codes and data, and began to move from codes to themes [19]. The team met regularly to discuss emergent ideas and refine interpretations

4. Participant and Organization Demographics

Table 1 provides an overview of the organizations and participants in the study. To protect confidentiality, product types and participant roles have been generalized.

The represented organizations were of different sizes, with six being very large (10 000 or more employees), six large (1 000 - 9 999 employees), three medium (100 - 999 employees), three small (10 - 99 employees), and three very small/micro (1 - 9 employees) [20][21]. All organizations developed a security product that uses cryptography (e.g., end user security software, hardware security module) or a non-security product that heavily relies upon cryptography to protect it (e.g., Internet of Things devices, storage devices, operating systems). Types of customers varied and included consumers, other parts of the organization, and organizations and businesses in multiple sectors such as government, technology, health, finance, automotive, and retail. Of the 15 organizations that reported how long their companies had been implementing cryptography in their products, 12 had 10 or more years of experience, with six of those having at least 20 years of experience. The remaining three organizations were startup companies that had been doing cryptographic development since their inception.

Table 1. Participant and Organization Demographics.

ID	Org Size	Product Type	Participant Roles
C01	VL	HW	Lead crypto architect*
C02	VL	COM	Lead cryptographer
C03	VL	HW, SW	Systems architect*
C04	VL	HW	Crypto design reviewer*
C05	VL	HW	Crypto architect*
C06	VS	SW	Systems analyst
C07	VS	COM	Founder & researcher
C08	VS	IOT	Founder & developer
C09	VL	IOT	Researcher
C10	L	SW	Founder & engineering lead
C11	L	HW, SW	Product manager
C12	S	SW	1) CTO 2) Marketing engineer 3) Business manager
C13	S	SW	1) Chief Evangelist 2) Strategy Officer
C14	M	SW	1) Marketing lead 2) Developer 3) Quality assurance
C15	L	SW	Principal engineer
C16	L	SW	CISO
C17	M	SW	1) CTO 2) Security engineer
C18	L	SW	Crypto engineer
C19	L	SW	CTO
C20	S	COM	1) Founder & architect 2) Compliance lead 3) Marketing director
C21	M	SW	Crypto specialist

OrgSize: VL=Very Large, M=Medium,S=Small, VS=Very Small/Micro
Product Type: HW=Hardware, SW=Software, COM=Communications Security, IOT=Internet of Things
* indicates a participant who had previous experience working in a cryptographic standards group

The 29 participants were a highly experienced group with several having made major contributions to the cryptographic field (e.g., contributing to standards, developing innovative cryptographic applications, or identifying serious flaws in standards). All participants had technical careers spanning 10 or more years, with several having been in a technical field for 30 or more years. At least one individual from each of the interviews either currently worked on cryptography and security as a major component of their jobs (19 participants), or had worked on cryptography extensively in the past (3 participants). The other participants were marketing or product leads, but all had a technical background.

Most of the participants had learned cryptography “on-the-job” as opposed to having formal training in the field. Five had an education in mathematics, but only two of those had studied

cryptography as part of their formal study. Three had an engineering education, one had a physics degree, and the rest were educated in a computer-related discipline.

5. NIST-Specific Findings

This section categorizes participant comments[1] specific to NIST standards and certifications. Given the technical expertise of this NISTIR's target audience, and because some of the examples were quite specific, longer quotes are included throughout the paper to ensure that the participants' exact words were not misinterpreted by the authors. The referenced quotes are examples that illustrate the point; not all quotes associated with each topic are included.

It should be noted that the answers to some of the interview questions reflected participants' perceptions, which may or may not reflect reality. Given that the researchers who conducted the interviews represented NIST, self-report bias [22] may have influenced participant responses. However, in general, the researchers observed that the participants did not hold back constructive criticism and were eager to share their insights as part of a community feedback effort.

5.1. Standards

All but one interview involved organizations using NIST cryptographic standards publications and test vectors, with FIPS 140-2 publications being the most commonly mentioned. The following describes participant comments specific to NIST standards, including benefits and challenges. Observations about the associated testing/validation programs and certifications are included in the next section.

5.1.1. Benefits

NIST standards were often used as a foundation for cryptographic development. Obviously, companies that sell to the U.S. Federal Government were required to use NIST standards like FIPS 140-2, but other companies voluntarily chose to reference them because of their robustness and public vetting and acceptance.

5.1.1.1. Solid Implementation Basis

NIST publications were often mentioned as a credible point of reference and a basis for cryptographic implementations:

> "Technically, we would start with NIST. The standard is the standard, and we would attempt to follow it the best we could. The fact that there's been reference implementations of the exact standard was very, very helpful to us in the beginning when we were trying to do things that hadn't been done

[1] Within the participant comments, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

before, like AES [Advanced Encryption Standard] and JavaScript or the fact that you had pseudocode or a C code. One reference implementation right in the spec [specification] or correctly connected to the spec was extremely helpful. The test suites that NIST would release were very helpful, is what we would start with. We ultimately would end up augmenting them with our own test. But I think those were very helpful in the beginning." (C10)

"I think, generally, our thinking is we should never be creating any of this stuff ourselves and that we should be always following the NIST standard for mostly assurance that we can and have done it correctly. Inventing it on your own is just a different level of complexity that we knew enough to know we did not want to be involved in that. And the fact that NIST has a review period, many people are involved, it gave us enough comfort that we could use the standards that had been followed, that we knew we weren't making a bad decision. So it gave us a lot of comfort knowing how AES evolved, all the steps, being able to see all the steps, having that all happen out in the open and why and how it happened. Very helpful to us making the decision for what we're going to use and why we're going to use it. I think it's been very helpful to be able to point at somebody and say, 'Look. This is how we do it. You can see exactly what choices we made, why we made them, why other people make them, why they are standards for the government.' " (C10)

5.1.1.2. Quality

Several participants remarked on the quality of NIST publications as a reason to use them:

"I love your documents. I read them more to kind of just make sure I understand what kind of potential best practices look like and that kind of thing." (C14)

"NIST has really decent, what I would call, documentation. Now what's interesting is, once you get into it and you understand how it's laid out and you know the basics, there's a wealth of information to be found." (C07)

"I found the algorithm descriptions and standards produced by NIST could be pretty good. I don't really have any suggestions for improvement there. I think they are clear and good." (C20)

"I do very much appreciate the work you all do. I mean, I burned a lot of trips to [office supply store] printing out NIST documents… So, thank you for the effort, the very high standards that you guys have." (C08)

"A lot of standards are notoriously difficult to read. Unless you're an expert in the field, a lot of them don't make sense. The NIST standards I think are actually probably better than most." (C12)

5.1.2. Challenges

In addition to the benefits of using NIST standards, participants voiced challenges and frustrations as consumers of the specifications.

