"We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products

Julie Haney & Mary Theofanos
National Institute of Standards and Technology (NIST)

Yasemin Acar
Leibniz University Hannover

Sandra Spickard Prettyman
Culture Catalyst

Cryptography

"The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification." (NIST SP 800-59)

- Standards examples: RSA, ECDSA, AES, SHA-256, TLS, FIPS 140-2
- Standards organizations: IEEE, ISO, IETF, ANSI, NIST, etc.
- Certification examples: FIPS 140-2, PCI DSS, Common Criteria

Cryptographic products are those that implement a crypto algorithm or use crypto to perform or support some function

Motivation

- Correct, secure crypto implementation is non-trivial
- Prior work focused on individual developers with little crypto expertise
- Limited understanding of how organizations approach development and testing for cryptographic products

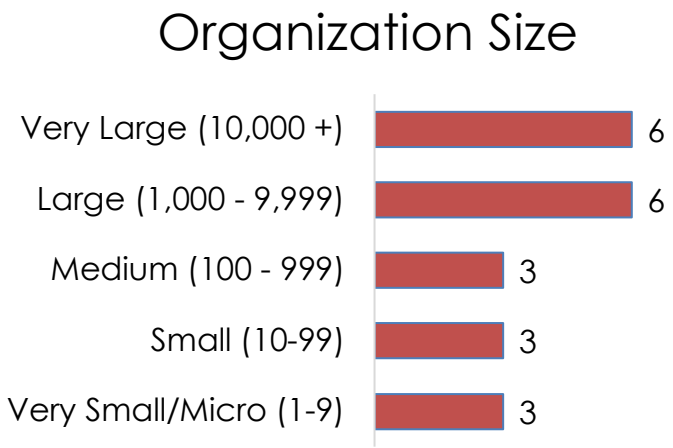
Research Questions

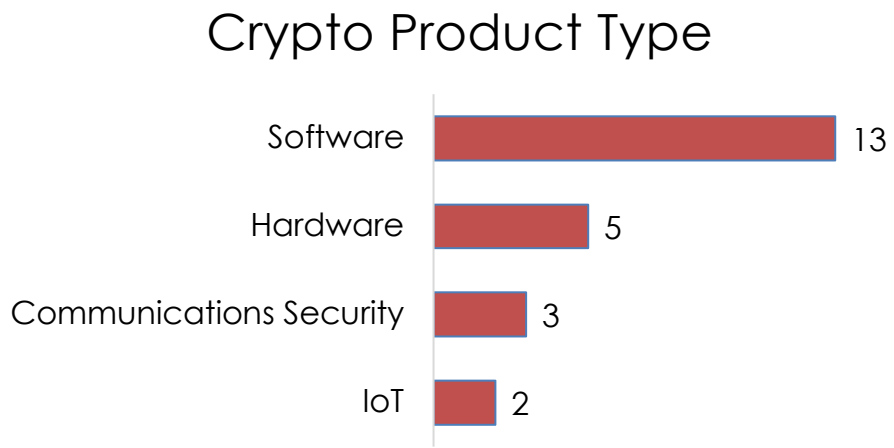
- What are the cryptographic development and testing practices of organizations?
- What challenges do organizations encounter while developing and testing cryptographic products?
- What cryptographic resources (e.g., standards, certifications, libraries, documentation) do these organizations use, and what are their reasons for choosing these?

Methodology

- Semi-structured interview study of representatives from 21 organizations that produce cryptographic products
- Recruited participants from a prior crypto survey and amongst vendors at RSA Conference, aiming for diversity of organization size and product type
- Questions - demographics, dev and testing practices, challenges, use of and suggested improvements to crypto resources
- Qualitative analysis – open coding, axial coding, memos, identification of relationships and core concepts/themes

Organization Demographics





Most had long histories of crypto development (15 reported)

- 12 with 10+ years experience developing crypto products, 6 of those with 20+
- 3 in existence < 10 years, but founders came from companies with long-established crypto development programs

Participant Demographics

29 participants in 21 interviews

Unlike past studies, these were experts in their field

- 22 had worked on crypto and security as major component of their jobs
- All had technical backgrounds with 10+ years experience, some decades
- Most had learned crypto “on-the-job” with no formal training
- Four had worked on crypto standards

Results

Disclaimer: Certain commercial companies and products are 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.

It’s all in the mindset.

- Security is “Core Value”, “Key to Quality”, ”Essential to Company Identity”.

“In our company, we are developing and selling security to our customers. So we care about, basically, all three sides of the sort of security triangle [confidentiality, integrity, availability] in what we do.’’

C15

It’s the culture.

”We have some fairly large teams which concern themselves with cryptography and secure design methodology. All engineers get training on secure design and we make it a big deal in the company.”

