From: David A. Cooper
To: Regenscheid, Andrew R. (Fed)
Cc: Chen, Lily (Fed); Moody, Dustin (Fed)
Subject: Re: Draft presentation slides
Date: Thursday, February 28, 2019 4:48:13 PM

Hi Andy,

We first started pushing a move from SHA-1 to SHA-2 in 2003. But, 10 years later, even after NIST had declared use of SHA-1 for digital signatures to be no longer approved, DoD continued to use SHA-1. They said that they were going to just keep using SHA-1, despite what we said, since they didn't think the threat was real. Even two years ago after an actual collision was announced, we had people arguing that this didn't yet demonstrate a real need to move away from SHA-1.

Given what happened with single DES and SHA-1, I think we can already predict that any transition to post-quantum algorithms will take longer than whatever time frame we set, no matter how much time we give agencies to transition. It just seems that things like the National Academies report could by some as an excuse to do what they already want (plan) to do --- nothing. Why spend time on something that might never be a real threat (or at least won't be for decades)? We may not really want them to do anything now, but at some point (in a few years?) we certainly want them to be seeking out (demanding) products that provide post-quantum security.

Dave

On 2/28/19 3:36 PM, Regenscheid, Andrew (Fed) wrote:

> David,
>
> I'm not sure what you mean by "but I don't want to give agencies an excuse to do nothing either."
>
> The FPKI community should be aware of the issues. They should understand the impact of quantum computers on current public key algorithms, and have some awareness of the possible candidates for quantum-resistant signatures. I thought your slides did a pretty good job that.
>
> I think we want to be careful when talking about stateful hash-based signatures. While we might be fairly confident in their security right now, I don't think we want to (possibly inadvertently) suggest that they should be seriously looking to use them in the near-term. They seem like the method of last resort, and I don't think we're there yet- particularly for something that doesn't really require forward security.
>
> The right thing for FPKI to do is to think about where its being used across government, and consider what the impact of the various candidates would be on their architecture, components, and processes. I imagine that's what you had in mind by identifying the public key and signature sizes of the candidates.

-Andy