5.1.2.1. Complexity

Given their years of experience, the study participants were generally knowledgeable enough to understand and use cryptographic standards. However, they remarked that, as is the case with most cryptographic standards, many find NIST standards to be complex.

Three people discussed the challenges that novice developers and those not expert in cryptography face when trying to understand cryptographic standards:

> "And I think the standards, whether written by NIST, or by the IETF, or by W3C [World Wide Web Consortium], or whomever, the people writing them do the best they can, but until people have grappled with the crypto issues, they won't realize the importance of this two or three little words right here or those over there." (C04)

> "We also found out that sometimes you kind of get a fresh contractor or maybe a fresh employee, and they'll look at these documents, and you can almost see people getting kind of overwhelmed by it. Part of the challenge is -- and maybe I'm biased a little bit -- not every person should be performing brain surgery on another person. I also don't believe every software engineer should really go write crypto code. Unfortunately, every large company, as you have seen, they have decided to go write their own crypto. Whether that's good or bad, it depends. But you have seen cases of how people get hacked left and right, and we can do it as well. So it's kind of a tough call because I think the NIST documents were meant for people who claim expertise in the area. And these are more helping them to kind of keep up with the latest developments, and then they kind of go do their job, and then there's certain vectors. They run those, and they're probably knowledgeable enough to build their own." (C07)

One participant remarked on the importance of "translating" highly technical information into a language that the standards consumer can understand:

> "You need to find somebody who can translate industry terms and cryptographic terms to the vernacular because most of the people who do development and have to implement or use cryptography in their software, don't have necessarily the same training I have, which is a degree in mathematics focusing on cryptology. There is a fairly complex language you have to learn, and there are some very basic concepts that you have to grasp to not mess it up." (C15)

Others commented generally on the complexity:

> "Well, I think that some of the standards are a little bit too broad perhaps…I think simplicity is always a very good thing when it comes to implementing a piece of crypto functionality. And sometimes there are too many options that create more code, more complication, more potential for bugs or misunderstandings..I think yeah, so clarity, simplicity are the most important quality." (C21)

> "I think some of the specifications of algorithms are pretty good. Some of them are a little bit confusing. So I'll give an example of the standard for key agreement schemes Diffie-Hellman, elliptic Diffie-Hellman. It seems to not quite know whether it's specifying the algorithm or a protocol or a series of protocols…And when it comes to talking about FIPS 140-2 itself, I think that is pretty confusing in places in terms of what its actual requirements are." (C21)

5.1.2.2. Context

Several interviewees commented on their perceptions of contextual issues with NIST standards publications, including a disconnect from real-world applications, a lack of transparency about the reason behind choices, and confusion about how to handle innovative applications.

Some participants thought that NIST crypto standards developers did not understand operational concerns, leading to a disparity in what they publish versus what the consumers of these publications experience and need. When a participant discussed his perception that NIST standards are not immediately testable, he conjectured about the reason for this:

> "And that's, I think because NIST don't build products so they don't understand that process. So they don't write well for it." (C05)

Two other participants felt that the standards developers were disconnected from those engaged in real-world implementation:

> "I can tell you from my personal experience understanding the fundamentals of these things, still the standards were a challenge to use because they were very divorced from the implementation day-to-day details that I encounter while I'm trying to plug all the pieces together." (C15)

> "NIST has written things about the best way to do key management, and it all tends to be a bit too academic and not actually related to what's done in the real world." (C19)

> "Software sort of randomly grows into meeting functionality. You think it's ordered but it isn't. And having to be backwards compatible, and having to quickly meet those requirements. So you tweak this. You tweak that. And jam this is in. And it works because nobody ever uses this feature which is really broken, and it sort of grows organically. And most of the guides I get from NIST doesn't take into effect that organic growth." (C19)

One participant felt that standards requirements don't allow for innovative approaches:

> "The question…is, when you get something really new and innovative, how do you take that and then start to say, 'How do I get to that base jumping off point where you can say, okay. We're going to take this idea. What's the process?' …It might be out there and I just haven't seen it…But what's that jumping off point for you guys to say, 'This is the starting off of a new standard?' " (C13)

One participant requested that NIST more clearly communicate the reasons behind standards decisions, which may motivate developers to implement them correctly:

> "Whereas other standards are, 'You shall do this, this, this, this, and this.' And, by the way, it's not as much in NIST as it is in some other standards of organizations that hate the 'teachy' part of standards. They don't like teachy. They don't want that in. To me, even in the hard core standards, it should always be-- it should always be the language which helps you put things in perspective. So you're thinking big picture, 'I'm doing this for this reason,' because otherwise, you just get in the cookbook approach of, 'Do I meet this? Yes, yes, yes. Check, check, check. I can now fly the plane. Oh! But nobody ever taught me how to fly. But I did the checklist.' " (C19)

5.1.2.3.Updates

Participants were asked how updates to standards impacted their product lifecycle. Sometimes, updates to standards specifications can be disruptive:

> "From the outside standpoint, making sure that we're still up to date and we understand what are the external factors that may change things. So, for example, NIST, a year and a half, two years ago, upped the key size requirements, right? And so I think the industry, in general…if you were looking, you knew about it. It's not like it was a secret from NIST. It was well-advertised, but maybe we, as an industry, we didn't realize the impact…I mean, I think the industry is still in the midst of that transition and you can see it from the waivers that NIST or GSA [General Services Administration] is providing to the government customers. Well, I guess we, as an industry, we could have been a little better going a little bit faster, but I guess those kinds of transitions can be disruptive and can be long-winded … I think on top of it there was also a purchasing cycle in the government. A purchasing cycle that

> also ended at the wrong time for the industry. It was just a perfect storm." (C11)
>
> "…changes to specs that arise a couple of months before a transition is due, that's almost impossible for us to deal with and causes a fair amount of angst. I mean, I can understand from the point of view of a spec is set up and then some problems are found and so they should be fixed. I don't know that there is a solution to the problem. But arriving a month or two before the transition is fully complete it can be really difficult. And I guess sometimes the requirements are a little bit confusing." (C18)

Two participants commented on interdependencies of standards, and that problems with updates to all applicable documents aren't always closely coordinated:

> "So we were kind of in a loop where we need to get out FIPS 140, but the FIPS…was changing. Do we do it before it changes? After? And then at some point, the test tools are there, but it still needs some work. And then you can't do the whole FIPS... It's difficult." (C11)
>
> "I don't know if changing all the specs that are related all at the same time would help. It might. Yeah, actually, it would make it a bit clearer if they could at least try to land them all at the same time or at least close to each other." (C18)

One participant discussed the long wait time for a standard to be finalized:

> "I think what is a bigger issue for us, is when we are developing a product with features to meet certain requirements of standards. For example, SP 800-90B [NIST Special Publication 800-90 B Recommendation for the Entropy Sources Used for Random Bit Generation] and C [NIST Special Publication 800-90C Recommendation for Random Bit Generator (RBG) Constructions]. We've been developing…to meet the requirements of those standards over our standards for three, four years now. And I don't want to be overly critical, but I think it deserves a little bit of criticism in this area as an organization. I've heard every time I've gone to a crypto module [conference] … 'Yeah, they'll be published in six months' time, still coming out in nine months' time.' … So from that point of view, I guess we don't mind changes as long as we've got a little bit of notice. But what hurts us more, I think, is the fact that there is a draft standard out there and it keeps on coming, but it never arrives." (C12)
>
> "So we're waiting for the SP 800-90B and C standards to be published and then we're waiting for FIPS 140 to get updated to allow non-deterministic brands of bit generators and evaluation. When that occurs then we'll put aside some money in the budget to go through a proper FIPS validation." (C12)

5.1.2.4. Consistency

Two participants noted an occasional lack of consistency among different standards. Unfortunately, no data was collected about the specific publications that participants thought were inconsistent.