C05

“We serve the kinds of customers who rely on the stuff to work reliably and properly from the get-go, when they buy it. So it's not like `Maybe we'll update something later, if we find some problems.' That's not our philosophy, and that's not what our kind of customers expect. Part of that is also company culture.”

C01

Experience learned on the job

- Experience and maturity are needed to do crypto.

"We have a couple of the same core people on our test team who've been here for 25 years. They've gotten very good."

C01

"Everyone we have has a lot of experience. I think the most junior person has a master's degree and 10 and a half, 11 years of experience."

C07

Focusing on the process

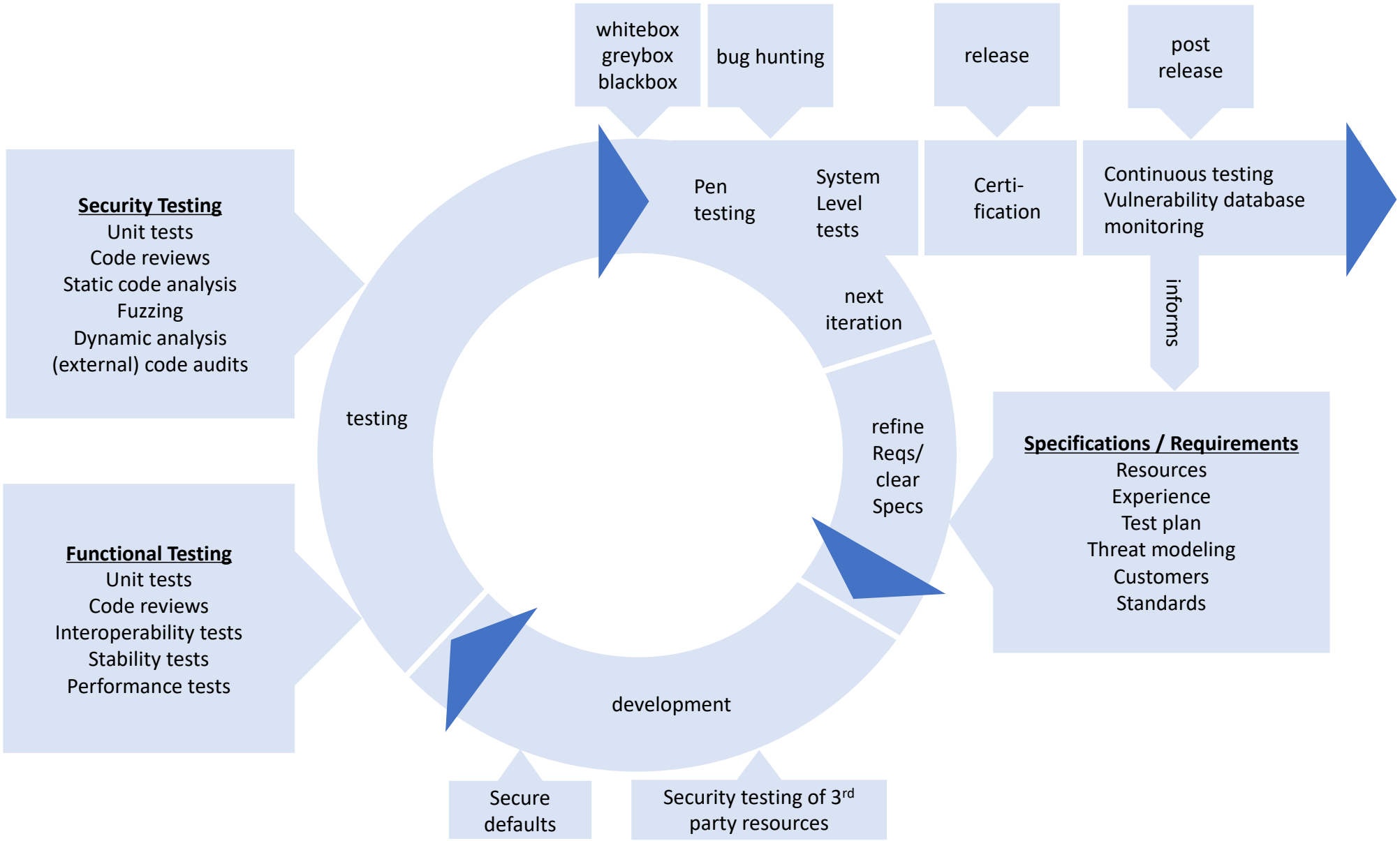
- There is no magic trick – it's all in the process.

``We have a mandatory and systematic code review. Each line of code and each comment of code needs to be reviewed by usually at least two peers.

