2021-April-20 CTAB Public Minutes - Office Hours Call

Tuesday, April 20, 2021

Baseline Expectations office hours

55 participants

Resources

Baseline Expectations Overview

- https://www.incommon.org/federation/baseline/

Baseline Expectations:

- https://spaces.at.internet2.edu/display/TI/TI.34.3?preview=/178160751/178160768/TI.34.3-BaselineExpectations-v2-2020-11.pdf

Implementation and Guidance Guide:

- https://spaces.at.internet2.edu/display/TI/TI.137.1?preview=/178160757/178160759/TI.137.1-BaselineExpectations2ImplementationGuide-2020-11.pdf
- Wiki showing community progress: Baseline Expectations for Trust in Federation

DavidB provided an overview of Baseline Expectations

Overview

- Baseline Expectations (BE) are specific expectations of participants in the Federation
- Requirements on how federation participants (IDPs, SPs and Operator) operate
- So that the rest federation has an elevated level of trust
- First round of BE focused on metadata being accurate and complete, including contact info
- Second round of BE focuses largely on security,
    - SIRTFI **https://refeds.org/sirtfi**
    - TLS Endpoint protection
    - Error URL

Discussion

Question : When will BEv2 verification start?

Answer: BEv2 starts July 19, so enforcement begins then.

- After July 19, 2021, if you are not up to date
    - you will not be able to publish new metadata,
    - You will get reminders
- Later in 2021 there may be further action for orgs that are out of compliance
- Currently there are already some warnings in the Federation Manager around SIRTFI and Error URL. No warning yet around TLS.
- Organizations are invited to check TLS score separately https://www.ssllabs.com/ssltest/
- InCommon federation can't test all entities all the time.
- InCommon federation SSL testing will occur on a periodic basis
- What's important is that you keep current with latest security threats and do mitigation
- Note that there are baseline expectations for IDPs, SPs and Federation Operator (InCommon)

Question: How is it determined if we comply with SIRTFI? https://refeds.org/sirtfi

- SIRTFI is new to us

Answer:

- It's a self attestation
- If you are not certain if it's OK to check a box for SIRTFI, discuss with your security team
- It's intended to be a low bar
- SIRTFI should not required big changes for organizations practicing security
- SIRTFI does not review your compliance, it's all based on self attestation
- Tom Barton is a good contact person for SIRTFI questions

Comment: our organization (an SP) reviewed the BEv2 requirements and determined we are in compliance.

Question: Is there a need to publish compliance to other members,
as was done for the InCommon Federation POP (Participant Operating Practices) prior to Baseline Expectations?

Answer: There is no need to publish a compliance statement.

- If you attest to SIRTFI, or other element of Baseline and someone questions whether you in fact meet the requirements, the questioning party can bring their concern to the InCommon federation. Here is a process to resolve such concerns. https://www.incommon.org/federation/dispute-resolution/

Timing for BEv2:

- July 19, 2021 is a key date for baseline expectations
- New NIH requirements for collaboration are scheduled for Sept 2021.
- https://spaces.at.internet2.edu/display/federation/get-nih-ready
  These NIH requirements include baseline expectations.
- Baseline Expectations 2 and NIH requirements are parallel.
- eRA is the main part of NIH that is setting the Sept 2021 NIH deadline
- https://era.nih.gov/
- Those signing in to eRA after Sept 2021 may need to obtain a login.gov credential if not meeting the NIH requirements
- Pubmed is also going through a transition.
  - But PubMed will not require MFA, the requirements are less strictQuestion re TLS Endpoint requirement

TLS Endpoint question

- once you review results and find some are not in compliance
- if there are local considerations that make it hard to turn off TLS 1.0 and TLS 1.1, will it be possible to “buy time”?
- How strict will be the enforcement?
- The BE requirement is stated to be graded as an SSL Labs A, and what SSL Labs requires for an A may change

Answer: there can be grace periods depending on circumstances

- SSL labs grading can help you know where to spend effort
- There are possible mediations if you can’t achieve TLS 1.2 in all situations
- Intent is not to pull the rug out, not to kick people out of the InCommon federation, we want to make the federation more secure
- The InCommon Federation has a procedure for security issues
- To support incident response at a high level
- 90 days remediation period is specified in the BE implementation guide .

Comment: Concerned about SHALL in upper case in implementation guide.

Reply: Your colleagues and peers will look at mitigation proposals

ChrisB and ScottCa : Or campus deals with many service providers who need to get metadata from our IDP, some of those SPs are not members of the Federation. Some are using an older version of SSL protocol for consuming metadata. We can’t turn of older SSL 1.0 on our IDP. We can never get better than a B grade on SSL labs grading

Andy :

- Using CAS, has backchannel connection
- legacy systems that can’t do TLS 1.2, so we spun off an instance of our IDP that we left with TLS 1.0 and TLS 1.1
- enabled and firewalled it off,
- so only those servers could contact it, and on those they servers poisoned local DNS to resolve to TLS 1 instance of our IDP.
- Felt that was an adequate mitigation measure.
- Other federation members are not exposed to that IDP

ChrisB : An option that does not require us to contact all the SP operators and get them to change something would be welcome.

Andy: there may some intermediary approach

Les:

- Concern with respect to SIRTFI acceptable use policy,
- Campus IDP Is for entire constituency,
- faculty and students are covered w AUP,
  but also alumni and others use the campus SSO for various services, for those there is no AUP.
- For folks accessing educational research sites, we are covered by the practices.
- But what about other scenarios?

TomB: The precise extent to which any of the specifications are implemented is a **risk management decision of an organization**. Must be made with the priorities of the organization in mind. It’s not just a strict compliance framework.

Albert: Saw on a thread: Case where a commercial login company is putting out login pages, that look like campus login pages, and they use justification that the user has given consent.

Comment: it’s a phishing scheme

Note difference between Baseline Expectations and Guidance doc

1. Normative text of Baseline Expectations, short statements

2. Guidance doc is meant to be implementation guide, to provide clarity

- BE can be a useful tool to drive positive behavior change on campus
- Comment: Need to be careful so people on campus won't see InCommon as "bad guy" making us do stuff we don't want to do
- Comment : Implementation guide provides clarity, issue is that have old legacy stuff that is an issue.

TLS Endpoint issue and possible approach

- It's challenging to figure out which are those entities that can't reach TLS 1.2 and handle those situations
- How do we as a community balance between practical, implementable solutions and the need to be more secure. Downgrade? attacks do occur and could make everything more vulnerable
- ScottC: will look at the telemetry approach to detect .
- Java may provide a way to do logging
- Brett suggests Modify Apache HTTP to get log in info
- An easy way to detect clients using weak SSL/TLS settings is to log the protocol and cipher used by them:
    - - SSL_PROTOCOL in Apache (https://httpd.apache.org/docs/current/mod/mod_ssl.html)
    - - CRYPT_PROTOCOL in IIS (https://www.microsoft.com/security/blog/2017/09/07/new-iis-functionality-to-help-identify-weak-tls-usage/)
- So you know the clients and identify who you need to talk to
- Interest in knowing how to do in Jetty directly for those not using Apache
- Good to share such examples

Comment: our company has many parts. Verifying that the BE only applies to those parts of our company that interacts with InCommon Participants.

Answer: Yes, that's correct

Comment: thanks to the whole InCommon team for working towards improved security

SSL Labs Testing

- Request to post link to a site that is not getting an A in SSL Labs testing.
- Albert shared link https://www.ssllabs.com/ssltest/
- Question: Is it possible to get a low SSL score, fix one problem, and still have a low score?
- Answer Yes, could happen

Thanks to all for participating