SECCOM CII Badging Focus Topic
Crypto certificate verification

SECCOM

2019/6/24

Why are we doing this?

Thank you to all of the projects that ***have*** already answered this question

Unfortunately, only half of the projects have answered this question.

Bottom line: Our job is to get ONAP projects to verify and/or improve the security of their code. Getting the silver star or gold star from the CII badge is truly secondary.

This is the first of a set of “focused CII issues”

The CII question

The software produced by the project MUST, if it supports TLS, perform TLS certificate verification by default when using TLS, including on subresources. If the software does not use TLS, select 'not applicable' (N/A).

[Show details] Note that incorrect TLS certificate verification is a common mistake. For more information, see "The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software" by Martin Georgiev et al. and "Do you trust this application?" by Michael Catanzaro.

http://crypto.stanford.edu/~dabo/pubs/abstracts/ssl-client-bugs.html
https://blogs.gnome.org/mcatanzaro/2016/03/12/do-you-trust-this-application/

Intro

- This question is about the use of TLS (and SSL) for
  - Machine to machine connections from the application to remote servers, such as
    - REST APIs, database connections, other APIs.
  - When TLS or SSL is used by a remote server, the server will use a "Server Certificate" issued by a Certificate Authority.
- This question wants us to make sure that our applications actually check the server certificates against appropriate certificate chains.
- Some languages make it easy to ignore the Server Certificates
  - E.g., curl --insecure / curl -k
- If server certificates are ignored, it enables man-in-the-middle attacks.

PTL Effort

Make sure that you have the right trust chain for whatever language you're dealing with to reach the API servers you're going to.

Understand how your languages enable or disable verifying the trust chain.

The PTL should check their code base to make sure the programs properly verify the trust chain.

You may delegate the checking of the code.

Where to answer

- Go to https://bestpractices.coreinfrastructure.org
- Click Projects
- Search for your project
- Click Login (at the top)
- Click Edit (at the top)
- Click the button that says [silver]
- Scroll to the bottom, click [v] Security
- Search for “crypto_certificate_verification”
- Fill in your answers
- Click one of the green buttons [Save (and continue)] or [Submit (and exit)]

- This part should take about 5 minutes

How to answer the CII question

For each remote call, answer these questions:

- If your remote API calls support TLS, are you using TLS?
- Do you have the proper certificate chains?
- If you are using TLS, are you verifying the certificate chains?
- Does your onap.readthedocs.io page describe your use of remote APIs? (optional)

If yes to all questions (for all APIs):

- Click (Met)
- In the description, enter the date (e.g., [2019/06/24]), the URL for the readthedocs.io page (if available), and an indication why (Met) is appropriate

How to answer, continued

If there are no APIs that support TLS or SSL:

- Click (N/A)
- In the description, enter the date (e.g., [2019/06/24]) and an indication why N/A was appropriate

If any of the other answers are NO:

- Click (Unmet)
- In the description, enter the date (e.g., [2019/06/24]) and a description where something was not met.
- File JIRA tickets for each issue that needs resolution.

If you have multiple remote APIs with a mixture of answers:

- If any of the APIs would be (Unmet), then use (Unmet) for the overall answer.
- If you have both (Met) and (N/A), then use (Met) for the overall answer.

Future Focus Topics

- Future focus topics will include
  - The use of TLS instead clear text, e.g. HTTPS instead of HTTP
  - The use of TLS v1.2 instead of earlier versions, e.g. TLS v1.1 or SSL
  - How certificates and passwords are stored

Thank you

- That’s all