> "I have seen that happen a few times, where one standard will say, 'You shall do this,' and another standard will say, 'You shall not do that. You should do it this way.' So I think there are certain errors, issues with that." (C12)

> "I was at the ICMC [International Cryptographic Module Conference] last week. And one discussion I was at least partially able to attend was about how to get different standards to align across different geographies. You have one side saying, 'Thou shall use AES,' and everyone's saying, 'No, you don't have to use AES.' Trying to get some alignment so that we're not chasing too many different, probably comparable standards. That's important." (C12)

5.1.2.5. Testing

Five participants mentioned challenges with current standards' testing resources and suggested additional testing support. When asked about testing challenges, one participant, remarked:

> "We often have trouble finding adequate, independently-produced test data that we can use to verify that something is working correctly. And it's gotten much better in recent years. A lot more standards recently are including that or have associated test data. But we've either found-- and we still find this a lot, that somebody says, 'Implement this thing,' and you say, 'How do I know if it's working right?' and they say, 'Well, we don't know.' And so it's very difficult to figure out. Sometimes, maybe you would do some kind of interoperability testing with something somebody else has produced, but then they don't match. You have no way of proving who's right. We have found test data that does not test adequately." (C01)

A cryptographic architect made several comments about his view of the inadequacy of current testing mechanisms:

> "… the standards-setting bodies, particularly in NIST have a role here [in cryptography testing]…They're not very good at writing standards that are immediately testable. So they'll write a bunch of English requirements. So how do I check that I've met that requirement? It's not clear. There's a lack of rigor in applying requirement to test and essentially creating those together so you know how you obtain that requirement. Other specs work that way. NIST specs certainly don't. ISO specs certainly don't. And that affects the test and validation because we can test to validate to our requirements, but we can't know we're testing and validating to government requirements." (C05)

> "… it's essentially wrong the SP800-90 spec asking you for tests with a low false positive error rate. And that implies statistically you will have a high false negative error rate which is exactly the wrong thing for security. That means you're letting bad data through." (C05)

One participant described the need for more test vectors to address corner cases and known cryptographic attacks:

> "One difficult area is what we call the corner cases. How algorithms behave if my input was zero. If something was missing, can those be used for side-channel attacks?... So even though maybe you and I know that if I run these 20 test vectors, things are great, right? But maybe there's actual value in having more vectors, so people can get a little bit more confidence on their implementation. Be also interesting for some, what I would call, a corner case analysis in this document. As an example, for certain constructs, there's requirements for padding, right? And there are multiple ways of padding the data, some of them are better than others, some of them are fine, right? But a lot of the times, testing will be implied. The person could actually do the wrong thing and still pass the test vectors…So I would venture to say that there might be value in cases where if they're known attacks or types of attacks that could be anticipated, providing a little bit more with those and then maybe providing an example of those. Because if NIST can figure it out, trust me, hackers have already figured it out as well, right? So publishing it isn't going to help them, but it's going to help an implementer now because those test vectors are no longer good. Because if you can run against them, you're not going to get caught against them. Those are not always that easy. And in some ways, if you think about it, if you thought generating a crypto library as a business and that's what you were kind of selling, you wouldn't want this to be out in the public. But the more you work on this, it doesn't appear that 'generating a crypto library' is an end business. As I mentioned, most organizations are doing their own and so forth. So we might as well actually get the right vectors out there and whatnot, to help everyone do the right thing." (C07)

A lead cryptographer had several suggestions for additional test vectors:

> "I would say, perhaps, not in the sense of easier, but provide an extra layer of security if they provided some sort of formal verification process to follow. I also appreciate step-by-step or intermediate test values, those are helpful. I've had to use that several times. I know NIST does provide some intermediate values with some of their test vectors. So those are valuable. To make them easier, perhaps provide a unit test." (C02)

> "In standards, sometimes with cryptography you have a lot of math. It would be good to have test vectors or intermediate-- I guess you would say subtest vectors - I'll call it that for now, for lack of a better word - that help

> developers understand how the operation works. So, for instance…modPow. So that's used in-- it's used in a lot of the digital signature algorithms. If you had a mod pow test vector, I think that would be useful for each size of DSA [Digital Signature Algorithm] that you guys may have or ECDSA [Elliptic Curve Digital Signature Algorithm]. That would be huge. It kind of acts as a bridge for those getting into cryptography or into the standards, because it's, typically, I would say for most software developers, the non-standard operation that you would come across. However, it's a specialty for those in numerical applications and cryptography. I would say that's of use." (C02)
>
> "It would be nice to see how a standards organization could incorporate a formal verification into standards or even validation. I would like to see something about that." (C02)

One participant suggested more interoperability testing as NIST standards are being developed. He provided examples of successful examples of interoperability testing efforts:

> "The USB [Universal Serial Bus] Consortium, the Bluetooth SIG [special interest group]. Bluetooth, when they develop new specs, they have what's called an UnPlugFest. USB has PlugFest where all the vendors get together with their new products implementing the new protocols and they try to get them to work together. And literally, everybody sits in the room and it's like speed-dating. You take your device, they take their device, plug it together and see what happens. And it's all very technical but the processes of writing the spec involves gathering data from the vendors by doing these kind of things. And, at the same time, the tests that are described are automated and that's how you can do this. In ITU [International Telecommunication Union] context you might have TTCN [Testing and Test Control Notation] as a test description language. There are other test description languages. Their software has test description languages. And the spec writes that and you can execute the test in an execution environment that can read the test out described in the spec. And it will then control how the product works and make it all happen. But that's a beautiful thing when it works together because everybody can get in the same room, run the same script, and their products work or don't work. When it doesn't, you feed that back into the spec-writing process. Because usually it comes from ambiguity in the spec and that's what you want to find. And the process of finding it and testing products for the spec is as much about finding errors in the spec as it is about finding errors in the product. The two have to both be right. So think of the process of developing the spec is as important as the process of what you end up with as the test spec for compliance to the spec. Those two things don't-- they're not ordered in time; they happen at the same time and there's an iterative process that feed on themselves. And, like I said, Bluetooth, USB do that really well. Ethernet does that really well. 802.11 does that well, but maybe not so well. FIPS certified devices, definitely not nearly as well. There's this working group in NIST where they're looking at automating tests, but the wall they're

running up against is, how do you automate a test when the spec is so woolly? Then you have many degrees of freedom to implement to the spec and the test language can't accommodate all those degrees of freedom. There's too many millions of possible configurations. So, yeah. Take making standards seriously and include all people in it so that they can bring their expertise to how to do it right." (C05)

