Collateral Damage

Impact of Frequent Policy Changes on Vendors and Customers

Joshua Brickman
Director, Security Evaluations
Oracle Global Product Security

Glenn Brunette
Distinguished Security Architect
Oracle Global Product Security

November 6, 2015

Today's Speakers

- 25 Years Information Security Experience
- 16 Years with Oracle (incl. 11 Years with Sun)
- Customer Security Compliance Focus

Glenn Brunette

- Leads Security Evaluations @ Oracle
- Frequent Speaker at Security Conferences
- Completed Many Cert. Projects since 2006

Josh Brickman

Session Agenda

1. Background
2. Customer Experiences
3. Vendor Challenges
4. Recommendations
5. Q&A

Background

Oracle

- 132,000 Employees
  - 36,000 Developers and Engineers
- 1,000s of Products and Services
  - #1 in 50 product/industry categories
  - #2 software company in the world
  - #2 cloud company in the world
- 400,000 Customers
  - Across 145 Countries

Background

Oracle and FIPS 140

- Validating Oracle Developed Modules
  - e.g., Oracle Solaris Cryptographic Framework, Oracle StorageTek T10000 Tape Drives, Java Card Platform, Acme Packet Session Border Controller
- Leveraging Third-Party Validated Modules (“FIPS Inside”)
  - RSA BSAFE Crypto-C Micro-Edition
  - RSA BSAFE Crypto-J
  - OpenSSL
- Many Products Contain Multiple Modules

Customer Pain Points

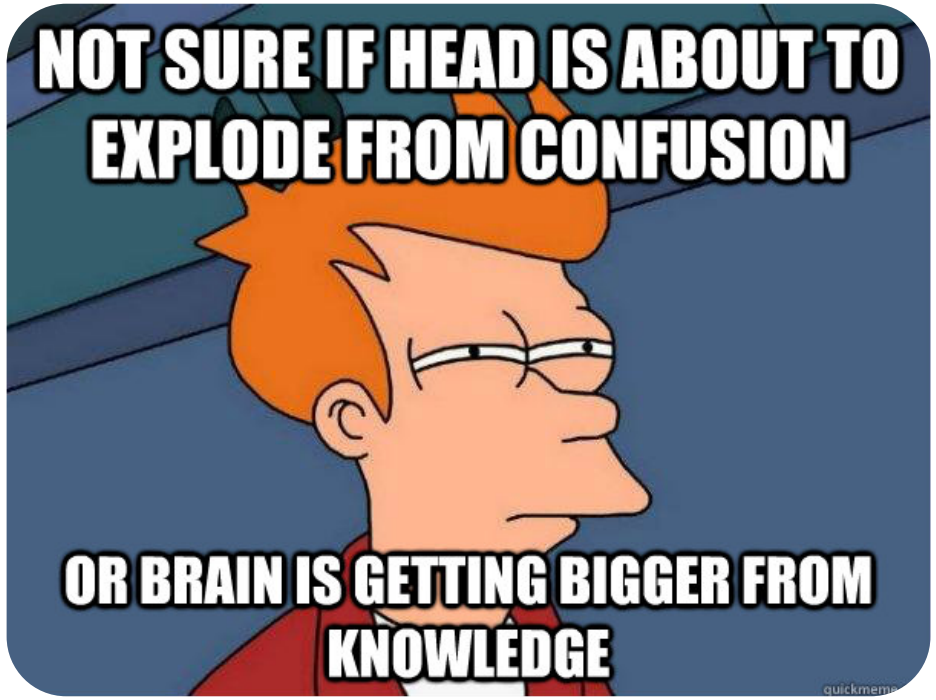
Education and Awareness

Comparing Apples and Oranges

Operational Decisions

Education and Awareness

- FIPS 140 Approved vs. Validated
  - Complicated Landscape to the "Outsider"
  - e.g., FIPS 197, NIST 800-38A, CAVP/CMVP Lists, IG
- Degree of Algorithm Specificity
  - "Encrypted" versus "AES" versus "AES-256-CTR"
- Module vs. Product Validation
  - Is "Oracle WebLogic" FIPS 140 validated?
- FIPS Inside vs. Vendor Validations
  - "I checked the CMVP site and you are not listed."



