Security Mindsets in Organizations that Develop Cryptographic Products

Julie Haney
Visualization & Usability Group
NIST Information Technology Laboratory

December 15, 2021
Visualization & Usability Group

Championing the Human in Information Technology

- Public Safety
- Biometrics Usability
- AI User Trust & Usability
- Usability Standards
- Usable Cybersecurity & Privacy
NIST Usable Cybersecurity

Championing the Human in Cybersecurity

• Conduct research and usability testing at the intersection of cybersecurity and human factors

• Provide actionable guidance so that the human element can be considered in cybersecurity decisions, processes, and products
Usable Cybersecurity Projects

**Past Efforts**
- Authentication
- Security & privacy perceptions
- Cryptographic development
- Social media privacy

**Current Efforts**
- Youth passwords & security
- Phishing difficulty & susceptibility
- Smart home security & privacy
- Security adoption & awareness
"We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products

Julie M. Haney, Mary F. Theofanos, Yasemin Acar, Sandra Spickard Prettyman
Leibniz University Hannover
dcar@acis.ltn.uni-hannover.de
Culture Catalyst
aspretty60@gmail.com

ABSTRACT

Cryptography is a essential component of modern computing. Unfortunately, implementing cryptography correctly is a non-trivial undertaking. Past studies have supported this observation by revealing a multitude of errors and vulnerabilities in cryptographic implementations of software products. However, the emphasis of these studies was on individual developers; there is an obvious gap in thoroughly understanding cryptographic development practices of organizations. To address this gap we conducted 21 semi-structured interviews with developers from 21 security-oriented organizations that include cryptography in their products. Our findings support a security mindset on organizations in other research results, demonstrates by security-oriented organizations and the day-to-day practice of the performing cryptographic development. This mindset, in turn, guides the overall adoption of cryptographic resources and informs development, rigorous development, and testing practices. The enhanced understanding of organizational practices encourages additional research initiatives to explore variations in those implementing cryptography, which can aid in transferring lessons learned from more secure-mature organizations to the broader development community through educational opportunities, tools, and other mechanisms. The findings also support past studies that suggest that the availability of cryptographic resources may be deficient, and provide additional support for making these resources more accessible and useful to developers of varying skill levels.

I. INTRODUCTION

In a distributed, interconnected digital environment, cryptography protects privacy, provides authentication, ensures the confidentiality and integrity of communications, and safeguards sensitive information. Given the need for cryptography, there is an abundance of cryptographic algorithms and theories for developers willing to integrate cryptography into their products and services. However, developers often lack the expertise to utilize these choices, resulting in the introduction of security vulnerabilities. A 2016 industry survey that included over 300,000 code submissions found that 39% of these applications had cryptographic problems. Implementing cryptography correctly is a non-trivial undertaking.

In 2007, security expert Bruce Schneier commented on the lack of cryptographic implementation rigor and expertise at that time, saying, “You can’t make extreme security by lucking on cryptography as an afterthought. You have to know what you are doing very very of the way. You can’t take a system that already has a lot of other security and add a layer on top of it.” Past studies have supported this observation by revealing a multitude of errors in the cryptographic implementation of software products (e.g., [47, 74]) and the related development practices (e.g., [47]). This body of research suggests that developers have not progressed much in the past 20 years. However, as these studies have largely focused on individual practices outside the professional work context or on the development of mobile apps, it is unclear if these observations also apply to organizational development and testing, particularly among organizations for which security and cryptography are essential components. Our exploratory survey confirms high-level organizational practices in cryptographic development and testing were significantly lacking. These considerations motivate the research questions described in this study. Clearly, there is a gap in the literature in more thoroughly understanding organizational cryptographic development practices.

To address this gap, we performed a qualitative investigation into the processes and resources that organizations employ to ensure their cryptographic products are not fraught with errors and vulnerabilities. We define the scope of cryptographic products as those implementing cryptographic algorithms or using cryptography to perform some function. We conducted 21 semi-structured interviews involving participants representing organizations that develop either a security product that uses cryptography or a non-security product that heavily relies on cryptography. Unlike previous studies, our participants were professionals who were highly experienced in cryptographic development and testing, not computer science students or developers with limited cryptographic experience.

The study aimed to answer the following research questions:

Q5. What are the cryptographic development and testing practices of organizations?
Correct, secure crypto implementation can be hard

"You can’t make systems secure by tacking on cryptography as an afterthought. You have to know what you are doing every step of the way, from conception to installation."

-- Bruce Schneier, Why cryptography is harder than it looks
To develop a deeper understanding of organizations’ practices and associated challenges when developing and testing products that use cryptography.
Research Questions

• What are the cryptographic development and testing practices of organizations?

• What challenges do organizations encounter while developing and testing cryptographic products?