5.2. Testing/Validation Programs and Certifications

Eighteen organizations mentioned FIPS 140-2 certifications and testing/validation, the Cryptographic Algoirithm Validation Program (CAVP) [12] or the Cryptographic Module Validation Program (CMVP) [13], and five mentioned Common Criteria [23] testing as something they undergo or reference when developing products that use cryptography. As noted in the Background section, NIST sets cryptographic standards through FIPS documents and Special Publications. The organization establishes guidelines for the conformance testing of cryptographic algorithms and modules through the CAVP and CMVP programs. NVLAP labs perform the actual testing, which NIST then validates. Once validated by NIST, an algorithm or cryptographic module is considered "certified." Of note, despite these differentiations, in their responses participants often conflated FIPS 140-2 standards with CAVP/CMVP guidelines and the actual FIPS 140-2 certifications performed by NVLAP-accredited labs.

In this section, both the benefits and the challenges mentioned in the interviews are discussed. Unless specifically noted, the comments below refer to FIPS 140-2 testing and validation.

5.2.1. Benefits

Participants noted several benefits to referencing NIST testing and validation programs, including that the certification criteria provided added assurance and were widely accepted by customers.

5.2.1.1. Added assurance/confidence

Several participants remarked that certifications guided by NIST testing and validation programs provide an extra level of confidence in addition to the organization's own testing:

> "I do think that there's some level of formalized testing, and certification is good to make sure it uses the proper algorithms and they, of course, are implemented, and so on." (C20)

> "So if the crypto primitives were already validated, for example, the FIPS 140-2 certification, we already have a baseline that we are comfortable with…The government can validate it. Then after we may build on top of that." (C11)

> "…the more scrutiny and testing it goes through the better." (C21)

Six organizations noted that, even though they do not undergo the formal FIPS 140-2 certification process, they build to and test against the testing and validation specifications to gain added assurance.

> "And I would like to add that as a small company, I think it is actually extra important to make sure that we go through this battery of tests just to in a way reassure the people we're talking to that this is a robust product, and that allows you to then have the next conversations. So I think it helps prevent the door closing too soon in the discussion." (C12)

> "I try to follow the FIPS 140-2 -- even though none of them I think have been certified --- FIPS 140-2 and try to follow best practices like doing the known answer tests on startup, implement, keeping that into the actual product." (C08)

> "But they often ask us if we are NIST certified, so we say, 'No. We are not.' But I think the competition [in our market] is not really hard, so it's not a real issue for us today, but perhaps it will become one later. But yes, they ask us, end-users sometimes ask if we use NIST certified things. We answer that we use these NIST certified primitives." (C17)

5.2.1.2. Customer acceptance and requirements

For many participants, certifications are perceived as being more useful for supporting customer requirements than for bolstering their organizations' confidence. Organizations most often obtain product certifications because these are widely recognized and required by customers in certain sectors (e.g., government, financial):

> "…when you go to the FIPS 140, that's well-established. People will know what this is about." (C11)

> "[Customers] want to do the something that they can go and see everybody in the world using." (C03)

> "[The certifications] are very critical in our ability to be able to sell to the US government. Of course, they're also important to provide a better solution to customers. So there's two aspects. Helps us make better solution for our customers, and it's also a checkmark…For some areas if you don't get the check-mark you don't get to play, so it's doubly important for us." (C11)

5.2.2. Challenges

Much data was collected on participants' views on challenges associated with certifications, including complexity, cost in time and money, lack of added value, and the disruption of updates to certification status.

5.2.2.1. Complexity

Like the standards, developers sometimes have a difficult time wading through the complexity of testing and validation requirements for certifications:

> "It's amazing how poorly understood the requirement [for FIPS testing and validation] is, or that you never know is it fully understood. And it's just a risk decision of a business unit." (C19)

Several participants had to rely on the testing labs to help them interpret the certification requirements:

> "So, sometimes the requirements were a little ambiguous. It's a standard that was written for a different time, and particularly as we were doing a software-based certification, some of the language was quite difficult to interpret. So, we had help from an external lab who advised us on how to meet the requirements and what sort of documentation was required. But, yeah, I think it would have been quite challenging without that." (C21)

> "We have to rely fairly heavily on the labs, of course, because there is no direct communication [with the NIST validation programs]. And I'm not sure that it would be solved if there was. But it can lead us down the wrong path occasionally without proper clarification. We have to work fairly closely with the labs just to keep up with that…Here in this development center we have we work with two sets of labs just with different products going through different labs. And we may end up asking both sets of labs clarification of the same questions just to get some sort of variety of opinion about how things are going to be going. And there is also a variety of opinions at that level so in the end, we will I suppose just have to…keep asking clarification by our labs until we can understand exactly what we're supposed to be doing." (C18)

> "The labs are incredibly important. We deal, as I said, with a couple of them. Sometimes though, it seems like the confusion that we have, they don't have immediate answers for either. So I don't know whether it's a matter of confusion all the way through. Often they'll say, 'We'll have to refer back to CMVP.' That's all part of the fun, but I guess it's something that happens reasonably often. Review comments from CMVP, when we go to finally validate, it's really variable. It seems to depend on the reviewer. Sometimes it'll be quite detailed and extensive comments and many things that we have to fix, and other times it seems to be quite okay just to say, 'Yes. That's fine.' I don't know what that means but sometimes it looks a little inconsistent." (C18)

5.2.2.2. Resource burden

The most frequently mentioned challenge, as noted in 12 of 21 interviews, was that the certification process can be expensive in time and resources.