ORACLE

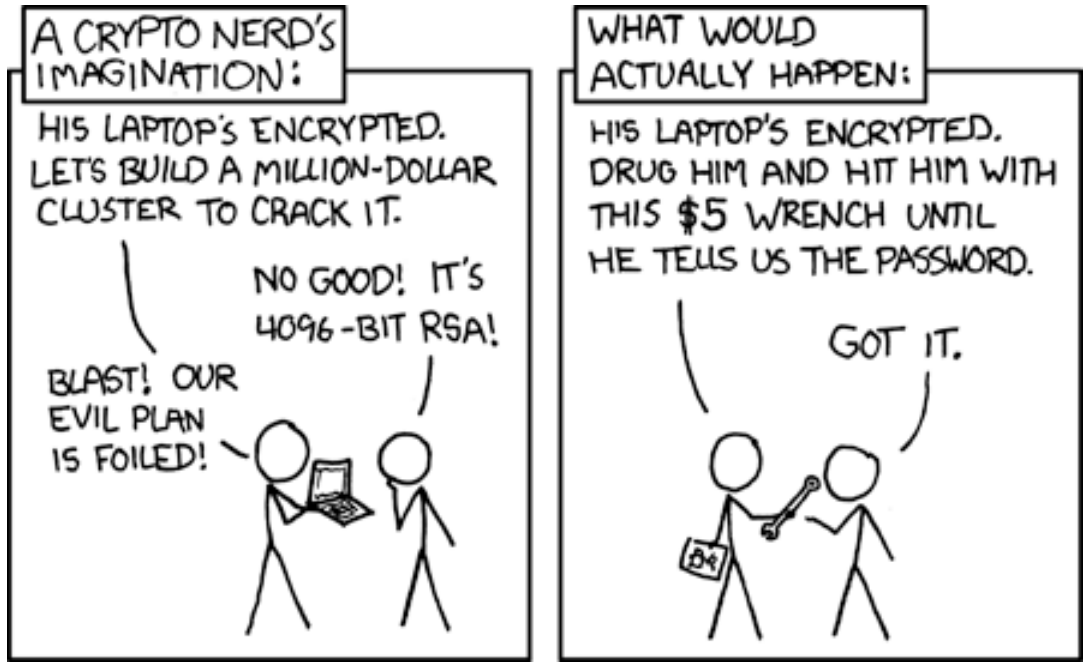
Comparing Apples and Oranges

"Explain to me how comparing apples and oranges is fruitless."

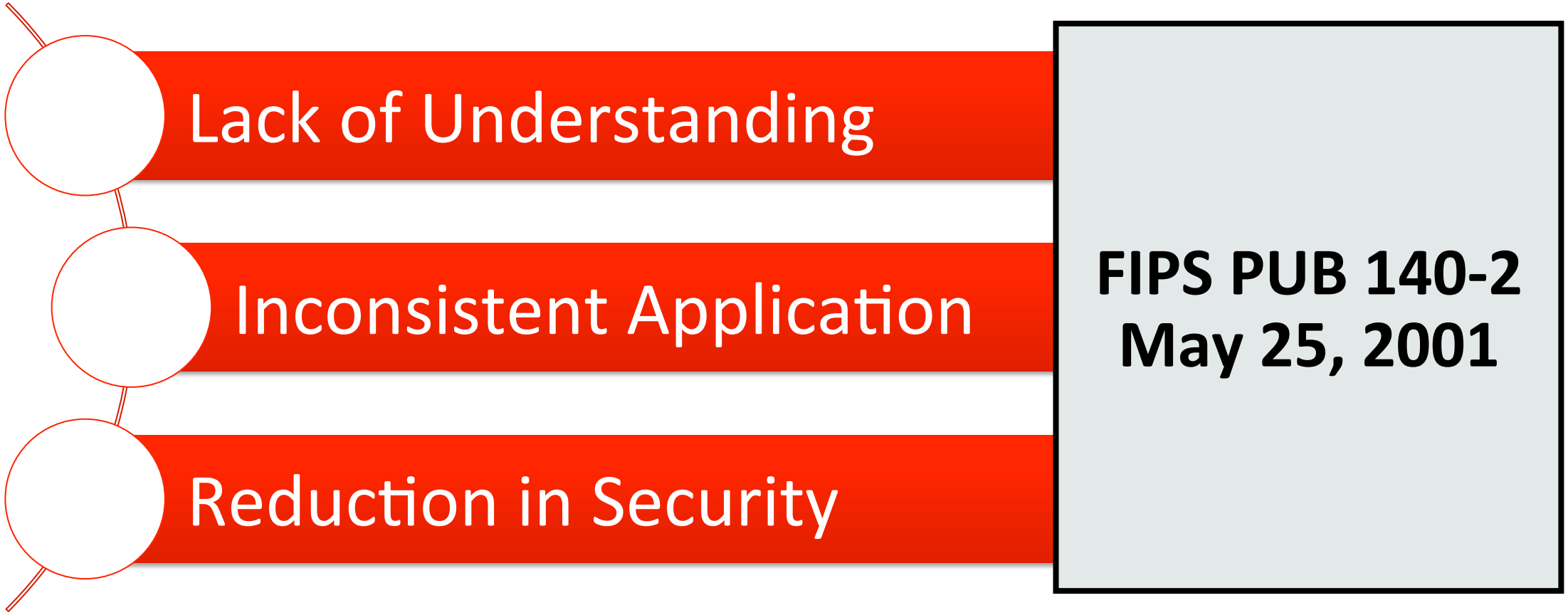
- Module Versioning != Product Versioning
  - Especially challenging with "FIPS Inside"
  - Module versioning can be somewhat arbitrary
  - Specificity of product versioning can also be challenging
- Mapping Product Cryptography to Modules
  - Products may not validate every cryptographic module
  - "What underlying module provides a given cryptographic service or function?"
- Cryptography in "Nested Products"
  - Satisfying compliance documentation mandates can get tricky...

