CII Badging Program for CLAMP

Xue Gao, Pierre Close, Anael Closson

September 20, 2017

The CII Badging Program

- Core Infrastructure Initiative Website:
  - https://bestpractices.coreinfrastructure.org/
- Evaluate how projects follow best practices using voluntary self-certification
- Three levels: Passing, Silver and Gold
  - LF target level recommendation is Gold
- ONAP Pilot Project: CLAMP
  - https://bestpractices.coreinfrastructure.org/projects/1197

The Questionnaire

- Edition is limited to a subset of users
  - Main editor can nominate other users as editors
- Divided into clear sections
  - For each section, a set of questions is provided, addressing best practices relating to the parent section
- Each question asks if a criterion is
  - Met, unmet, not applicable, or unknown
- Criteria are generally high-level as targeted to best practices, e.g.
  - “The project MUST have one or more mechanisms for discussion”
  - “The project SHOULD provide documentation in English”

The Goals

- Give confidence in the project being delivered
  - By quickly knowing what the project supports
- See what should be improved
  - Self-questioning helps project stakeholders identifying strengths and weaknesses, do’s and don'ts
- Align all projects using the same ratings
  - Makes projects connected together to follow the same practices
- Call for continuous improvement
  - Increase self rating and reach better software quality

To Be Discussed

- Introduce test coverage rules: how many tests should be added for each code changes
- Digital signature: use digital signature in delivered packages (already in the plan?)
- Vulnerability fixing SLA: vulnerabilities should be fixed within 60 days
- Security mechanisms
  - Which cryptographic algorithms to use to encrypt password
  - The security mechanisms within the software produced by the project SHOULD implement perfect forward secrecy for key agreement protocols so a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.
  - If the software produced by the project causes the storing of passwords for authentication of external users, the passwords MUST be stored as iterated hashes with a per-user salt by using a key stretching (iterated) algorithm (e.g., PBKDF2, Bcrypt or Scrypt).
  - The security mechanisms within the software produced by the project MUST generate all cryptographic keys and nonces using a cryptographically secure random number generator, and MUST NOT do so using generators that are cryptographically insecure


ONAP
OPEN NETWORK AUTOMATION PLATFORM