FIPS and CC Certification

Tales from the Dev side

May 17, 2017

My background and experience

- 14 years as product/project manager responsible for all of Fortinet's FIPS and Common Criteria certification projects
- No experience with FIPS or CC prior to joining Fortinet
- Previous background in product management and IT
- On average, a team of one or less
- 66 completed FIPS certificates, 8 EAL4, 5 EAL2, 4 NDPP

Agenda

- What is the job?
- The outsourcing dilemma
- Creating documentation
- Insulating your internal teams
- Understanding your customers
- Pre-testing and gap analysis

What is the job?

- Communicating with the labs
  - » Delivering documentation
  - » Q&A
  - » Understanding requirements
  - » Explaining implementation
- Communicating internally
  - » Explaining and translating requirements
  - » Getting information to create documentation
  - » Getting the product changes you need

- Everything is just a problem that needs to be solved

Setting the scene…

…Your company

Validators!

Developers!

You’re this guy…

The outsourcing dilemma

Question: Outsource or do it yourself?

Answer: Doing it yourself is possible, not has hard as you think and MUCH cheaper

- The CC Security Target is the only documentation Fortinet outsources
- As an example, the FortiOS EAL4 design doc set (HLD/LLD) is 100 pages total and has been accepted by two different country schemes
- The initial time investment may be steep, but the payoff is worth it

CAVS test vectors were applied (where/by whom):

- ☐ Test vectors applied to IUT by the CST Lab at the CST Lab
- ☐ Test vectors applied to IUT by the CST Lab offsite (location other than vendor or CSTL site)
- ☐ Test vectors applied to IUT by the CST Lab at vendor facility
- ☐ Test vectors applied to IUT by the vendor at vendor facility and directly observed by the CST Lab
- ☒ Test vectors applied to IUT by the vendor at vendor facility and unobserved by the CST Lab. (Vendor's signature required affirming the Algorithm Testing was performed on the above IUT on the specified version(s) and referenced OE's.)

Additional testing Details. Check Yes and provide required information. No, or leave blank if don't know

Was testing performed via simulation?

☐ Yes, enter simulator used: ☒ No

Test harness was used and was constructed by the CST Lab	☐ Yes	☒ No
Test harness was used and was constructed by the vendor	☒ Yes	☐ No
Test harness was used and was constructed by other	☐ Yes	☒ No
CST Lab reviewed the test harness if it was developed by vendor or other	☐ Yes	☒ No

Who puts the output from the IUT into the format required by the CAVS values?

The CST Lab	☐ Yes	☒ No	
The Vendor	☒ Yes	☐ No	
Some Other Lab	☐ Yes, Specify		☒ No

Creating documentation

- Focus on addressing the FIPS or CC specific issue or requirement
- Write the document for the specific audience – i.e. a FIPS validator, a CC evaluator or your internal development teams
- Don’t create documentation for multiple audiences
  - For example, don’t try to create a document useful to the CC evaluation lab and your internal development team
  - You can’t keep both happy using the same language
  - You will lose your shirt when one set of readers starts pulling on threads intended for the other audience
- Create a workable template and reuse, recycle, repurpose

When does outsourcing make sense?

- The document format is so arcane or complex that it doesn't make sense to learn all the rules – for me that defines the Security Target…
- When you have no idea what goes into the document and you can't find public examples – e.g. the old EAL Security Policy Model
- You need external expertise to jumpstart your internal program

Insulating your internal teams

- Keep your internal teams insulated from the labs, validators and evaluators
- Your main goals are to:
  1. Translate requirements in one direction and answers in the other direction
  2. Make the certification problem go away
  3. Get the certificate
- If you outsource, the external consultants will likely have to talk directly to your internal teams – in my experience this rarely goes well and violates Goal #2

Understand your customers

- FIPS and CC customers sit on a spectrum of compliance
  - » Strict – they get audited for compliance against the SP or ST
  - » Loose – FIPS and CC are checkbox items for purchasing

- Most customers sit somewhere in the middle
- Most customers do not understand the details of the FIPS or CC standards, even if they are on the strict end of the spectrum
- Where the majority of your customers sit can affect how you implement FIPS/CC requirements and how you certify your products

Regional issues

- FIPS and CC certification can be just the start:
  - USA – FedRAMP, UCAPL, STIGs, JITC
  - UK – CPA
  - Australia – ACE
- Many countries add their own flavour (or flavor) on top of CC or both FIPS and CC
- Who owns these issues within your company?
- Are there regional benefits for where to do your projects? i.e. what country scheme should you use (or not use)

Pre-testing and gap analysis testing

- Pre-testing for FIPS and a gap analysis for CC
- Get things sorted before you start your official test cycle
- Worth every penny, but a learning process for both the labs and the vendor
- For a first time product, take the estimate from the lab and double it for your consulting PO…
- There are now some automated testing tools out there – try them out and see what they can do for you
- The problem with NDcPP testing (as an example) is not the big ticket items, it's the obscure little ones that will kill your schedule

Odd and ends

- Entropy! What is your solution? Do you have access to the raw entropy output?
- What do your customers expect to see certified? FIPS validated crypto may not be sufficient if your customer wants your solution certified
- Customers buying appliances almost always want FIPS 140-2 level 2, but 99% will never install a tamper seal
- Assume your projects will go badly and then be mildly surprised if they don’t


FORTINET®