Flowcharts for compliance in the supply chain

Armijn Hemel, MSc
Tjaldur Software Governance Solutions
armijn@tjaldur.nl

November 12, 2015

Today's goal: get started on easy to use flowcharts

Let's see if we can start on making flowcharts that are:

- easy to use in countries where English is not the main language
- useful to getting people up to speed
- codifying best practices

Guides from SFC, FSF and SFLC are great, but use language that is difficult for non-native speakers. They are also very long so it is easy to miss steps.

Building blocks

Let's first look at:

- distribution methods
- compliance options

Distribution methods

Software is usually distributed in one of the following ways:

- offline distribution: physical device, DVD, CD, memory stick, etc.
- online distribution (regular case): downloadable (partial) firmwares, apps
- online distribution (special case): over the air updates

Compliance options

For companies there are two ways to comply with GPL version 2:

- supply source code with binary code (GPLv2, section 3a)
- written offer (GPLv2, section 3b)

GPL requirements

- ship a copy of the license text with the software (source or binary)
- ship copyright notices with the software (source or binary)

Depending on how you distribute the binary there are different options available for fullfilling the GPL requirements:

	source code	written offer
offline	X	X
online (regular)	X	X
over the air		X

Let's quickly run through these and look at benefits and drawbacks.

Offline distribution: Source code

Benefits:

- all license texts present
- all copyright statements present
- after distribution you have no more license obligations

Drawbacks:

- possible e-waste (DVD/CD/memory card)
- correcting mistakes is expensive (possible recall)

Offline distribution: written offer

Benefits:

- easier to correct any mistakes
- less possible e-waste

Drawbacks:

- extraction of license texts
- extraction of copyright statements
- after distribution of the binary you have license obligations for an extended period of time (3 years or longer), so you need to keep track of what you distributed, and when, and where you stored the GPL archive

Source code with binary: online (regular)

GPLv2 states:

```
If distribution of executable or object code is made by
offering access to copy from a designated place, then
offering equivalent access to copy the source code from
the same place counts as distribution of the source code,
even though third parties are not compelled to copy the
source along with the object code.
```

which is understood by many as having source code with a firmware update online is good enough.

Online distribution: Source code

Benefits:

- all license texts present
- all copyright statements present
- after distribution you have no more license obligations
- correcting mistakes is relatively easy

Drawbacks:

- it is easy to lose track of GPL source code releases (website redesign by marketing department, server crashes)

Online distribution: written offer

Benefits:

- easy to correct any mistakes

Drawbacks:

- extraction of license texts
- extraction of copyright statements
- after distribution of the binary you have license obligations for an extended period of time (3 years or longer), so you need to keep track of what you distributed, and when, and where you stored the GPL archive

OTA updates

Over the air (OTA) updates can be performed with or without user interaction. If done without user interaction (auto-update) it is sometimes impossible to inform a user of its rights.

OTA distribution: Source code

Source code distribution for OTA updates is very impractical.

Drawbacks:

- huge download being forced upon users automatically
- very clear instructions needed for a user to get source code off the device

OTA distribution: written offer

Drawbacks:

- needs thought of where to put the written offer (device manual? device menu?)
- written offer might need to be renewed if software is added or removed
- extraction of license texts
- extraction of copyright statements
- after distribution of the binary you have license obligations for an extended period of time (3 years or longer), so you need to keep track of what you distributed, and when, and where you stored the GPL archive

Let’s try to make some flowcharts!

Assumptions:

- source code archive is “complete and corresponding source code
- there are no license violations in the code

Future work

We can probably make more flowcharts for other scenarios:

- incoming code
- scanning

Contact

- armijn@tjaldur.nl
- http://www.tjaldur.nl/
- Binary Analysis Tool: http://www.binaryanalysis.org/