The Bid by OpenChain to Transform The Supply Chain

Shane Coughlan,[a]

(a) OpenChain Project Director, Linux Foundation.

DOI: 10.5033/ifosslr.v9i1.122

Abstract
OpenChain aims to increase open source compliance in the supply chain. This issue, which many initially dismiss as a legal concern or as low priority, is inherently tied to ensuring that open source is as useful as possible with as little friction as possible. In a nutshell, because open source is about the use of third party code, compliance is the nexus of where equality of access, safety of use and reduction of risk can be found. OpenChain is built to increase trust between organizations to accomplish this.[1]

Keywords
Law; information technology; Free and Open Source Software; Supply Chain; Compliance

Today many companies understand open source and act as major supporters of open source development. However, addressing open source license compliance in a systematic, industry-wide manner has proven to be a somewhat elusive challenge. The global IT market has not yet seen a significant reduction in the number of open source compliance issues discoverable in areas like consumer electronics over the last decade.

The majority of compliance issues originate in the midst of sharing multiple hardware and software components between numerous entities. The global supply chain is long and the participants are simultaneously intertwined and disparate. It is perfectly possible to have companies making hardware, companies making software and companies doing both collaborating around a relatively small component. The results in terms of products are often outstanding but the challenge of keeping track of everything is substantial.

Compliance Is A Process Challenge That Spans Multiple Organizations

Open source presents a specific challenge in the global supply chain. This is not because open source is inherently complex but rather due to the varying degree of exposure and domain knowledge that companies possess. By way of example, a company developing a small component that requires a device driver may have staff entirely unfamiliar with open source. One mistake, one misunderstanding, and one component deployed in dozens of devices can present an issue. Most compliance challenges arise from mistakes. Few, if any, originate with intent.

1 This is an edited version of an article originally appeared on OpenSource.com

Ultimately solving open source compliance challenges involves solving open source compliance in the supply chain. This is no small task: there are thousands of companies across dozens of national borders using numerous languages in play. The solution lies beyond the realm of inter-company negotiation. To address open source compliance challenges the global supply chain must align behind certain shared approaches.

Because No Single Company Makes A Finished Device, No Single Company Can Solve Compliance Challenges

Awareness of this fact and the provision of a practical solution are two different matters. It takes time for ideas and suggested approaches to percolate and mature. It took input from lawyers and managers and developers and political scientists. It took, in short, a while for the ingenuity of the human community to bounce ideas back and forth until a simple, clear approach could be found.

The Best Solutions Are Often The Simplest, With The Lowest Barriers To Entry

The OpenChain Project formally launched in October 2016 and is hosted by The Linux Foundation. It originated in discussions that occurred three years earlier and continued at an increasing pace until a formal project was born. The basic idea was simple: identify key recommended processes for effective open source management. The goal was equally clear: reduce bottlenecks and risk when using third-party code to make open source license compliance simple and consistent across the supply chain. The key intention was to pull things together in a manner that balanced comprehensiveness, broad applicability, and real-world usability.

OpenChain Is Intended To Make Open Source License Compliance More Predictable, Understandable And Efficient For The Software Supply Chain

The OpenChain Project is trying to build and disseminate an industry standard for license compliance. It is designed to be the foundation for open source compliance in the supply chain. Engagement and adoption is simple, free and supported by a vibrant community backed by leading multinationals across multiple sectors.

There are three interconnected parts to the OpenChain Project. A Specification that defines the core requirements of a quality compliance program. A Conformance method that helps organizations display adherence to these requirements. A Curriculum to provide basic open source processes and best practices.

A Simple Specification That Explains The Key Requirements Of A Quality Compliance Program

The core of the OpenChain Project is the Specification. This identifies a series of processes designed to help organizations of any size to address open source compliance issues effectively. The main goal of organizations using the OpenChain Specification is to become conformant. This means that their organization must meet the requirements of a certain version of the OpenChain Specification. A conformant organization can advertise this fact on their website and promotional material, helping to ensure that potential suppliers and customers understand and can trust their approach to open source compliance.

A Clear And Free Way To Check Conformance With The Specification

OpenChain Conformance can be checked via a free online self-certification questionnaire provided by the OpenChain Project. This is the quickest, easiest and most effective way to check and confirm

adherence to the OpenChain Specification. There is also a manual conformance document available for organizations whose process requires a paper review or disallows web-based submissions. Both the online and the manual conformance can be completed at a pace decided by the conforming organization and both methods remain private until a submission is completed.

A Curriculum To Support Conformance And With Broader Questions Of Training And Processes

The OpenChain Curriculum helps organizations meet certain aspects of the OpenChain Specification. It provides a generic, refined and clear example of an open source compliance training program that can either be used directly or incorporated into existing training programs. The knowledge it contains can also be applied to adjusting or adopting various processes for managing open source inside an organization. The OpenChain Curriculum is available with very few restrictions to ensure organizations can use it in as many ways as possible. To accomplish this it is licensed as Creative Commons – Zero[2] (CC-0), effectively public domain, so remixing or sharing it freely for any purpose is possible.

Community and Support

The OpenChain Project provides what we believe to be a compelling approach to making open source compliance more consistent and more effective across multiple market segments. However, good ideas need implementation, and in the context of open source this inevitably hinges on the creation of a supporting community. The OpenChain Project at the time of writing has twelve Platinum Members that support its development and adoption: Adobe, ARM, Cisco, GitHub, Harman, Hitachi, HPE, Qualcomm, Siemens, Toyota, Western Digital and Wind River. It also has a growing community of almost 200 participants on the main mailing list.

At its core the OpenChain Project is about providing a simple, clear method of building trust between organizations that rely on each other to share code and create products. Any organization that is OpenChain Conformant is aligning behind key requirements that their peers agree are required in a quality compliance program. This is about confirming overarching processes and policies, while allowing the specifics of each process and policy to be crafted by each organization to suit its specific needs.

Conclusion

The OpenChain Specification is ready for adoption by any organization that creates, uses or distributes free and open source code. The online conformance is free of charge, the mailing list and Work Team calls are open to everyone. Arguably, this is the first time a single, unifying approach to addressing the challenge of open source compliance in the supply chain exists.

References

- About the OpenChain Project: https://www.openchainproject.org/quick-start
- About the OpenChain Specification: https://www.openchainproject.org/spec
- About OpenChain Conformance: https://www.openchainproject.org/conformance

2 https://creativecommons.org/publicdomain/zero/1.0/

- About the OpenChain Curriculum: https://www.openchainproject.org/curriculum

About the author

Shane Coughlan *is an expert in communication, security and business development. His professional accomplishments include spearheading the licensing team that elevated Open Invention Network into the largest patent non-aggression community in history, establishing the leading professional network of Open Source legal experts and aligning stakeholders to launch both the first law journal and the first law book dedicated to Open Source. He currently leads the OpenChain community as Project Director.*