Master-Thesis Description

Certification of Open Source Supply Chains

Many products today contain software. This software in turn may be created from multiple sources, including open source projects. For a product company, it is important, among other things, to understand which open source components are included in its products, including components sourced from third-party vendors. Today, to ensure proper sourcing, the product company has to audit its software suppliers for following best practices of open source governance. With increasing complexity and depth of software supply chains, auditing may become prohibitively expensive. A better option is to require the certification of suppliers to follow best practices of open source governance. No such certification program exists today. This thesis analyses the situation, collects best practices, and proposes (within the scope of a Master thesis) a certification program.

Expected Work Results

- Literature review of best practices of …
  - Open source governance in software product companies
  - Software supply chain management
  - Process certification
- Interviews with people responsible for open source governance (optional)
- Best practices of open source governance for handling suppliers
  - A model of the risks from the use of open source by software suppliers
  - Proactive best practices for handling these risks (certification requirement, auditing)
  - Defensive best practices (due diligence, e.g. code scanning, etc.)
- Proposal for a certification program for open source governance in software product firms
  - Governance best practices and how to assess them
  - Certification level 1 (use and embedding of open source)
  - Certification level 2 (active contribution to open source) (optional)

Thesis Advisor

Prof. Dr. Dirk Riehle

Friedrich-Alexander-Universität Erlangen-Nürnberg

dirk.riehle@fau.de, http://osr.cs.fau.de

2013-04-09, 15:02:12