Panacea or Pandora?
An *Open Source* Geek Tragedy

Training Notes
for
Software Development Project Managers
on
Implicit and Explicit Assumptions
of
Code Ownership

Introduction

James Lindley

CISSP-ISSAP / ISSEP / ISSMP, CSSLP, CISA, PMP, etc.

Chief Secure Software Construction Engineer

Internal Revenue Service

Cybersecurity

Advanced Technical Analysis Team

Agency Executives and Software Development Managers are being told...

- Go to Open Source
- Save time and money
- Use other people’s work for FREE!!!

When Open Source is Used in Federal Software

- Project Manager is an ***agent*** of the agency
- Acceptance of Open Source license terms establishes both ***implicit*** and ***explicit*** contractual obligations
- Inclusion of Open Source in agency source code establishes implicit and explicit ***ownership obligations***

Project Manager as an A*gent*

- Inclusion of Open Source within agency source code is a ***project management*** decision
- Inclusion decision establishes a legal agreement with the copyright holder
- Agreement is subject to copyright law and civil enforcement
- License must be *understood* and *managed*

Implicit and *Explicit* Contractual Obligations

- Inclusion of Open Source in agency source code is an explicit action in acceptance of the Open Source license (specific license terms)
- Inclusion of Open Source in agency source code is an implicit acceptance of the general terms surrounding the license scheme (GPL, LGPL, etc.)

Implicit and Explicit ***Ownership Obligations***

- Project Manager responsible for ***business*** ownership obligations
- Project Manager is responsible for agency ***Enterprise Architecture*** (EA) obligations
- Project Manager is responsible for ***security*** obligations

Business Ownership Obligations

- Project Manager must ensure that Open Source meets original business functionality requirement (BFR)
- If BFR changes, PM must ensure that
  - Unaltered Open Source still meets BFR
  - Open Source can be altered – ***within the license terms*** - to meet changed BFR
  - Other Open Source that meets BFR can be found
  - Non-Open Source original code is written to meet BFR

Agency ***Enterprise Architecture*** (EA) Obligations

- Agency Enterprise Architecture (EA) generally requires
  - Written request to add identifiable software applications and components to the EA Accepted Software List
- Ageny EA software approval requirements are generally
  - Non-duplication of functionality
  - Establishment of a software maintenance chain
- Project Management responsible for obtaining specific written EA organizational acceptance
  - Demonstrating non-duplication
  - Specific acceptance of Open Source maintenance ownership

Security Obligations

- Submission of Open Source source code to any static source code security analysis team (SCSAT)

- Use of only Open Source source code that has been analyzed by the SCSAT and treated as below

- Alteration of original Open Source source code to eliminate insecure code constructions identified by SCSAT or in the National Vulnerabilities Database (nvd.nist.gov) to a *risk level acceptable to the base application's Designated Accreditation Authority (DAA)*

- Agency needs a "certified" Open Source reuse library

Software Copyrights

- Software is considered to a literary work
- Literary works are copyrighted by creation
- Copyrights do not have to be explicit
- Copyright holders control reproduction and use
- Control is asserted through a ***license*** mechanism
- There is no limitation on the license provisions
- There are some ***de facto standard*** licensing schemes (not legislative, but court supported)

Licensing Schemes

- Copyrighter grants various ***rights*** to others through a license mechanism
- No legally defined standard license, although various schemes, including the GNU family, have been held to be binding by courts in several nations
- May by unique in provisions, as a license is a copyright-holder-customizable contractual document
- Some *de facto* standards in the open source community
  - Apache License, Version 2.0
  - GNU General Public License (GNU GPL or GPL)
  - GNU Lesser Public License (LGPL)
  - Affero (GNU AGPL) (GPL for networked software)
  - Berkeley Software Distribution (BSD)

GNU General Public License (GPL)

- The GNU GPL is the most popular and well-known example of the type of strong ***copyleft*** license that requires derived works to be available under the same copyleft.
- Under this philosophy, the GPL grants the recipients of a computer program the rights of the free software definition and uses copyleft to ensure the freedoms are preserved, even when the work is changed or altered.
- This is in distinction to permissive free software licenses, of which the BSD licenses are the standard examples.

The GNU Lesser General Public License (LGPL)

- A modified, more permissive, version of the GPL, originally intended for some software libraries.

- There is also a GNU Free Documentation License, which was originally intended for use with documentation for GNU software, but has also been adopted for other uses, such as the Wikipedia project.

Affero General Public License (GNU AGPL)

- The GNU AGPL is similar to the GNU General Public License, except that it additionally covers the use of the software over a computer network, requiring that the complete source code be made available to any network user of the AGPL work (e.g., a web application).
- The Free Software Foundation recommends that this license is considered for any software that will commonly be run over the network.

GPL Not GPL

- The text of the GPL is not itself under the GPL.
- The license's copyright disallows modification of the license. Copying and distributing the license is allowed since the GPL requires recipients get "a copy of this License along with the Program".
- According to the GPL FAQ, anyone can modify the license as long as they use a different name for the license, not mention "GNU" and remove the preamble. The preamble can be used in a modified license with permission of the FSF.