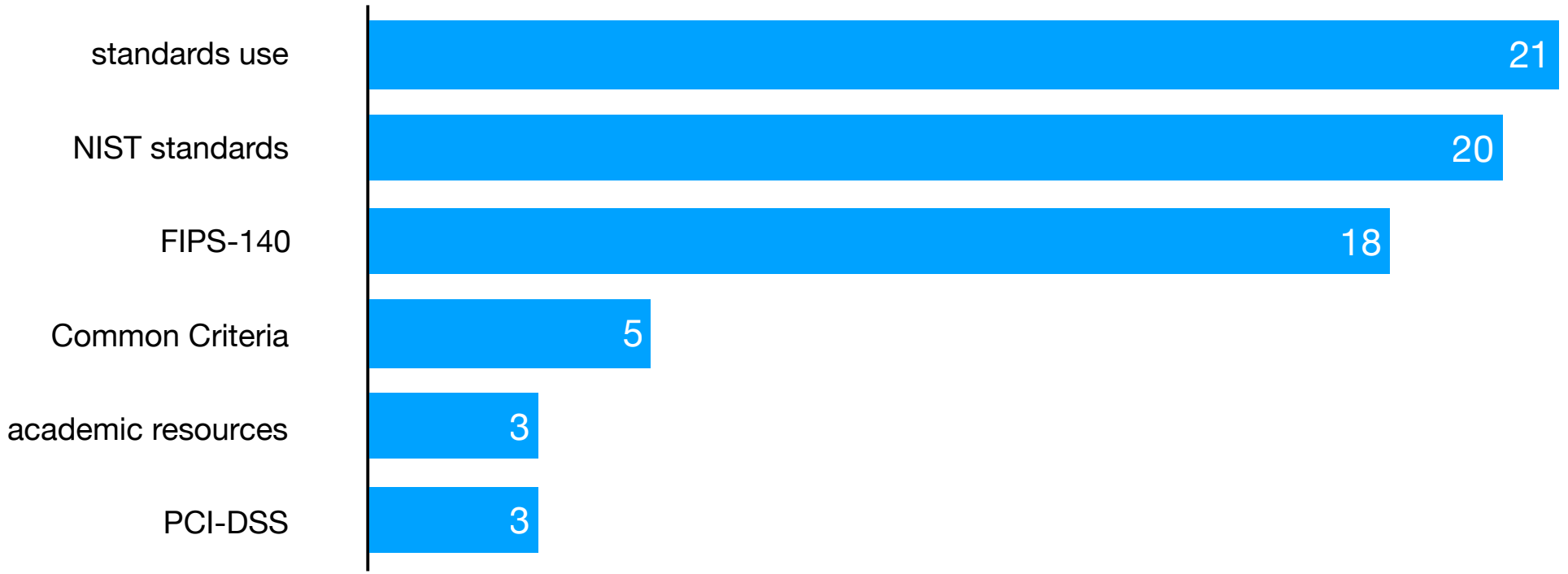
We have automatic tests, unit tests, integration tests, functional code analysis... We have additional, manual tests being done on top of the automated tests."

