Heber Paz
1 February 2007
ITEC 4390

Open Source and Security

The argument of whether it is more secure to use open source or closed source software is an ongoing one. The article "Increased Security through Open Source" by Jaap-Henk Hoepman and Bart Jacobs makes the argument in favor for open source software. The term open source in this short paper will refer to the open access of the source code of software. There are several reasons for using open source software as opposed to continuing to use closed source software according to the article by Hoepman and Jacobs.

In the article "Increased Security", the authors use the analogy of whether you would trust a locksmith who keeps his locks secret as opposed to the locksmith who reveals his locks for all to scrutinize. The first locksmith would have less incentive to create a better lock because its secrecy would feel like part of the security of the lock. Also, how would a regular user be certain the lock is designed in the best possible manner? The second locksmith would have more incentive to create a better lock, because everyone can see it, and can also gain feedback on what the vulnerable points of his lock are. In the longer run the second locksmith's locks would be more secure because of the feedback that he would get from many users, including thieves and experts. This gives an advantage over the first locksmith because the second locksmith locks will have gone through scrutiny, feedback, and adjustments to improve the locks. People using the first locksmith will just have to trust that that person knows what they are doing.

Open source puts greater pressure and responsibility on a company or programmer to use the soundest methods to writing software. If the software code written is going to be accessible to the public, there is a greater incentive to do a thorough job in writing the code. It would not pay to be sloppy and careless in writing the code because everybody would be able to see the level of sophistication in writing your code. You would lose potential clients or at the very least you would lose credibility if you write inferior code.

Having an open source code puts the software at a greater risk for a short period of time because attackers can view the vulnerabilities. After the initial onslaught, however, patches and fixes are contributed by the many software users which make the software more secure over the long run. Open source also allows users – companies or individuals – to assess the security for themselves. Using their own team or third party to assess the security of a code as opposed to trusting that the source party (the writers of the code) has done an adequate job is a major benefit for open source users. If a bug is found, they themselves can make a patch in open source. As opposed to closed source, where a bug could be reported and never be fixed or the fix is provided months later.

In their article, Hoepman and Jacobs conclude that making existing systems open source will increase security despite making the systems more exposed, not more vulnerable since any vulnerabilities were already there to begin with. They conclude that the exposure would be only for a short period of time as patches and security fixes become available. Users would not have to wait for the closed source party to provide a fix since they would have access to the source code.