> "It's very cost-prohibitive to get our own stuff listed on the NIST site [for certified cryptographic algorithms and modules]. We did, once, a long time ago. But now, since there seems like OpenSSL, where we can just leverage what somebody else has done, that's kind of the direction that we've gone." (C14)

> "…the FIPS thing is very expensive. And so, I think there could be an opportunity to make kind of certification for, if not a certification then some other-- so maybe it isn't certification. Basically, that's not as detailed as the FIPSs, but something that gives you a middle-of-the-road approach…But I do feel in the certifications is standard right now, there's basically steps or nothing which makes it kind of difficult. Like the incentive is not there for a lot of people to go through the full-step certification that they-- I think there could be benefits for getting some other kind of certification." (C08)

> "I've always seen FIPS 140 as a challenge which has driven revenue because we would be selling a product. Now, I see FIPS 140 as a challenge that keeps me from selling a product because my own engineering group doesn't have the resources, the time. They have other things they think are more valuable to put their resources on than to meet this requirement." (C19)

> "We have examples of products which, or ranges of products which, achieve an effective certification regime. I can point to Ethernet, which has certification. I can point to cell phones, which have certifications. They're run by industry bodies, and their certification…tends to be tied to designs, so I could have a software stack certified and then deploy it. The certification tends to be testable, right? Very rigorously, they've defined the requirements of the certification along with the tests that establish those. So that the designers can check whether they comply before they've gone for certification. So getting the certification is turning up and showing you pass all the tests that you've already been able to run. That's not true of NIST and NSA [National Security Agency]. So, yeah, it's kind of test by surprise; that you don't have the same tools as the validation lab-- the certification lab has to test your designs before you take it in for certification, so this is part of this exhaustive iteration and cost." (C05)

Participants also remarked that having to obtain certifications for multiple platforms can be cost-prohibitive:

> "…but the testing process is -- it's, I'd say, onerous, especially for a startup, especially someone like us who covers every platform. So when we did the

math on it, it was going to be over $100 000 per release. Because we have Windows, Mac, Linux. We have Chrome, Firefox, IE, Safari. Yeah. Every single one is separate. We have iOS, Android, Windows Phone. It just goes on and on and on…Even if I didn't change anything to do with the crypto, that's what made it kind of untenable. And there are companies that try to help solve this where they will just have their crypto piece certified and then you can license to them, but there wasn't anybody that covered all of the platforms. And we're doing stuff like in JavaScript only on the website, and so no plug-ins, no compiled code…I think when it [FIPS certification] was created, it didn't contemplate a company like ours…And I think the way the world is moving is many, many more releases. So certifying just becomes such a high bar that we just took the stance we're not going to sell to the government. They knock on our door all the time and we send them away." (C10)

Smaller companies have difficulties in affording certifications:

> "I'd say the biggest challenge is resourcing and cost. So it's one thing to develop products such that it conforms with all the past tests, it's another to actually go to a formal validation process." (C12)

> "It's a hard path. It's a long path. And for small companies, it's very resource-intensive in terms of both money and people's time to get it correct." (C13)

> "You can't really have a customer, especially in the federal government space if you're using cryptography, if you're not FIPS140-2 certified…And then, from a money perspective, how do I tell my bosses we're going to basically spend half a million dollars to get FIPS-certified and…I don't have a government customer. It's a chicken and the egg that really takes small companies and really puts us behind the eight ball." (C13)

> "Well, that's a question of choices and resources we see with small companies...We probably intend to do [FIPS certification]…But it's just a question of maturity and style, and having the people to manage it, because it's quite resource-intensive if we go ahead with the certification." (C17)

Several participants also mentioned the length of time involved in the certification process as a hindrance:

> "The biggest challenge is time. It's a fairly extensive process. We have to dedicate at least one developer to review the paperwork every time we go through a certification, and one tester is dedicated purely to running the test cases, making sure they pass all the test cases, and submitting it to the lab…So it can take six to eight months to do this, and it prevents us from being able to use those people to do more innovation. We wouldn't be doing it if we didn't find value in it, but we don't find any value in going for any higher certification." (C15)

> "We've been doing this [FIPS certification] for a few years now, and there have been challenges reasonably often. I guess sometimes it comes down to the length of time it takes to validate software or get the certificates for the software. In particular, there was a release to the software we did a couple of years ago, where it was an exceedingly long time before we got our certificate. And I can understand there were changes happening in the departments that were doing the certification, but it was well over half a year, going on to a year before we got certificates back for the software. And at that time…we have to be supporting the customers and supplying the customers these changes and…that was a difficult period." (C18)

Three interviewees suggested creating a simplified, less expensive option for FIPS certification:

> "That's one thing I would love, is if it somehow [FIPS certification] could be simplified where it would be cost-effective for us to do it. Because I get customers that…say, 'Oh, I don't see you listed on the NIST site.' And then we have to explain why we're not actually on the site." (C14)

> "I would think one of the answers might be whether NIST would certify things that are open source. That if you guys took it upon yourselves to say, 'This version is certified so long as you compile with X compiler options,' or whatever, I think that would go a huge way to kind of alleviating a lot of the burden with it." (C10)

> "I think there could be an opportunity to make a kind of certification…that's not as detailed as the FIPSs, but something that gives you a middle-of-the-road approach." (C08)

5.2.2.3. Lack of value added

Several interviews illuminated opinions that certifications did not provide significant value, even if they were required in some cases. Two participants expressed their belief that the certifications provided no assurance above and beyond what was provided by their own internal processes:

> "We always design and test ourselves to have confidence that [the product] meets all those requirements before we release it to the lab for their testing. So when they come back and say, 'It passed this,' we say, 'Well, okay, we expected that. Thank you.' So the surprise is if something fails, that we expected to pass. That doesn't happen very often." (C01)

> "…it's a place where we've done enough testing ourselves. I know it's fine. I know we would pass." (C10)

Several participants also remarked that certifications may not be a significant contributor to the security of a product. Some expressed opinions that certifications, including FIPS 140-2, are more of a customer compliance checkbox than a security defense.

> "…as nice as FIPS 140 is, it just becomes a checklist piece that people try to work around, and that, sometimes, demands so many resources it actually gets in the way of achieving security." (C19)

> "FIPS 140 is. . . not focused on how to use crypto securely. It's focused on how to safely provide crypto functionality." (C19)

> "I don't feel confident at all with third-party [certification] testing…For instance, I have a FIPS- validated product, it's entirely possible to just get a validation without any additional benefit of security. For instance, they probably haven't done a binary static analysis on their software, and so what that means is we could not be able to give a full-fledged level of confidence that it would last very long in the field…So it would be easier to reverse engineer some FIPS-validated product than, say, our own, for that very reason. It's because the FIPS validation testing does not protect against reverse engineering whatsoever. It only protects against correctness. And some hardening techniques at the higher level, such as level three, level four FIPS validation. But it does not protect against the next binary reverse engineering, whatsoever." (C02)

> "I know that FIPS validation, in terms of the business case, it could mean monetary value, but in the security sense, it doesn't really add any value. So it would be nice if FIPS validation had a business and security value together." (C02)

> "…we're more focused on ensuring customer security…through product security than on compliance to government standards. So we'll aim at compliance to government standards as one thing, but it's not the primary focus." (C05)

5.2.2.4. Product updates

In addition, seven out of 21 organizations commented that maintaining FIPS certification may, in some cases, weaken security and erode confidence by discouraging updates throughout the lifecycle of the product. Once a product undergoes a significant update (for example, a planned product revision or a bug or security vulnerability fix), it may lose its certification. Organizations are then put in a difficult position or may experience resource burdens to remedy the situation.