Operational Considerations

- Understanding Requirements Scope
  - Data at Rest? Data in Transit? Business versus Management/Operations Uses?
- Ill-advised "Workarounds"
  - Avoid using cryptography
- Lack of Organizational Expertise
  - Keeping up is somewhat predicated on already "being up to speed"?
  - FIPS 140 requires a broad and diverse organizational understanding



Customer Experiences Summary



Changes are Coming

It's been a long time coming

But I know a change is gonna come,

oh yes it will,

--**Sam Cooke, A Change is Gonna Come,** *1964*

Wants

- NIST/CMVP **want** the strongest crypto now for their customers
- Vendors **want** the strongest crypto for their customers (with the least performance impact)
- Customers **want** the highest security for acquired products for the lowest price

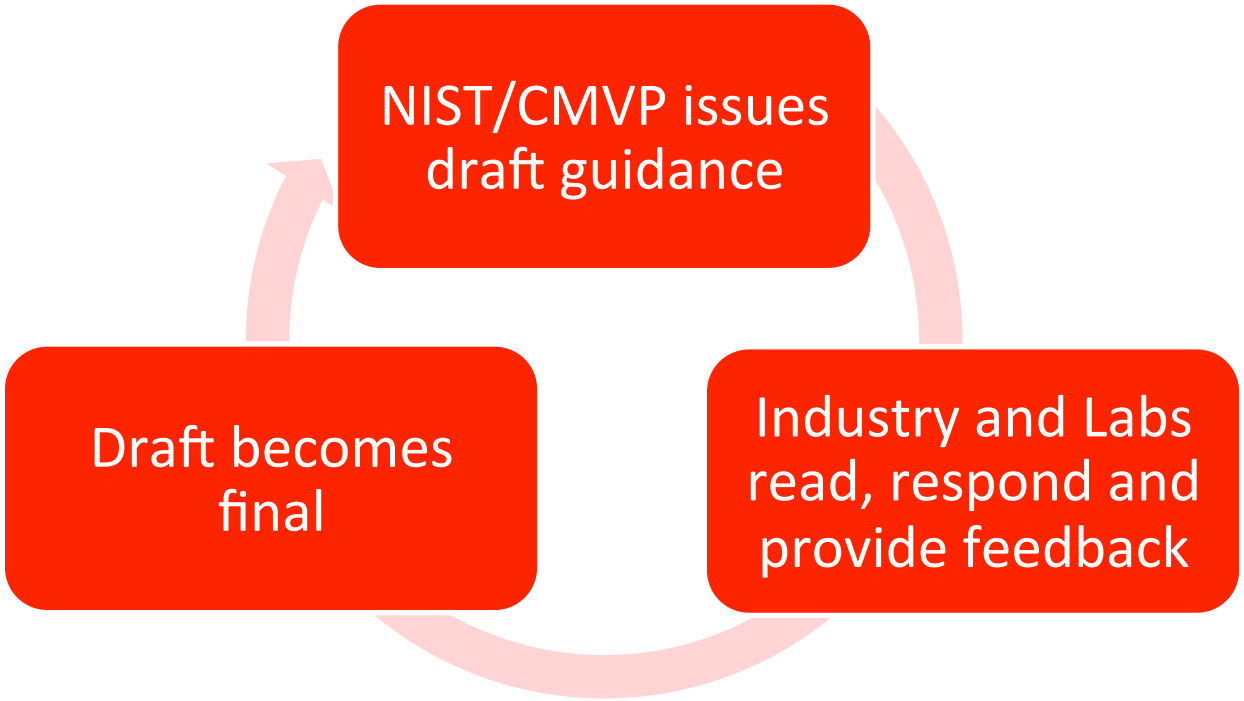
SO WHAT'S THE PROBLEM?