Terms And Conditions

- The terms and conditions of the GPL are available to anybody receiving a copy of the work that has a GPL applied to it ("the licensee").
- Any licensee who adheres to the terms and conditions is given permission to modify the work, as well as to copy and redistribute the work or any derivative version.
- The licensee is allowed to charge a fee for this service, or do this free of charge. A distributor may not impose "further restrictions on the rights granted by the GPL". This forbids activities such as distributing of the software under a non-disclosure agreement or contract. Distributors under the GPL also grant a license for any of their patents practiced by the software, to practice those patents in GPL software.
- A requirement that programs distributed as pre-compiled binaries are accompanied by a copy of the source code, a written offer to distribute the source code via the same mechanism as the pre-compiled binary or the written offer to obtain the source code that you got when you received the pre-compiled binary under the GPL.
- A requirement giving "all recipients a copy of this License along with the Program".
- When not using one of the de facto *standard* license forms, copyright holders can write unique licenses with unique terms

Copyright And Contract

- In computing, software that is copyrighted and licensed under a software license is done under a variety of licensing schemes.
- For end-users there are proprietary licenses and there are free software licenses. Within these schemes are further classifications. There are also different licensing schemes for access to and use of source code. To address special intellectual property issues regarding source code, Open Source licenses and special copyright schemes, such as copyleft, have been created.
- Not all software is licensed, or even formally copyrighted. Software may be published without an accompanying license, as License-Free Software, in which case it remains copyrighted, its distribution is subject to ordinary copyright law, and its sale is subject to ordinary sales law.
- Software may also be released to the ***public domain***, in which case it is not copyrighted and the notion of a copyright license simply does not apply at all (although the other parts of a software license, including warranty provisions, will still apply to the *sale* of such software).

GPL 2 *compatible*

- The GNU General Public License is a popular license, with offerings including Linux, such that it is useful to know if the license chosen is compatible with it. Knowing compatibility is important if a developer wants to avail him- or herself of the wide GPL software 'commons'.

•Artistic License 2.0
•Berkeley Database License (aka the Sleepycat License or Sleepycat Software Product License)
•BSD license (modified version)
•BDL / BSD Documentation License
•CeCILL (*CEA CNRS INRIA Logiciel Libre*)
•Cryptix General License
•EUPL - European Union Public License
•GPL / GNU General Public License
•Intel Open Source License

•ISC license
•LGPL / GNU Lesser General Public License
•License of Perl
•License of Python
•MIT license
•Poetic License
•Public Domain
•W3C Software Notice and License
•WTFPL
•X11 license
•zlib/libpng license
•Zope Public License

GPL 2 *incompatible*

The GPL has certain special requirements that make code under licenses incompatible (that is, cannot be consequently licensed) under the GPL.

Academic Free License (AFL)
Affero General Public License
Apache License
Apple Public Source License (APSL)
BSD license (original version)
Common Public License
Common Development and Distribution License (CDDL)
Eclipse Public License (EPL)
IBM Public License
LaTeX Project Public License
Microsoft Public License
Microsoft Reciprocal License
Mozilla Public License (MPL)
Netscape Public License (NPL)
Open Software License
OpenSSL license
PHP License
Q Public License (QPL)
Sun Industry Standards Source License (SISSL)
Sun Public License

Software License Types

- **Non-free software license**
  - Microsoft Reference License
  - License given to the users of software marketed by reputed software companies for a price and for a specified period (in some cases).
- **Commercial Royalty-Free**
  - A form of licensing where typically a development version of the product is for a fee but the deployment of applications built or assembled with or using the product do not incur an additional fee.
- **Free Licensed Closed Source**
  - Free Solaris Binary License
  - Free For non commercial Use
  - Can be used for free by a party if the goal does not involve commercial gain. If it is used for commercial gain, payment is required. If it is used for charity/personal objectives payment is not required.
- **Pay Licensed Viewable Source**
  - Microsoft's Shared Sources
- **Pay Licensed Closed Source**
  - Microsoft Windows' EULA

Applying copyleft

- Common practice for using copyleft is to codify the copying terms for a work with a license.
- Any such license typically gives each person possessing a copy of the work the same freedoms as the author, including (from the Free Software Definition):
  - 0. the freedom to use the work,
  - 1. the freedom to study the work,
  - 2. the freedom to copy and share the work with others,
  - 3. the freedom to modify the work, and the freedom to distribute modified and therefore derivative works.
- (Note that the list begins from 0 due to a hacker tradition — first array element in C is numbered as 0.)

Copyright Domains

- Private Domain (the normal)
  - Creator is copyrighter
  - Work for Hire
- Government Domain
  - Owned by government
  - In some cases, usable without charge by citizens of government
- Public Domain
- All domain *releases* subject to **license** except public domain

Questions