

2019-Nov-6

CTAB Wed. Nov. 6, 2019

Attending

- Mary Catherine Martinez, InnoSoft (chair)
- David Bantz, University of Alaska (vice chair)
- Rachana Ananthakrishnan, Globus, University of Chicago
- Tom Barton, University Chicago and Internet2
- Brad Christ, Eastern Washington University
- Jon Miner, University of Wisc - Madison
- John Pfeifer, University of Maryland
- Chris Whalen, Research Data and Communication Technologies
- Ann West, Internet2
- Albert Wu, Internet2
- Emily Eisbruch, Internet2

Regrets

- Brett Bieber, University of Nebraska
- Eric Goodman, UCOP - TAC Representative to CTAB
- Chris Hable, University of Michigan
- John Hover, Brookhaven National Lab
- Adam Lewenberg, Stanford

Action Items from this call

- [AI] (Rachana) talk with her team to get more perspectives about improving the TLS
- [AI] (John) talk with his team to get input about improving TLS
- [AI] Albert consult with NickR on engineering or other practical concerns that would arise if InCommon does the testing around secure endpoints
- [AI] Albert flesh out the BE 2020 doc with more on SIRTfI, endpoints, and other matters
- [AI] (MC) email InCommon Steering chair TedH and cc Brad Christ with the slate of nominees for CTAB 2020

Discussion

Baseline Expectations (BE) 2020

- OWASP cheat sheets - how do we apply them to BE requirements (TomB)
 - https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
 - https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html
 - TomB: for consumer electronics, not subject to those restrictions. People can travel with their cellphones.
 - Regarding this BE statement:
 - "All SP service endpoints must be secured with current, supported, unbroken transport layer encryption"
 - Need to have appropriately encrypted endpoints
 - The 2 OWASP cheat sheets demonstrate there are many details and choices
 - CTAB must decide which are satisfactory choices
 - TomB shared scanning mechanism used at U. Chicago
 - DavidB: suggests most restrictive approach
 - Jon: if a platform (eg, Windows) can't support the most restrictive approach, is that outside of baseline?
 - We must do the research to tell participants what to do on an open SSL platform and what to do on Windows
 - Hard to figure out the best approach on containers
 - SSL Labs has an API, can be used to measure, provides a grade and provides feedback
 - Goal now is to support TLS 1.2 but eventually the goal posts will change
 - TLS 1.1 will soon mean a grade of B instead of A
 - If we apply the SSL Labs standard to a commercial SP (such as Box) that is crucial for campuses, it will be a problem if Box gets "kicked out"
 - Suggestion that MC, Rachana, and others try this SSL Labs test
 - AI (Rachana) talk with her team to get more perspectives about improving the TLS
 - AI (John) talk with his team to get input about improving TLS
 - Use API to automate the SSL Labs testing?
 - What would be the next steps and consequences and timeframe for fixing if an organization does not pass
 - It would be convenient to reply on SSL testing and grade for Baseline Expectations
 - There would be cycle time for remediation if grade falls below an A
 - Issues around International browsers ?
 - Is the suggestion that participants test themselves and submit their results?
 - Or would InCommon do the testing?
 - [AI] Albert consult with NickR on engineering or other practical concerns that would arise if InCommon does the testing around secure endpoints
 - Important to provide guidance on how to disable TLS 1.1
 - DavidB found lack of documentation for Windows on this

- CTAB would need to provide guidance
 - Find out the top platforms being used, Tomcat, JEDI,
 - There will be some support burden; "I want to do this but I don't know how"
 - CTAB needs to figure out what is reasonable, be careful in setting a high bar that is hard to implement
 - For those who do not meet this, there would be a process, including dispute resolution, and could lead to extensions being given and/or an exception being mad
 - Steering is the final judge in cases where an entity might be removed from metadata
 - The community will have time to adhere to any new baseline requirements
- **Sirtfi** - what do we need to say to clarify? (David)
 - Do we need to go beyond "by checking the box you agree to support the SIRTFI framework"
 - At U Alaska, they don't adopt SIRTFI as practice, and that would be OK under the proposed Baseline Expectations. They can respond to a request for SIRTFI and that is what is required.
 - Al Albert flesh out the BE 2020 doc with more on SIRTFI, endpoints, and other matters
- **IAM Online**, Wed. Dec 4, 2019, 2PM Eastern
 - Dean suggested CTAB participate in IAM Online webinar on Dec. 4 to preview what's happening at TechEx 2019
 - DavidB volunteered, Albert will help. JonM may be able to attend as well (if we want more)
- **Nominations** for CTAB membership starting in 2020
 - MC worked with David and Brett to reach out to nominees
 - They spoke to 5 of the 6 nominees for CTAB.
 - Did not contact one CTAB nominee who had chosen another governance group as 1st choice
 - All seemed motivated to be part of CTAB and were good fits for CTAB.
 - Good variety of individuals.
 - We may need to change our CTAB call time to accommodate European nominees
 - Candidates asked about the next step
 - Potentially CTAB could provide a tentative yes, contingent on InCommon Steering approval.
 - Steering may look at representation to be sure a variety of key stakeholders are represented
 - Once CTAB has the slate ready, MC (CTAB Chair) would email the InCommon Steering Chair (Ted Hanss)
 - InCommon Steering next meeting is Dec 2
 - We may request that Steering do an online vote prior to then
 - Al (MC) email Ted and cc Brad Christ with the slate of nominees for CTAB 2020
- Planning for TechEx - InCommon and CTAB update - <https://docs.google.com/presentation/d/1bqaBpgZzyVTWEWcQCvFYGxWx6ZZOvLBhb6PPvgwFyHk/edit>
 - TechEx - Open CTAB Meeting: Discussion of Baseline 2020
 - <https://meetings.internet2.edu/2019-technology-exchange/detail/10005609/>
 - Review community consensus process
 - Outline BE changes
 - Discussion
 - Capture input from attendees
 - Gain greater clarity on implementation items (what to include; what not to include)
- Proposed Agenda
 - Review community consensus **process**
 - Outline BE changes
 - Discussion
 - starting draft for TechEx based on last year's slides
- Likely we won't be ready with a wiki about proposed baseline expectations
 - Goals:
 - Capture input from attendees
 - Gain greater clarity on implementation items (what to include; what not to include)
- BE 2020 Prep
 - The main Doc
 - Clarification wiki pages
 - Email list for community consensus
 - Draft announcement - BE 2020 entering community consensus
 - others?

Next CTAB Call: Wed. Nov. 20, 2019