The Shampoo Algorithm

Lather, Rinse, Repeat

CMVP Guidance is it following the Shampoo Algorithm?

Lather/Rinse Repeat



But we never get to a place where we are working together

Vendor Challenges (Example #1)

AES-GCM IV Generation

2007
- NIST SP 800-38D published
- Two IG's issued

2009
- IG A.5 Key/IV Pair Uniqueness Requirements
- External IV generation is not allowed for CMVP (allowed for CAVP)

2015
- IG A.5 Overhauled
- IG effective immediately (no grandfathering)

Vendor Challenges (Example #1)

Oracle's reaction (one product)?

1. When the new IG was issued we immediately dropped all ongoing work to analyze the new IG
2. Oracle wrote up a proposal to mitigate the impact of the new IG while still meeting the spirit of the IG. We sent it on to the CMVP
3. While waiting for a response CMVP came out with another IG
4. On August 7th the new IG became effective immediately. Oracle never heard back on our proposal

Vendor Challenges (Example #2)

Entropy

- In 2012 NIST releases two draft Special Publications (SP 800-90 b and c (for comment))
- Comments are collected but the SP is never finalized
- August 2015, IG 7.15 published, effective immediately (no grandfathering) New requirements for Entropy Assessment for labs
- 3rd party components provide certain functionality (for example to improve performance or provide a source of entropy).
- Most vendors have no ability to test or assess the entropy provided

Vendor Challenges (Example #2 cont.)

Oracle's reaction (An Oracle product)

1. Oracle product gets entropy from a 3rd party
2. The status of the project at the time of release of IG was "Under Review"
3. Oracle has no ability to provide detailed design information as the 3rd party is unwilling to share with Oracle
4. Oracle also volunteered to the CMVP available information on entropy that was accepted by CMVP for previous validations
5. Oracle asked for and received a waiver*

**For the next project we may not get a waiver. With better transition planning CMVP won't be getting all these requests for waivers*

Recommendations

<Or how to get out of the Shampoo Algorithm>

Recommendations

(or How to get out of the shower)

- Form a Technical Community (CMUF working with CMVP)!
  - Take a page from NIAP or the CCRA and work together to solve problems
  - Take advantage of the vast resources of industry
  - Create one for IG
  - One for FIPS 140-4 etc
  - Instead of throwing IG's over the wall, work together to come up with consensus
- Timing
  - When IG's are released, give industry time to react!
  - Every reactive response to IG is less time for industry to build product and fix bugs

Recommendations (and while were on the topic)

Collaborate

- It's high time that NIAP and NIST go back to being a partnership (still too much overlap-- see Entropy)
- Negotiate with other crypto schemes (Brazil anyone) to see if any mutual recognition can be negotiated
- NIST: Lets add a "FIPS Inside"List (maybe voluntary?)

Questions?
Shampoo Advice?

Josh Brickman

joshua.brickman@oracle.com

781-442-0451

Glenn Brunette

glenn.brunette@oracle.com

267-792-5224

Integrated Cloud

Applications & Platform Services


ORACLE®