The OpenSSF Best Practices Badge Program

Date: June 14, 2023

Presented by: Roscoe A. Bartlett (Sandia National Laboratories)

(The slides will be available under “Materials from the Webinar” in the above link.)

Q. Why Gold has lesser requirements when compared to Silver badge level (Slide-9)

A. It does not. Gold has more than Silver and Silver has more than Passing. Each level only adds more practices. For example, Silver adds 44+10+1 additional practices above the Passing level (gold Silver has 87 MUST, 20 SHOULD, and 15 SUGGESTED practices). And Gold additional 21+2 practices above the Silver level (so Gold has 108 MUST, 22 SHOULD, and 15 SUGGESTED practices).

Q. Do most exascale projects provide information on how to contribute?

A. I don’t personally know the answer to that. It would take quite a bit of investigation to answer that question. But if they all provided an entry for their projects on the OpenSSF Best Practices Badge App site, we would know the answer for that 🙂

C. Sharing my experience: SUNDIALS (exa-scale project) does have information on how to contribute.https://github.com/LLNL/sundials

Q. Can you clarify how “Should” differs from “Suggested”?

A. SHOULD is stronger than SUGGESTED. See the exact definitions used by the OpenSSF Best Practices Badge Program in the section “Key words” on the page Criteria Discussion.

Q. (Alfred Tang) Does the openSSF badge program install any software on the registrant’s system for verification purposes? Or does the registrant just have to answer some questions on the web?

A. The full implementation is on the site https://bestpractices.coreinfrastructure.org/en/projects and is accessed through your web browser.

Q. Who decides what is a “best practice”?

A. These practices were curated from the existing open source software development community and are already followed by the best projects. As stated on the Criteria Discussion page, “These criteria are what we believe are widely ‘preferred or considered standard’ in the wider FLOSS community.” Otherwise, you should examine

these practices for yourself and decide for yourself. But note that these practices are considered “standard” in the FLOSS community and projects that don’t follow these practices may be considered less trustworthy.

Q. So does the badge get reset every 18 months?

A. The badge does not reset on any schedule. You may be referring to slide 38 that stated that the Free OpenSSF course takes 18 hours to complete and the certification expires in 2 years.

Q. (Alfred Tang) Are the two books that you mentioned the only good ones on software security?

A. I can’t answer that question. All that I can provide are materials pointed to by the OpenSSF Best Practices Website and the OpenSSF: Concise Guide for Developing More Secure Software.

C. When I was in graduate school, I took two security courses, and they were fabulous. They included hands-on projects, one in which groups were assigned a machine to secure against the other groups; each group was encouraged to hack away to capture the root password of another machine. This type of course is extremely valuable.