From: Vadim Olun
To: Regenscheid, Andrew R. (Fed)
Cc: Black, Paul E. (Fed)
Subject: Re: Hold for NIST/PCI-SSC Teleconference
Date: Thursday, June 30, 2016 12:42:38 PM

Andy,

I will be glad to join the call.

Friday, July 15 works for me. Paul will not be able to attend.

Thanks,
Vadim

On 6/29/2016 1:07 PM, Regenscheid, Andrew (Fed) wrote:

> Microsoft Outlook Web Access: https://outlook.office365.com/owa/nistgov.onmicrosoft.com/?ItemID=AAMkAGU0NjE1MTE5LTk5N2YtNDJhZS04NjQ1LTJkOGMwNmZmYjkyNwBGAAAAADfJjt855RtT7li0nQNRlUWBwDXoEI%2BXbk%2FQL5ulBJpMMSTAAdOXKVOAAAXwxcEWp8vToqID07g1%2B3yAALDwVy4AAA%3D&exvsurl=1&viewModel=ICalendarItemDetailsViewModelFactory
>
> To receive meeting invitations as .iCalendar attachments instead of Outlook Web App links, go to https://outlook.office365.com/owa/nistgov.onmicrosoft.com/?path=/options/popandimap and select Send meeting invitations in iCalendar format.
>
> (copying email sent on 6/29/16)
>
> All,
>
> Most of you at one time or another have participated in a meeting/teleconference with the PCI Security Standards Council. We usually talk with them a couple times each year about on-going projects at NIST relevant to their mission.
>
> Ralph Poore contacted me to request another teleconference. Ralph would be joined by Troy Leach, CTO of the PCI-SSC. We're tentatively planning/hoping that Friday, July 15th from 2:00-4:30PM ET would work for a time. A backup date/time would be Monday, July 18th from 2:00-4:30.
>
> They would like to talk about the following topics:
> · Standards/best practices for software security
> · Current cryptographic standards and sun-setting
> · Cryptography for Post-quantum computing
> · End-user authentication (e.g., multi-factor, biometrics, latest thinking on passwords, and federated identity)
> · Mobile security
> · Tokenization, dynamic data, and other approaches to devaluing data
>
> I'd appreciate it if you could join the call to cover your topic or topics. We could set up a specific time on the agenda so you wouldn't need to stick around for the full 2.5 hours.
>
> **Vadim, Paul Black**- thanks for talking to them about SAMATE at our last meeting with them. They have the materials you provided following that meeting, and I asked them to take another look at that material in order to find out if there are specific topics/issues they'd like to address. If you're able to join, I'd appreciate it if you gave a quick update on current activities, and then let the discussion dive into more details as needed.
>
> **Paul Grassi**, given their interest in authentication, it would be great if you could give a quick update on SP 800-63-3. If you can't do it, is there someone that can cover for you? I know just enough to be dangerous there, but it would nice to have someone that has been more active in the development.
>
> **Apostol**, I'm including you because one of the main topics they are interested in is the security of software-based crypto modules. This has been a major interest area for them for quite a while. I tend to think that the main advantage you get with a HW module is that it (hopefully) provides its own isolated environment for crypto operations and services. There's no particular reason, in my mind, you couldn't achieve similar properties with a software module, but then it comes down to: 1) the architecture of the operating environment, and 2) how to actually assess the security. If you have thoughts on this, it would be great to have you around.
>
> **Josh**, I'm including you because of your mobile security work, both at the NCCoE and with the report. They've separately been talking to people at the NCCoE. If you have time, it would be great if you could provide a brief update on the building block, and then participate in a more open discussion with them about security and trends with mobile devices. I'd recommend a separate follow-on discussion if they're interested in more details on the building block.
>
> Please let me know if the primary date/time works for you: Friday, July 15th from 2:00-4:30. If not, let me know if the same time on Monday (the 18th) would work better.
>
> Thanks,
> Andy