Linux.com

Everything Linux and Open Source

Why open source works for weapons and defense

January 21, 2006 (8:00:00 AM) - 2 years, 10 months ago

By: **Jay Lyman**

Military, weapons, and national defense are certainly not synonymous with open source software, but developers and companies that provide Linux and other open source software for such applications indicate the ideals of open source communities are not contrary to its use in defense.

In fact, what would be contrary to the guiding principles of open source, namely freedom and flexibility of use, would be to preclude the use of open source anywhere, regardless of whether it is the Peace Corps or the Department of Defense (DoD).

Those most vocal about claiming open source is unsuitable often have proprietary software solutions to sell. **Green Hills Software** President and CEO Dan O'Dowd has said that FOSS is only for those who cannot afford proprietary software, and is not fit for military and defense.

O'Dowd **argued** that open source software is not better than proprietary software, and claimed that no open source real-time operating system, debugger, or compiler could rival his own company's proprietary technology.

"Open source is not about making better software, it is about making cheaper software for those who can't afford the best software," O'Dowd told NewsForge. "The military must have the best software: the most secure software and the most reliable software. Unlike students, academics, and third-world computer users, the military has the money to buy the best software. The military doesn't buy used uniforms at Goodwill, they don't buy hand-me-down weapons systems from other countries, and they don't buy used trucks for transportation. No, the military must buy the best equipment and software, because doing anything less is a threat to national security."

O'Dowd claimed he had even convinced some within the open source software community that it was not appropriate for such applications with a series of papers he wrote on "the enormous security problems in Linux" in 2004. However, many in the open source community **were not convinced**.

"Since then, almost all military programs have backed off of considering Linux," he said. "After reading my papers, even open source advocates usually acknowledge that Linux is not appropriate for military, weapons, and defense applications."

For the needy, but not defense

Sam Nitzberg -- an information security specialist with publications and presentations related to military informatics, computer security, technology, and ethics -- indicated the argument is far more complex than O'Dowd makes it, and while he said he believed open source software was indeed appropriate for military and defense application, he added such systems are typically expensive to develop, and pose grave consequences if they fail.

"These systems can also be very complex in nature, and may have to interact with a great number of other systems," Nitzberg said. "Open software and standards can help in these areas. However, just as in the case of proprietary or closed software, an organization tasked with building these systems must carefully deliberate when making software and baselining decisions: identifying the risks involved in using the open source or proprietary software components as its building blocks, weighing how the risks compare to its alternatives, estimating the total costs to be borne, how will the operating systems and tools work with existing technologies being used, considering what degree of support is available, and how will any programmatic risks be mitigated."

"Perhaps the greatest potential strengths of open source revolve around its transparency," Nitzberg said. "You know what you are getting, and this can foster a high degree of trust in the software."

Developers have ideals

Open source developers have heard all the arguments about the quality of propriety vs. open source software before, and answered them ad nauseum. What concerns them more is the moral issues for software authors, not buyers.

"Freedom is the number one ideal of open source and I believe it would be contrary to these ideals to restrict what the software is being used for," said **Brandon Philips**, an open source developer and Oregon State University Open Software Lab contributor who worked on NASA software that has potential weapons applicability last summer. "The FOSS community is providing a general purpose foundation for a computing system that requires a great amount of customization for a military application, and because of the dedication to the ideals of freedom, I think it is a valid, however possibly unfortunate, use of the software."

Citing a passage of Martin Krafft's *The Debian System*, Philips referred to the prohibition against preventing "persons, groups, or fields" from using the open source Debian operating system. The Open Source Initiative's **Open Source Definition** also prohibits licenses from discriminating based on fields of endeavor or persons or groups.

When asked about the ethical implications of creating something with applicability in weapons or warfare, Philips said the intent is good software for any number of potential uses.

"The project I worked on this summer while in the NASA Goddard Robotics Internship Program was general purpose hand recognition software that had as much application on use for Mars rovers and programs for physical rehabilitation of children as it does on a military robot," Philips said. "This is the only software that I have ever developed that has any military applications. Although I am concerned that the software could be used in a weapon, I am hopeful that more productive application may be found. And by using a FOSS license, a developer may be inspired by this software and create an entirely new application."

Free as in freedom

Nitzberg reiterated the point that military, weapons, and defense applications are not at all in conflict with the ideals of much of the open source community.

