From: (b) (6)
To: Alperin-Sheriff, Jacob (Fed); Perlner, Ray A. (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed)
Subject: Re: FAQ update
Date: Sunday, October 23, 2016 8:45:46 AM

That's actually a good idea. Do we indicate that the submitters should specify compiler/options/flags? I feel like we did. Instead of specifying and exact compiler and option set, perhaps it is better for us to require that simply some common compiler and options are used without demanding a single option. Then the submitters can be responsible for these issues, but free to do anything that we can easily deal with. I'm curious what Larry thinks.

Cheers,
Daniel

Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date:10/21/2016 12:02 PM (GMT-08:00)
To: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, Daniel Smith (b) (6), "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>
Cc:
Subject: Re: FAQ update

I assume we're going to be compiling and building it on our end for testing purposes, if for no other reason than to avoid any catastrophes of submissions containing malware/viruses/etc.

Are we specifying a compiler too? I remember a discussion about how compiler "optimizations" can cause problems for cryptography …

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Friday, October 21, 2016 at 2:26 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, Daniel Smith (b) (6), "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Alperin-Sheriff, Jacob M. (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: RE: FAQ update

I broke up the material previously in section 4.A.6 among 4 questions added to the Q&A. We may need some additional work on formatting, but. Please let me know if this approach seems good.
Thanks,
Ray

From: Moody, Dustin (Fed)
Sent: Thursday, October 20, 2016 8:10 AM
To: Daniel Smith (b) (6); Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Alperin-Sheriff, Jacob (Fed)

<jacob.alperin-sheriff@nist.gov>
Subject: Re: FAQ update

Daniel added a FAQ on the differences with a competition. Reading NISTIR 7977, we certainly share a lot of commonalities with the process described for competitions. I think it's good that we explain what's different.

I've added some revisions/comments. Let me know what you think.

From: Daniel Smith (b) (6)
Sent: Wednesday, October 19, 2016 10:45:18 AM
To: Moody, Dustin (Fed)
Subject: FAQ update

Hi, Dustin,

Here is a draft of a FAQ on the IP issues. This is a contentious point, and we'll probably want to talk about and revise this.

Cheers,

Daniel