C17

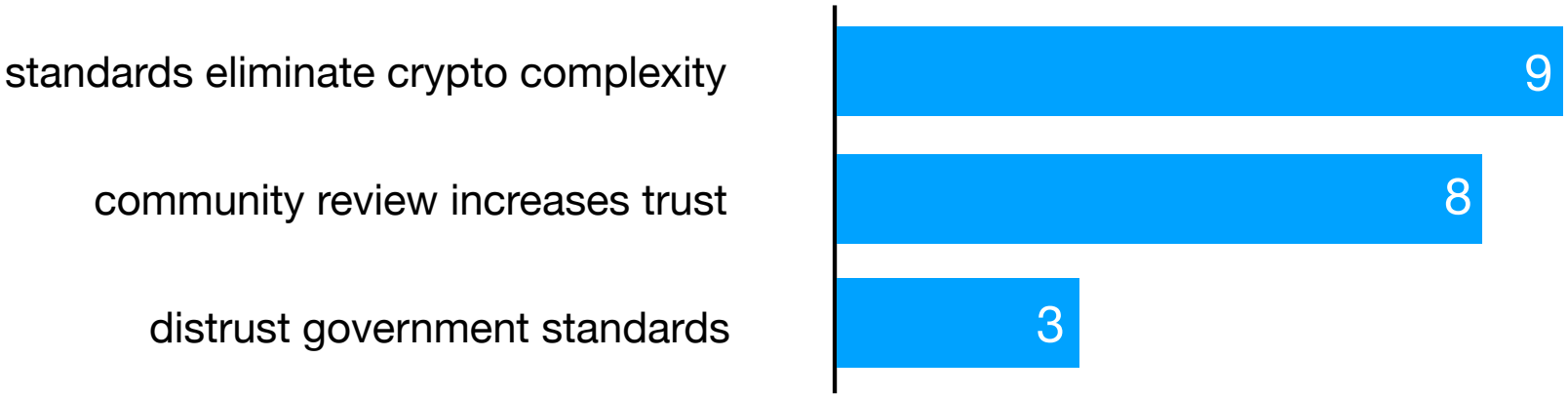
Careful adherence to best practices



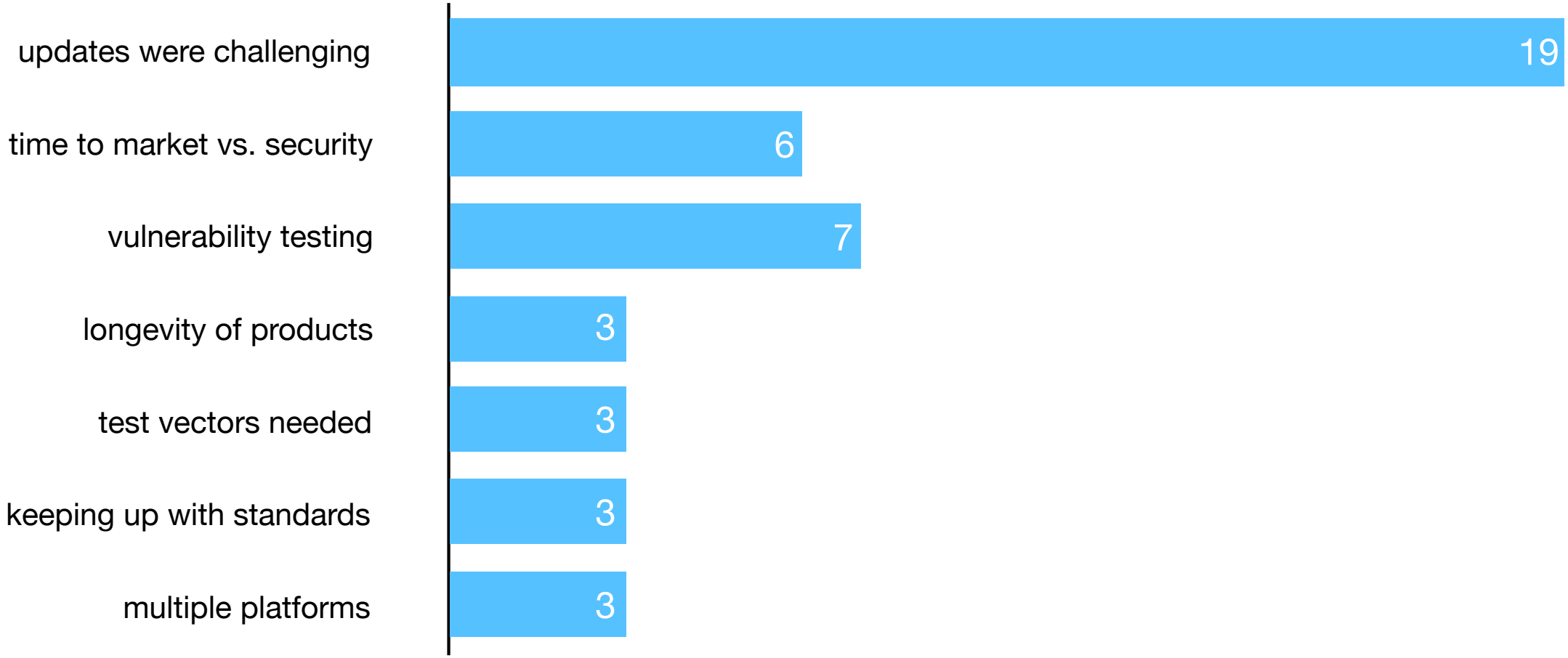
Resources


standards use
21
NIST standards
20
FIPS-140
18
Common Criteria
5
academic resources
3
PCI-DSS
3

Trust in Resources



Challenges


updates were challenging
19
time to market vs. security
6
vulnerability testing
7
longevity of products
3
test vectors needed
3
keeping up with standards
3
multiple platforms
3

Implications

- Crypto education
  - How to teach a mindset?
  - How to convey the importance of testing?
  - How to ”streamline” years of experience and education learned “on the job”?
- Crypto resource usability
- Certification usability
  - Multiple platforms, updates, cost
- Better integration of academic research and crypto community

Summary: Crypto takes a lot of experience.

- Insight into crypto expert population
- Strong security mindset; process-oriented
- Experience and skillset learned on the job
- Standards go-to resource; usability a major challenge

"We cannot afford for this thing not to work properly."

C07

julie.haney@nist.gov
mary.theofanos@nist.gov
acar@sec.uni-hannover.de
sspretty50@icloud.com