> "We haven't done any [certifications] yet, for two reasons. Because none of our stuff is at the fielding level, if you will. So getting into full blown production or field deployment, and stuff changes. So one of the biggest challenges of validating an algorithm is once you change it, you've got to

validate it again. And the cost for us is relatively large. So sometimes for a large company, they'll get things validated to go market it and say, ‘Hey, our stuff is validated.’ And then if things change in six months, they have the funds to go do it again.” (C07)

“The vulnerability is inside of-- let's say it's inside the FIPS module. This is the case where FIPS 140 is horrible because literally the way the rules are written now, fixing that vulnerability takes the FIPS 140 validation away. And theoretically, you should not be able to sell to a company now. So instead of fixing it, we put it in a queue. And then there's six months to a year to a year and a half to two years before it comes out. So the right thing to do is you fix it. So literally, the right thing to do is they fix it. They don't have FIPS 140 anymore, so why do they worry about FIPS 140 at all? They just lost it. The right thing to do from a security standpoint. So this ability to address vulnerabilities and to patch validated code is a real problem. It sends the wrong message if you do what you should do, which is patch it and live without it. Just live without the compliance until you're able to go through the FIPS process. In fact, the FIPS process takes so long, at some point they go, ‘Why?’ … I was at the CMVP conference three or four weeks ago, and…three or four people that program OpenSSL said their code was more secure without FIPS than with FIPS. The FIPS made it less secure. And I think one of the main reasons is this inability to quickly and agilely address vulnerabilities. So that needs to be fixed. They need to find some process.” (C19)

“Now, certification is a problem there. It's the same for medical equipment and for security equipment, that you get your certification and you're not allowed to change it. If you change the product you lose the certification for that product. And so you can have a vulnerability baked into a product and you're not even allowed to fix it because you're not then allowed to use it if it loses its certification. And there was a discussion by ICMC 2016, the International Cryptographic Module Conference, which basically FIPS 140 vendors, and certification houses, and NIST get together. And there was a discussion about this and we had [someone] stand up and say, ‘Well, that's not true, the recommendation to the government departments is to put the patch in. If there's a patch and it's a vulnerability, put the patch in.’ Then everybody else stood up and said, ‘Yeah, but that's all right for you. We're not the government, we lose our certification. What do you think about that?’ He didn't respond. And I think that got to the core of frustration in the vendor space with the way that the government does its certifications with respect to how do we address vulnerabilities and updates. A certification probably should be a-- how do I say? A process of state where you get something into this program where it's a certified design, and then the process of rolling out updates is part of the certification. So we might have an update and you have a vulnerability, and we have a change or a bug fix and that would go to NIST, and that would be a fairly lightweight, or the certification house and there would be a fairly lightweight mechanism of getting that checked and stamped

as a legitimate or necessary change in order to maintain certification. So the process is requiring updates instead of inhibiting updates." (C05)

"There's funny things that happen with the way it works today where someone can certify their own copy of something, and even though OpenSSL gets decertified because they find a bug, the copy isn't decertified because they didn't tell NIST that it is actually open to sell underneath the covers. And so the whole process seems broken, and who suffers? It's really people that require that certification. The government…pays more and people price it in. And it just wasn't my model to…We had [big tech company] and other people saying, 'Well, if you 20 X your price of your products, then we'll partner with you and go through and do the certification and then you won't change it for two to three years.' … I had a real hard time with that concept because software does have bugs. I don't want to make a cost-benefit analysis on is my bug worth the certification process." (C10)

5.2.2.5. *Certification status of third-party components*

Several participants noted challenges involving the certifications of third-party components used within their products:

"…we use wolfSSL as our cryptography, and they've got a version that is FIPS-certified and got a version that's not FIPS-certified. Now let's jump forward to our customers. Our customers are going to have to build the applications using our software, which uses wolfSSL. So now all of the sudden, we're in a really weird world in terms of FIPS." (C13)

"…programming languages often come with their own widely used, widely tested crypto libraries, but they typically aren't FIPS certified, especially not for the custom platform that might be used in IoT device for instance, or in a virtual appliance for high-security applications where you might not want to use a Java distribution for instance… So it's not just one library that you struggle to certify, it's multiple libraries written in different programming languages, some of them in the kernel. And in the R&D [research and development] process, you pretty much trust those libraries because they are widely used, and you can run test vectors against them easily. But you wouldn't implement them, you should use them. And if you have to spend $100 000 on five different libraries for every version, it becomes the showstopper pretty quickly." (C20)

"I believe most people try to somehow meet the certification requirements, but kind of live or work around it in some way, so that they have the FIPS version of the FIPS library that they use. And I have experience in having to choose the sub-optimal crypto library just because it had been certified." (C20)

One participant experienced the reverse situation in which his company's products are included in another company's product:

> "So the other problem there is who does the certification? There is an inheritance problem with the certification that if I'm a customer of [company 1] and I make a product with a [company] CPU [central processing unit], and I'm trying to get FIPS 140-2 certification, I want to be able to point to the SP 800-90 certification of the random number generator inside that product. But the certification of FIPS 140-2 requires you to show it as well, that you can do the test. And they can't do the test because it's locked up inside our silicon. They should be able to show SP 800-90 certification that that's good enough, that that was sufficient. The testing was done, and then you can just inherit that…You've met the random number generator requirement for your FIPS module. And so, thankfully, it's a small number of customers who have had that situation. But we've then had to go in and get involved in enabling that customer by working with their certification house and to get them raw data samples and the entropy source and things like that. And that's the test examples. I think this is a mess. The certification process is a mess. The way it's structured is a mess. It's counter to getting certified products out there in a widely-deployed way. And so it's a niche product to government markets, and it's one of the reasons that government products are expensive." (C05)

5.3. Education and Awareness

A number of participants commented on a need for greater education and awareness of cryptography basics and cryptographic standards for both consumers and developers of cryptographic products.

