From: Chen, Lily (Fed)
To: McKay, Kerry A. (Fed)
Subject: Re: idea for next year"s SURF students
Date: Thursday, June 22, 2017 2:01:58 PM

Hi, Kerry:

I think you list what I can think about. I will be happy to do the first one.

The only thing we might need to do before hand is to coordinate about the content. For example, in asymmetric key based crypto, you may talk about hard problems like factorization, discrete log. When Dustin or Ray talk about post-quantum crypto, he will review RSA and DH and may start from some other hard problems. We also talk about NIST standards like 56A/B and also FIPS 186. Then when whoever talks about TLS or IKE or IPsec, they will use asymmetric key crypto. So the students can make connections.

Lily

From: "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
Date: Thursday, June 22, 2017 at 1:27 PM
To: Lily Chen <lily.chen@nist.gov>
Subject: Re: idea for next year's SURF students

Lily,

Here is an initial proposal. Anything that I haven't listed possible speakers for is something that I'd be willing to do. I could do the first one too, but I think it would be better from a manager. Please let me know if there are additional topics that you think the students should be exposed to, or ones that I've listed that you think are too heavy for a quick intro.

-Kerry

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Thursday, June 22, 2017 at 8:19 AM
To: "McKay, Kerry A. (Fed)" <kerry.mckay@nist.gov>
Subject: RE: idea for next year's SURF students

Hi, Kerry:

I think this is a great idea! I will be happy to be one of the instructors to give tutorial. In order to avoid conflicting from other meetings and activities, we can make the seminar earlier like before 10:00. We will make a seminar schedule for next summer.

Lily

From: McKay, Kerry A. (Fed)
Sent: Thursday, June 22, 2017 8:06 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: idea for next year's SURF students

Lily,

One of the "problems" we have with SURF students in our group is that they have little to no exposure to cryptography. This doesn't prevent them from doing their projects (which is why I put "problems" in quotes) because we design the projects such that understanding of crypto isn't a prerequisite, but it also means that the students don't really get that great of an idea of what it is we do and what we're all about. I've been doing weekly crypto bootcamps with Nicole to give her an idea of the different areas we work in. It is a bit like drinking from a firehose because it's a lot of info in a short amount of time, but I think it is helpful to at least expose her to concepts which can explore more if she found them interesting.

I was thinking that it might be cool to have several people in our group put together a weekly series for all the crypto SURF students next summer, and have it open to any SURF student, particularly those in CSD/ACD. I could take the lead and cover most topics (I've already got slides from this year), but I have knowledge gaps. I would say the biggest one is post-quantum crypto, so it would be nice to have someone form the PQC team make a 1-hour presentation (or less) that is accessible to students. I'd also like to have people give short intros (maybe 20-30 mins each) to applications, such as blockchain, security protocols, identity management, etc.

Do you think this is something we could/should pursue? It might help us get some more interest from the students, and then maybe get some of the students to consider joining us under the pathways program as they continue their educations.

-Kerry