Open source software is the better choice

SUN QIANG

21804416

Because of the lower cost, better quality, security and flexibility, open source software becomes more and more popular around the world. Governments use it to ensure daily operations or even deal with some top secret information. Schools use it to provide service to their staffs and students. Enterprises use it to make profits by providing service to their customers, such as the social media, Facebook. It almost affects all aspects of our lives.

In the information age, people pay more and more attention to their own information security. So, the problem is here: is open source software safe enough?

Open source means everyone can get full access to the codes. So everyone can help to find bugs. Just as the father of Linux said: " Given enough eyeballs, all bugs are shallow"[1]. However, some opponents believe that the number of people who are willing to find bugs is not as many as we thought. People are lazy. There are only 1.5% projects on Github which have more than 10 forks. At the same time, some people, who might be driven by money, are finding defects in open source software and attacking them, which might threaten our information safety. For example, the Heartbleed bug for OpenSSL in 2014.

No matter what they think, the fact is that there are less defects in open source software than commercial software according to Coverity scan report. We can see from the graph below:[4]

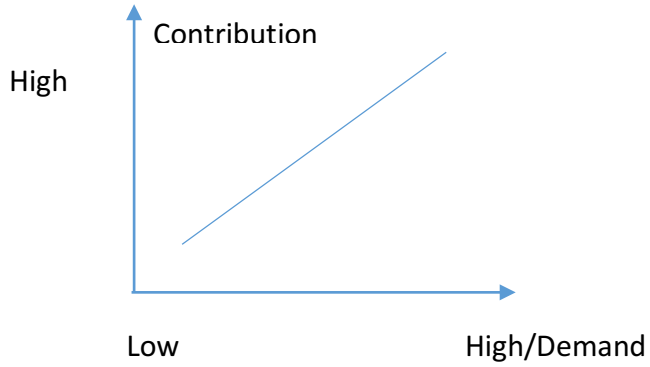
TABLE 7: 2013 DEFECT DENSITY BY PROJECT SIZE OPEN SOURCE VS. PROPRIETARY C/C++ CODE		
Size of Codebase (Lines of Code)	**Open Source**	**Proprietary Code**
Less than 100,000	.35	.38
100,000-499,999	.50	.81
500,000-1 million	.70	.84
More than 1 million	.65	.71
Average across projects	.59	.72

Fig: Defect Density Open source VS Proprietary Code

The defects in open source software is obviously lower than proprietary. If open source software has some risks, the proprietary won't be better.[5]

In fact, we can not eliminate all defects in software, so safety is a relative concept. If I am an individual user, when I use the open source software, I do not actually care about the safety problems. What I am only concerned about is whether it is useful and time saving. So I won't spend time finding bugs. However, if I am an enterprise user, I will have to think about the safety. I will consider that whether it is safe or whether I can bear the worst consequences if it is not safe, what I can do to reduce risks and whether I can review the code to reduce the defects.

The demand for security can be divided into different levels for different users. For individual users, it will be the lowest level. They will take no action and just use the software. For the governments or enterprise users, if they want to use the open source software to deal with some sensitive, important and top secret information, it will be the highest level. They will not only review the codes, but also take some actions to make their systems which build on the open source software more solid. The higher the demand level, the more contributions the users will make for the open source software.



So the point is that it doesn't matter how many people have reviewed the code. What matters is how many significant defects have been found and fixed. Different people from different countries, with different knowledge, work for different industries will work together to make one software better. The number and the diversity of the people who review the open source software are much more than the proprietary ones which are developed by one team with similar

background. This will make open source software better than the traditional ones.

At the same time, not every open source software will become Linux, OpenSSL, and play a very important role in our society. Some open source software are very handy and used to benefit out lives, we can accept that they will crash sometimes. So there is no need to make every project on Github have more than 10 forks to prove “Given enough eyeballs, all bugs are shallow”.

Good guys find defects, then report and fix it while bad guys find defects, then attack it and make money from it. So opponents insist that the proprietary is safer than open source software. The fact is that if some hackers want to attack you, unrevealed codes won’t stop them. On the opposite, seven hours after the Heartbleed was revealed, the defect was fixed. Things like this won’t happen if the OpenSSL is provided by Microsoft, they might take seven months to find the defects, fix it and release update. Some good open source software have communities with thousands of people, so a defect can be fixed within hours after it is revealed.

On the other hand, people who want to make profits from the defects of open source software also help to make open source software safer. They might do better than normal users or even professional testers. They will find some ‘ghosts’ in open source software and make it safer.

We can not eliminate defects. however, it doesn't mean that the number of defects are unlimited. As time goes by, there will be more and more defects found and fixed, and there will be less and less defects in open source software which makes them safer and safer. While the proprietary will get less and less resource to support them, eventually being killed. They will become more and more dangerous, just like windows XP. Much more defects like Freaks, Ghost and Venom found now, there will be less defects in the future and the software will be safer. The reuse of codes can make open source software safer and safer as time goes by.

Time saving, nearly free and security, it is not very hard for users to choose open source software even if they have a high demand for security because they can not develop a better one with limited time and budget.

The factor which really threatens the security of open source software is resource. OpenSSL only had 2 engineers who developed the project after work. Many good open source projects are lack of funds. Without enough funds, developers can not develop open source software with good quality within limited time. Things have changed after 2014 when the Heartbleed and Shellshock found. Big companies like google and Facebook invest a lot of money to support the good open source projects. They also join in the development of open source projects. This will promote the healthy development of open source software.

Nowadays, about 78% companies run on open source, and less than 3% never use open source. Use of open source to run business IT environments have gone up twice since 2010. Open source will inevitably become more and more popular. So the problem is not whether open source is safe, the problem is how we can make open source software safer and safer. It depends on how many resources we are willing to invest.

Compared with proprietary software, open source software is time-saving, easy to use and safer. While we can not eliminate all defects in software, so the safety of the software depends on our investments of resources.

Open source software is not perfect, but it is the better choice nowadays. And with the investment of resources, they can be better and better.

[1]"Open-source software", *Wikipedia*, 2016. [Online]. Available: https://en.wikipedia.org/wiki/Open-source_software. [Accessed: 14- Sep- 2016].
[2]"Open source software getting better", *Network Security*, vol. 2008, no. 6, pp. 1-2, 2008.
[3]M. Silic, "Dual-use open source security software in organizations – Dilemma: Help or hinder?", *Computers & Security*, vol. 39, pp. 386-395, 2013.
[4]2016. [Online]. Available: http://softwareintegrity.coverity.com/rs/coverity/images/2013-Coverity-Scan-Report.pdf. [Accessed: 14- Sep- 2016].
[5]*Sans.org*, 2016. [Online]. Available: https://www.sans.org/reading-room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements-1305. [Accessed: 14- Sep- 2016].
[4]2016. [Online]. Available: http://softwareintegrity.coverity.com/rs/coverity/images/2013-Coverity-Scan-Report.pdf. [Accessed: 14- Sep- 2016].
[7] Mohamed, Arif. (2008). Business & Technology.(open source software security). Computer Weekly, (164), Computer Weekly, April 8, 2008, Issue 164.