Several comments were focused on product customers:

> "…the general public…is having to become more aware of security and their information. They have to have trust and confidence in any company or organization that they deal with, that their information is being protected. That social consciousness has risen over the past few years… Such things as movies have given us an indication that you can plug something in, run a quick program, and within 10 seconds you're in. Some of that's all smoke and mirrors. It's not reality. But then, at the same time, you cannot be casual that the information about you at your local dentist, that's in their computer, is being protected. So there has to be a level of education on a much larger scale of what is encryption, what is secure information security. And when I listen to news reports and hear a politician talk about there needs to be a golden key, I think that's just he doesn't understand and know what encryption is, and he's watched too many movies. So those who are in the know need to get out there and educate." (C06)

> "Certainly, those in the industry who are developing products and certainly, clued-in users, are probably aware of your [NIST] standards. But perhaps you could do a bit more of a marketing activity to make your standards better

known to I guess, I wouldn't say the general public, but at least the IT community. Because you do have good standards. And obviously, if they are readable, they make sense. And it might benefit the entire community if there was more awareness of those sorts of standards so that actual end users take that into account when choosing products, when evaluating products. I think that'd improve the quality of products that are being deployed and used, and we improve the posture of most organizations if they're actually more aware of what standards there are and what they can do for them." (C12)

"…we have a lot of small businesses that are customers, small to medium size companies. With their limited IT resources, the documents you have are great, but they're very detailed… I don't know if maybe there could be some kind of higher level…" (C14)

"But really what our customers want is they ask for FIPS-compliant software, or they want their product to become FIPS compliant. They don't mention any particular profile which they're working. They just want to do FIPS. That's what their understanding is. And so when they say, 'And we want to make a tierless connection,' and then we have to tell them about all the constraints about what data they can use and all that sort of thing that they can actually use within a tierless connection that is still FIPS compliant, that's a major difficulty, I guess, educating our customers as well as being able to work a library that can sometimes work with FIPS restraints on it and sometimes without." (C18)

Other participants offered suggestions on ways NIST could provide more education and additional instructional information for developers and engineers:

"…sometimes it's really difficult from a software engineering perspective… First of all, writing decent code is hard. Fulfilling…this requirement to get an algorithm to properly work, isn't that easy either. And a lot of the times, these [cryptographic] attacks are based on understanding all the math. Well, there are attacks as you know for analyzing the system, looking at memory bits, and this and that, and I'm not talking about those. So it's probably more valuable to have, I guess maybe tutorials for beginners, rather than trying to plug those into a special publication, if you will. And I'd rather see in a special publication…more advanced concepts in those. And maybe there is another mechanism, maybe either a tutorial series…Maybe there's a series of crypto for beginners…I bet NIST has a ton of experts, that they could either do this in slides on a video. And maybe then those beginner folks will say, 'Huh, maybe I should go do something else, because this sounds a lot harder than I thought,' or they would actually kind of get guided up, and then they'll figure out how to get to the next level." (C07)

"…sample code is sometimes very helpful." (C20)

> "It would be useful in some way to have more motivational text and more example." (C04)

> "I guess also other intermediary steps help too. The difference between integer division versus a not integer division… Identifying particular values in an algorithm and declaring their type. There's a lot of times you'll just say like, 'Oh, hey, we were given a key K, X, Y, and Z.' And you'll have intermediate values in an algorithm. You should say what those intermediate values are by their type, not just, 'It's X divided by Y times Z,' or something." (C02)

> "With FIPS 140, there were some implementation guidance documents. And I wonder if it might be a good experiment to have, for each of the standards, an implementation guidance document that had more examples, counter-examples, here are things that people tried that don't work, and that sort of thing. I was talking with somebody recently about SP 800 90-A, and this person didn't understand the purpose of the personalization string, the nonce, the additional data context. And so I had to explain what you can use these for because there's no guidance. Well, we have these things in there for good reasons." (C04)

> "I think it's one of those things where there almost needs to, once again, be sort of an annotated version of it with, perhaps, a hypothetical deployment. Maybe a few different hypothetical deployments like a secure site, a classified site, requires these things, like a non-classified site would require these things, and actually get down to nuts and bolts. As an example, maybe not an adherent guideline, but it helps the reader interpret the guidelines. I mean, I feel like I'm a fairly educated individual, but I don't have a degree in law, and [the FIPS document] almost reads like a brief." (C15)

Two participants recommended improvements to NIST cryptography-related websites to aid in finding relevant publications:

> "…if you could have someone with a little bit more focus on user experience, look at some of those websites to make them more usable and more navigable, that would not hurt. Yeah, I mean, if you really dig a little deeper into it, it is understandable and you can parse through this, but as I came across them the first time, somewhat unenlightened, it was not exactly very intuitive. And I see it in this day and age that a lot of my more junior staff could easily be very frustrated over that experience." (C16)

> "I found it difficult at times to find what I'm looking for on the NIST website when I've been there before and I know that the document's there. I don't quite remember what the number is or the title. So some revamping of the website to make it more capable, search capable." (C14)

5.4. Trust of NIST and Governments

As evidenced by the frequent usage of NIST standards and testing/validation programs, many participants respected and trusted NIST's expertise in the cryptography domain:

> "I primarily trust NIST…" (C02)

> "I'm repeatedly impressed by working with people at NIST how competent they are, and how easy it is to work with them compared to a lot of other organizations." (C20)

However, three participants commented on distrust of government standards because of allegations of government agencies purposely trying to weaken cryptographic algorithms. This allegation also damaged trust in NIST by association. One participant, who had a favorable view of NIST, but recognized the distrust of others, suggested:

> "…seeing NIST taking a seat at the larger community table and leading with your expertise there, and making that available to a large variety of ombudsman, technology-research organizations, etc., could really foster a great collaboration, and then also essentially increase your reach as well into those organizations. I hate to say it. You guys lost a little bit of credibility over the past couple of years. So any kind of outreach to those organizations, I think, could repair some of those relationships." (C16)

Although one participant's organization made extensive use of standards, he scrutinized these due to his perception that governments try to purposely weaken algorithms for their own gain:

> "The second problems are governments who with their consistent attempts to make bad standards-- to impact standards, break cryptography-- get bad cryptography into specs. They're very good at doing that and we have to be vigilant and work against that. And we do. And I encounter that on a regular basis." (C05)

A consulting company participant observed that many of his customers distrusted government standards. This distrust, coupled with perceived usability problems with most cryptographic product interfaces, led his company to justify the development of their own crypto primitive:

> "I think it comes from the Snowden revelations and news reports or exposés that say this standard may not be as secure as we think. In this post-Snowden world, there is a lot of doubt out there. And those individuals who have concerns over privacy, and over security of information, have to be convinced that maybe that the standard is not one that is exploitable, or somebody is reading their secrets. Of course, at the same time, in my opinion, you can never know what an adversary can do. You don't know what

their level of technology is, and their capabilities, and the resources that they have, so there's never an answer to that. It's constant back and forth. That's why there has to be additional options and alternatives out there." (C06)

6. Summary

This report enumerates NIST-specific comments made by participants during an interview study of organizations that develop cryptographic products. Participants described the benefits of NIST standards and testing/validation programs as providing a quality implementation foundation, adding assurance, and being widely accepted by customers. Standards challenges included complexity, lack of incorporating real-world context, update disruption to product lifecycles, lack of consistency in some documents, and shortfalls in testing support. Testing and validation challenges included complexity and lack of understanding of the requirements, the large resource burden to undergo certification, a perception of the lack of security value, and confusion over certifications of third party crypto components. In addition to voicing the pros and cons of NIST cryptographic resources, participants also provided suggestions for improving cryptography education for customers and developers as well as insight into their trust of NIST and other government organizations within the cryptographic context.

References

[1] Acar Y, Backes M, Fahl S, Kim D, Mazurek ML, Stransky C (2016) You get where you're looking for: The impact of information sources on code security. *Proceedings of the 37th IEEE Symposium on Security and Privacy*, pp 289–305.

[2] Duong T, Rizzo J (2011) Cryptography in the web: The case of cryptographic design flaws in ASP.NET. *Proceedings of the 31st IEEE Symposium on Security and Privacy*, pp 481–489.

[3] Egele M, Brumley D, Fratantonio Y, Kruegel C (2013) An empirical study of cryptographic misuse in Android applications. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*, pp 73–84.

[4] Fahl S, Harbach M, Muders T, Baumgartner L, Freisleben B, Smith, M (2012) Why Eve and Mallory love Android: An analysis of Android SSL (in)security. *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*, pp 50–61.

[5] Nadi S, Kruger S, Mezini M, Bodden E (2016) Jumping through hoops: Why do Java developers struggle with cryptography APIs? *Proceedings of the 38th International Conference on Software Engineering (ICSE '16)*, pp 935–946.

[6] Haney JM, Theofanos MF, Acar Y, Prettyman SS (2018) "We make it a big deal in the company": Security mindsets in organizations that develop cryptographic products. *Proceedings of the 14th Symposium on Usable Privacy and Security*, pp 357-373.

[7] National Institute of Standards and Technology (2001) *Security requirements for cryptographic modules*, Federal Information Processing Standard Publication 140-2, http://csrc.nist.gov/publications/ fips/fips140-2/fips1402.pdf [accessed 8/1/2018]

[8] Internet Engineering Task Force (2018). IETF. Online https://www.ietf.org/

[9] International Organization for Standardization (2018). Standards [Web site], https://www.iso.org/standards.htmls

[10] National Institute of Standards and Technology (2018). Cryptographic standards and guidelines [Web site], https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines [accessed on 11/15/18]
[11] National Institute of Standards and Technology (2018) Cryptographic Algorithm Validation Program [Web site], https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program [accessed on 11/15/18]
[12] National Institute of Standards and Technology (2018) Cryptographic Module Validation Program [Web site], https://csrc.nist.gov/projects/cryptographic-module-validation-program [accessed on 11/15/18]
[13] National Institute of Standards and Technology (2018). National voluntary laboratory accreditation program (NVLAP) [Web site], https://www.nist.gov/nvlap [accessed on 11/15/18]
[14] Patton MQ (2005) *Qualitative research* (John Wiley & Sons, San Francisco, CA).
[15] Dell Incorporated (2018) RSA Conference: Where the world talks security. Online https://www.rsaconference.com/
[16] Corbin J, Strauss A (2015) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (Sage Publications, Thousand Oaks, CA) 4th Ed.
[17] Merriam S, Tisdell E (2016) *Qualitative Research: A Guide to Design and Implementation* (John Wiley & Sons, San Francisco, CA), 4th Ed.
[18] Glaser BG, Strauss AL (2009) *The Discovery of Grounded theory: Strategies for Qualitative Research* (Transaction Publishers).
[19] Saldaña J (2015) *The Coding Manual for Qualitative Researchers* (Sage) 3rd Ed.
[20] Gartner (2018) IT glossary: Small and midsize business (SMB). Online http://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses/ [accessed on 8/1/2018]
[21] Headd B (2015) The role of microbusinesses in the economy, https://www.sba.gov/sites/default/files/Microbusinesses_in_the_Economy.pdf [accessed on 8/1/18]
[22] Donaldson SI, Grant-Vallone EJ (2002) Understanding self-report bias in organizational behavior research. *Journal of Business and Psychology*, 17(2):245–260.
[23] Common Criteria (2018) The Common Criteria [Web site], https://www.commoncriteriaportal.org/ [accessed 8/1/2018]

Appendix: Interview Questions

1. Can you tell me about your organization - what it does, what it produces?
2. What is your role within your organization with respect to cryptographic products?
3. How did you get into this field?
   (a) At what point and why did you become concerned with cryptography and secure development?
   (b) In which field(s) is your formal education?
4. Do you work in a unit or department that is part of a larger organization?
   If yes : What is the size of the unit or department?
   (a) What is the size of your overall organization?
5. Can you tell me about the kinds of products that your organization develops, and specifically those that use cryptography?
6. Who are the typical customers for your products that use cryptography?
7. How long has your organization been working on products that use cryptography?
8. Is cryptography your organization's primary business focus, or is it an enabler within your products?
9. For your products that use cryptography, what processes or techniques , if any, does your organization use to minimize bugs and errors in code during the development process?
   (a) Why does your organization choose to use these methods? [only use if the participant has difficulty coming up with response:] for example, industry standard, customer demand, robustness and quality
10. What processes or techniques does your organization use to test and validate the cryptographic component in your products?
    (a) Why does your organization choose to use these methods? [only use if participant has difficulty coming up with response:] for example, industry standard, customer demand, robustness and quality
    (b) What kind of end-user testing, if any, does your organization do to prevent customers from misconfiguring or misusing the cryptographic component in your products?
11. Does your organization do any certifications or third-party testing?
    (a) What reasons led you to decide to use certifications or third-party testing?
    (b) How do you establish confidence in the results of the certifications or third-party testing?
    (c) What are the challenges or issues your organization has experienced with certifications or third-party testing, if any?
12. What, if any, are your organization's biggest challenges with respect to developing and testing cryptography within your products?
    (a) How do you think these challenges can be overcome, if at all?
    (b) Has your organization experienced a tension between secure development and testing and getting a product to market? If so, how has that impacted your organization's processes?

13. Do your customers have specific requirements regarding development and testing? If so, what are those requirements?
14. How do updates impact your development and testing processes, if at all? (time-sensitive vs. deprecation)
15. What resources do you use to help you develop and test the cryptographic component of your products? [only use if participant has difficulty coming up with response:] for example, standards, industry specifications, books, academic papers, standard libraries, APIs
    (a) What are the reasons that your organization chooses to use those particular resources? If the participant does NOT use standards: What are the reasons that your organization does not use standards?
16. [If the participant uses standards:] What kinds of standards do you use?
    (a) What is the role of standards in your organization's development and testing processes?
    (b) What do you see as the value or benefit of using these standards, if any?
17. How could standards or other cryptographic resources be improved to be more useful?
    (a) How could NIST standards and guidance be improved to be more useful?
18. Is there anything else you'd like to add about the topics we've discussed?