• What cryptographic resources (e.g., standards, certifications, libraries, documentation) do these organizations use, and what are their reasons for choosing these?
Methodology

• Interview study of 29 representatives from 21 organizations that develop products that use cryptography

• Interview questions
  ▪ Professional background and org information
  ▪ Development and testing practices
  ▪ Challenges
  ▪ Use of and suggested improvements to crypto resources
Organizations

- Varying sizes
- All developed either a security product that used crypto or a non-security product that heavily relied upon crypto to protect it
- Hardware and software products
- Customers included home consumers, internal org groups, orgs/companies in multiple sectors

<table>
<thead>
<tr>
<th>Represented Organizations by Size (# employees)</th>
</tr>
</thead>
<tbody>
<tr>
<td>very large (10,000+)</td>
</tr>
<tr>
<td>large (1,000-9,999)</td>
</tr>
<tr>
<td>medium (100-999)</td>
</tr>
<tr>
<td>small (10-99)</td>
</tr>
<tr>
<td>micro (&lt;10)</td>
</tr>
</tbody>
</table>
Participants

• All had 10+ years of experience
• At least one from each org either currently worked on crypto/security as major component of their jobs or had worked on crypto extensively in the past
• All had STEM degrees, but most had learned crypto on-the-job
• 4 had been involved in crypto standards groups
Compared to developer populations in prior studies, the organizations in our study appeared to have a stronger security culture and were more mature in their crypto and security experiences.

These security mindsets permeated the entire development process as they informed selection of crypto resources and rigorous development practices.
Security Mindset Characteristics
The level of education somebody needs to attain to be effective at doing crypto is relatively high. So, it’s not like I can put somebody who’s fresh out of school on something and expect good results.
Crypto algorithms are already very highly optimized...It’s like balancing a supertanker on a 40,000-foot-high razor blade, and if you make one small change, you destroy the performance. If you make it the other way, you just destroy the security.
**Security Culture**

**Commitment to security**

All engineers get training on secure design, and we make it a big deal in the company.

**Perpetuating a security mindset**

We take smart people who care about doing good work, and we foster an environment where they’re not afraid to receive constructive criticism.

**Size doesn’t matter**

Being a small company, we’re trying to gain credibility... We cannot afford for this thing not to work properly.
Selection of Resources
Standards

Standards are vetted and provide assurance.

The standard, because it’s out there and everybody’s looking at it and testing it, we depend on that as kind of a layer of security.

But they can be difficult to use.

The standards were a challenge to use because they were very divorced from the implementation day-to-day details that I encounter when I’m trying to plug all the pieces together.
Certifications

Some orgs believe certifications provide assurance.

You have a lot of assurance that everything’s going to be tested and get that nice, kind of warm and fuzzy.

Others are more skeptical about the value of certifications.

FIPS 140 is...not focused on how to use crypto securely. It’s focused on how to safely provide crypto functionality.
Third-Party Implementations

"[Crypto libraries] in general don’t provide enough to be able to use them correctly out of the box...But there’s many out there that think that they can just use AES. “I included it and I’m using it.” But I’m not using it correctly, and then I’m leaving myself open to attack."
We don’t reference academic papers. They’re not where we are in understanding the test problem...
There’s a six-year gap between the methods that we developed being identified in academia.
Development & Testing Rigor
We have architects that do security reviews, that do threat modeling. And it’s not just about the crypto but more in general, how do you use the product? Who gets to do what? What are the risks? How do we mitigate those risks?...And one of the items for the engineering gate release is making sure...we mitigated anything that needs to be mitigated.
Development & Testing Challenges

- Time to market vs. security
- Vulnerability testing
- Longevity of products
- Product updates
- Test vectors
- Keeping up with standards
- Multiple platforms
Takeaways
Contributions

• Explores crypto development practices and security mindsets in organizations from viewpoint of those with extensive experience in the field
• Provides systematic validation to anecdotal point that good crypto is the result of a concerted effort
• Aids in transferring lessons learned from more security-mature orgs to the broader development community
• Suggests usability improvements for crypto resources
Organizational Views of NIST Cryptographic Standards and Testing and Validation Programs

Julie Haney
Mary Theoefanos
Yasemin Acar
Sandra Spickard Prettyman

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

• Benefits
  • Solid implementation basis
  • Quality

• Challenges
  • Complexity
  • Lack of context
  • Updates to standards
  • Inadequate test data/vectors
NIST Testing/Validation Programs & Certifications

• Benefits
  • Added assurance/confidence
  • Customer acceptance

• Challenges
  • Complexity of requirements
  • Resource burden
  • Perceptions of lack of value added
  • Product updates
  • Certification status of third-party components
Education and Awareness

Product customers

What our customers want is they ask for FIPS-compliant software...They don’t mention any particular profile...They just want to do FIPS. That’s what their understanding is.

Developers and engineers

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 or a video. And then maybe those folks...would actually kind of get guided up, and then they’ll figure out how to get ot the next level.
Trust of NIST and Governments

Many trust and respect NIST’s expertise

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.

But others distrust government standards

Governments who with their consistent attempts to make bad standards – to impact standards, break cryptography – get bad cryptography into specs
Thank you!
Whitfield Diffie
Pioneer of public-key cryptography and 2015 recipient of Turing Award

https://primetime.bluejeans.com/a2m/live-event/uvyugstq
Questions?

julie.haney@nist.gov

https://csrc.nist.gov/usable-cybersecurity