"Software licenses for open source tend to revolve around distribution mechanisms, defining appropriate copyright mechanisms, requirements to provide any modified sources, rights of users, and the software being 'free' -- as in freedom, not price," Nitzberg said. "If the basis of open source is that a central and defining theme is 'freedom,' there is an immediate contradiction if you then indicate what organizations and bodies you do not wish to make use of these products. Is it OK to restrict such use sometimes, but permit it when you approve of the actions of the government or military?"

Nitzberg dismissed the idea of tying licensing to conditions of how the software is used, or trying to limit its use based on the missions of a given organization that might employ the software.

"I believe this would be problematic," he said. "Very quickly, 'socially-aware' open source software bodies could be partitioned by their areas of interest. If the basis for using the software is restricted based on whether an organization is governmental, military, eco-friendly, or socially aware by any other measure, this could degenerate to the creation of white lists, black lists, and others -- defining organizations permitted to use the software decided by committee. This could become an intractable quagmire for such open source. Also, the talent pool and cumulative efforts would be likewise divided into specific areas of interest. I do not think that factionalizing open source or freeware development on this basis would be desirable or healthy for the open source movement.

"If open source is truly about free software, government or military use will be a natural aspect of broader and growing acceptance of open source."

A matter of ethics

Nitzberg said the ethical issues are faced not only by open source software communities, but by much of the software community and industry in general.

"If you work for a major database vendor, an operating systems provider, an Internet service provider, develop embedded or real-time software technologies, or work with other software technologies, you often really don't control to what ends your product is ultimately used," he noted.

Nitzberg said if people have personal beliefs that guide how software is to be used, but want it to be open, they can produce a customized license, which would help ensure that the efforts were further developed and extended under the beliefs that guided the software's creation, and guide its further use. However, Nitzberg added, this might also limit the software's use, adoption, and any chance for broader acceptance.

"People also have to make sure that they understand the ethical and real ramifications of their work, and that they are comfortable with its use," he said. "In their day-to-day software work, do they believe and support their missions and the legacy their software may leave behind? The personal approach that I take is to try to support the development of systems using the best skills, methods, and efforts that I can to help ensure that the systems do not cause any harm through the results of errors, poor design, weaknesses in security, or other discrepancies. This stands whether I am using open or proprietary products."

Stability, security, and peace

Companies such as **LynuxWorks** -- which counts Linux-based embedded operating systems and other software sold to the aerospace and defense industries as half of its business -- are evidence that both government and the military really do see a place for open technology and open source software in mission-critical applications.

LynuxWorks Director of Business Development Steve Blackman said that his company's open architecture and open source software solutions play prominently in US defense systems and solutions.

"The Department of Defense believes it's appropriate," he said, adding that the government agency has deemed open source adequate and compliant with software acquisition and assurance standards, such as **National Information Assurance Partnership** (NIAP) standards.

"That's a whole industry to make sure any software -- be it open source or proprietary -- is safe and doesn't have inappropriate backdoors," Blackman said. "Open source software is not an issue to them."

Blackman said government and the military are more interested in the "free as in freedom" aspects of open source software, as opposed to "free as in beer," adding that FOSS is ideal for such applications because of its flexible and customizable nature. Referring to deployments of open solutions in Iraq, for instance, he argued open source is often more agile for military uses.

"That gives them the autonomy to respond to what needs to be done," he said. "It makes it easier if they don't have to go back and change or re-license. They can just do it."

Blackman also argued the creation and support of a strong military posture, with help from open architecture and open source technology, helps promote peace.

"I believe by supporting our government, aerospace, and defense, it's very ethical to support a secure world," he said. "I think we try to do good things."

While he added it might not sound like a good thing to help provide the components of a nuclear firing control device, companies such as LynuxWorks using open technology are determined to ensure that such systems are safe, reliable, and free of bugs.

Open source rising

Looking ahead, Nitzberg indicated open source software may be building on the base it has already established in defense.

"Open source operating systems have in fact been successfully and productively used in these areas, and will continue to do so," he said. "I believe that the true impact, and true potential, may be yet unseen."

Nitzberg said he was unsure if open source software could reach a critical mass in weapons and defense in the near term, but he stressed the nature of what open source aspires to be -- epitomized by high quality, maintainable code -- will give open source its place in mission-critical systems that must perform repeatedly, predictably, reliably, and accurately.

"Determining if open source systems will become ubiquitous in mission-critical or defense applications really calls for a long event horizon," Nitzberg said. "I will say that I think that it is possible that someday, open source could be prevalent in these environments, but that the systems and applications may not reflect the current software or baselines. Any such trend may start before too long, but take an entire generation to take hold."

Read in the original layout at: **http://www.linux.com/articles/51413**