Seven Concerns Open Source Should Worry About - Part 1

By Roy Schestowitz
Created 17/07/2019 - 2:09am
Submitted by Roy Schestowitz on Wednesday 17th of July 2019 02:09:10 AM Filed under OSS [1]

Not long ago, the Linux community celebrated the twenty-fifth anniversary of Linus Torvalds' famous Internet post, and thus its birth. While Linux was not the first open source project (Richard Stallman announced his GNU Project eight years before), it soon became the poster child of a new way of collaborative development that changed not only how technology is created, but many other aspects of the world as well. Today, most critical software platforms and architectures are open source, and virtually all proprietary software is riddled with free and open source software (FOSS) as well.

So, what could go wrong? Well, a lot, actually, unless we pause to think about where the potholes may emerge in the future, and how we can successfully navigate our way around them. That's what I plan to do in a series of articles to which this is the introduction.

Happily, all the potential concerns I will address can be addressed. That's the good news. The bad news is that neither the commercial world nor the community of developers has a very good history of thinking about some types of risks that might be expensive, inconvenient, or just plain boring to manage or fix.

Take security. That's hardly a risk that's unique to FOSS. But it is a concern that's been around for a very long time. So long that we have a pretty compelling record of how both human and commercial nature act in response to security risks. Or, more to the point, don't act. It would be impossible to find a single new wave of technology ? and there have been very many ? where security was not addressed as an after thought rather than designed in from the start. Almost always after multiple disasters had already occurred.

The latest example is the Internet of Things. The IoT has been building out for going on a decade now, and none of the initial devices had any security features at all. Most of the latest devices still don't. Some even have designed-in vulnerabilities, like factory programmed, unchangeable passwords.

Other risks arise from a different type of complacency ? assuming that because FOSS is ?good? that it's not possible to do anything ?bad? when it's created. That's a dangerous attitude to have when you consider that there are increasing numbers of projects that are heavily funded by multiple head to head competitors. FOSS projects need concise antitrust policies - and then they need to follow them. Codes of Conduct, too.
Other aspects of complacency relate to how effective FOSS licenses (as compared to what might be referred to as social pressures) are in a legal sense. Another is unquestioned assumption that the world will always be better with a single, dominant code base. Sometimes, competition between multiple architectures and platforms is a good thing. And while everybody wants to contribute to a rapidly expanding project that’s taking over the world, not everyone wants to do the boring maintenance work after its finished and becomes stable. If too many developers lose interest and drift away, still-crucial elements of the technology ecosystem can become dangerously vulnerable, stagnant and weak.

[2]

OSS

Source URL: http://www.tuxmachines.org/node/125969

Links: