Open Source Software and Cyber Defense

A White Paper provided to the National Security Council and Homeland Security Council as input to the White House Review of Communications and Information Infrastructure.

Bob Gourley
Chief Technology Officer, Crucial Point LLC
bob@bobgourley.com
01 April 2009

Open Source Software is providing computer defenders with a new tool which can dramatically enhance the security posture of the federal enterprise and the IT fabric which drives our nation's economic engines. This paper examines key trends in open source software and provides facts regarding its enhanced security features relevant to the White House cyber review.

For the last year the US government and several allied nations have been providing increasing amounts of information to the public about a wide range of computer threats, including intrusions into government and industry computers from organized crime, malicious code, foreign militaries, and the intelligence services of foreign countries including Russia and China. Although these threats have been highlighted every year in congressional testimony, the threat has grown so great that increasing amounts of information are being shared in a wide range of venue, including interviews with senior leaders, editorials by government executives, and official liaison with information sharing organizations set up to exchange threat information with state and local governments and leaders of key critical infrastructure sectors.

A new phenomenon is also contributing to our understanding of this threat. Independent teams of researchers using publicly available information and computer forensics investigations have been conducing assessments and analysis of major threat activities. For example, on 29 March 2009 a report of investigations conducted by a consortium led by researchers at the University of Toronto issued stunning conclusions on the incredible cyber espionage network emanating from China. The espionage network has invaded over 1,295 computers in 103 countries, including many belonging to embassies, foreign ministries and other government offices.[1]

Of particular interest is a companion study conducted by researchers at the University of Cambridge titled "The snooping dragon: social-malware surveillance of the Tibetan movement."[2] This research, which was sponsored in part by the U.S. Department of Homeland Security, was a more technical look at attacks from the Chinese espionage network. **A key conclusion:** countermeasures which can address technical dimensions of these attacks should include open source software. Security Enhanced Linux and Open Solaris with Trusted Extensions are particularly emphasized.

Which leads to the key thesis of this white paper: Commercial Open Source software (COSS) is more secure and, when used in integrated solutions with good security engineering practices, **Open Source software results in more secure systems.**

What is Open Source software? It is computer software for which the source code and other rights are provided under a software license that meets the open source definition. This definition permits users to use, change and improve the software and redistribute it in modified or unmodified forms. Open Source software is always available for review, and in most cases it is developed in an open, public, collaborative manner. Open source does NOT just mean access to the source code. The distribution of open source software must comply with several specific criteria of the open source license, including free

---

1. See http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network
2. Available online at: http://www.cl.cam.ac.uk/techreports/

redistribution, source code, ability to produce derived works, integrity of the author's source code, no discrimination against persons or groups, and no discrimination against fields of endeavor.[3]

Examples of Open Source software exist in every layer of the software stack. Operating systems that are open source include Linux, Solaris and BSD. All are Open Source Initiative (OSI) license approved and all run on many types of processors, including x86/x64 chips. Open source middleware includes application hosting and application, websever, optimization tools like JBoss, Glassfish and Apache. Open source databases include MySQL and PostgreSQL. Open source applications include the Firefox browser and the Open Office application suite.

These and other open source applications now exist in almost every organization in the US. Gartner estimates that 85% of all enterprise IT runs on open source. 73% are fielding large solutions based on MySQL. The majority of the intelligence community's data centers now run on open source software.

Open source software now has a large and thriving developer community. Over 900,000 developers are coding in open source software today. This is larger than all the proprietary developers of all the proprietary closed source software companies put together. And these open source software developers are highly skilled, experienced programmers (the average age of an open source developer is 30. The average length of programing experience is 11 years).

But what about security? The facts are in. Years of tracking of vulnerabilities detected in proprietary systems and in open source systems have shown that the care in design of open source and the models of scrutiny and code review produce real results. Almost all software (at least all I have ever heard of) has some vulnerability and requires patching and updating to be optimized against the threat, but Commercial Open Source software is much more secure. The number of raw vulnerability reports is much less, but as a measure of risk and significance we can also track those reports which the federal government's network and computer defenders have assessed to be so significant that they require special technical alerts and/or vulnerability notes. US CERT vulnerability notes and technical alerts are searchable in the National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security Cyber Security Division and is maintained by the National Institute of Standards and Technology. It is the US government repository of standards based vulnerability measurement data. [4]

As search of this database over the last three years reveals:

For operating systems:

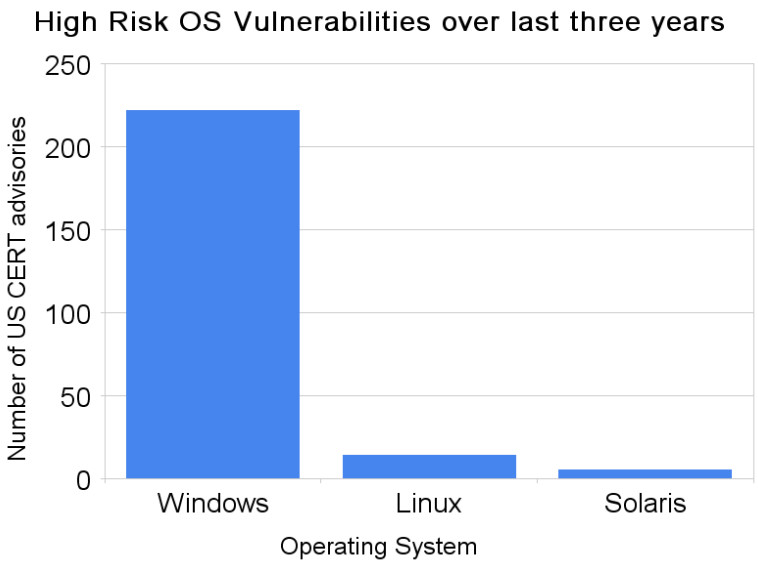
- 222 US CERT technical alerts and vulnerability notes have been issued on Windows.
- 14 US CERT technical alerts and vulnerability notes have been issued on Linux (open source).
- 5 US CERT technical alerts and vulnerability notes have been issued on Solaris (open source).

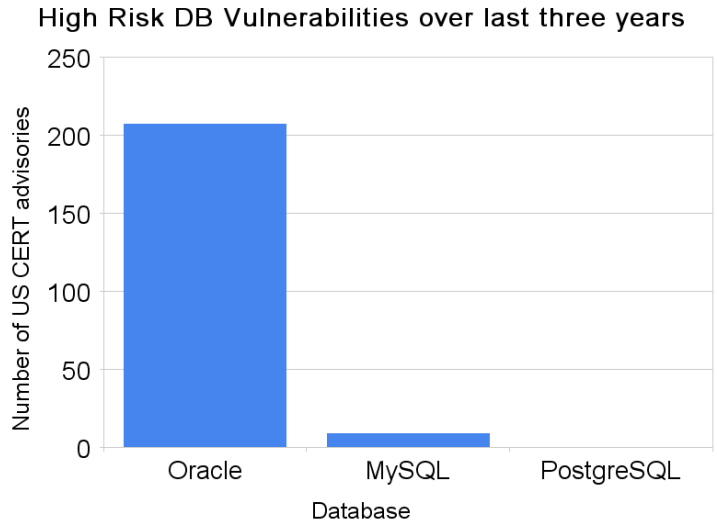
For databases:

- 207 US CERT technical alerts and vulnerability notes have been issued on Oracle.
- 9 CERT technical alerts and vulnerability notes have been issued on MySQL (open source).
- 0 CERT technical alerts and vulnerability notes have been issued on PostgreSQL (open source).

---

3. There are some variants to the Open Source license. For details see: http://www.opensource.org/
4. These and other statistics are available from the national vulnerability database at http://nvd.nist.gov/nvd.cfm .





These trends are apparent in many other aspects of the software industry. One clear example worth noting is the Commercial Open Source Software Java. Java is used on almost every cell phone and hand-held device in the globe (it has been fielded on over 6 billion devices to date), has had only 7 vulnerabilities ever discovered.

Other evidence of open source security strength comes in approval of operating systems under their common criteria framework. The Common Criteria for Information Technology Security Evaluation is an international standard for computer security certification. It is a framework in which computer system users can specify their security requirements, vendors can implement and/or make claims about security attributes of their products, and testing labs can evaluate the products to determine if they meet the claims.[5] The top three enterprise operating systems in terms of testable security profiles in the common criteria framework include Solaris, Security Enhanced Red Hat Linux, followed by a distant third by Microsoft Windows. In other words, Microsoft does not even assert its systems are as secure as open operating systems.

---

5. For more on the Common Criteria see: http://en.wikipedia.org/wiki/Common_Criteria

Perhaps the greatest metric regarding security, however, is a review of all major incidents known in the cyber security dimension. Attacks, for the most part, are against windows devices. And, although for the most part the biggest attacks are against boxes that are not fully patched, red team practitioners are always quick to point out that there is no such thing as a secure windows box.

Why are open systems more secure? Perhaps the greatest reason is the code development and code review process, which allows bugs to be found before fielding and also enables more complete testing and vetting of code. Bad code is found earlier in the development process and is more easily discovered during testing after development. This applies to all open source code, not just operating systems. Operating systems that are open source, however, share a common design feature of having security build into initial designs, and that early on design focus on security is paying off for its security resiliency today.

Proprietary closed source software is less likely to have vulnerabilities discovered early in the development cycle and, since many vulnerabilities are only discovered after software is brought into the enterprise, costly, reactive patch processes must be developed and expensive continuous testing and evaluation processes must be put in place. Even open source software needs testing and continuous evaluation, but this is made much more efficient by visibility into the source code.

What can federal IT leaders to to leverage Open Source software for enhanced security? The following are some tips/suggestions:

- As always, ensure that security is planned into all IT projects from the beginning. Security engineering is an important step regardless of which technologies are used.
- The same is true regarding patching. Commercial open source systems require far fewer patches because they are designed better. However, patching processes must still exist.
- Ensure users are trained to never disclose their password or fall for social engineering tricks. Open source software can provide technological barriers to attack, but the human element must also be strongly enabled to defend information.
- To the greatest extent possible, base servers on open source operating systems, and base databases on open source databases such as MySQL and PostgreSQL.
- The most secure desktops should be Solaris or Linux and should run Open Office applications.
- When applications or users demand Microsoft desktops, those should be presented through secure operating systems. For example, Microsoft desktops can be presented through remote desktop protocol onto a Sun Ray thin client or a Linux or Open Solaris desktop. This makes patching windows far easier.
- The federal government should continue to expand engagement with the open source community by continuing efforts designed to continually improve the security of SE Linux and Open Solaris.
- The open source community can also be engaged to greater degree by focused interactions with the US vendors who support and grow open source, including IBM, Sun Microsystems, Red Hat, and Sourceforge.

The smart use of Open Source software can enhance the security posture of the federal IT enterprise. Since it also increases agency agility and reduces costs, this is a particularly virtuous capability that should be considered in conjunction with other dramatically transformational technologies such as cloud computing. Open Source software is more secure and it can make the federal IT enterprise more secure.

Bob Gourley is the former CTO of the Defense Intelligence Agency and is a recipient of Infoworld's Top 25 CTO award for 2007. He won AFCEAs award for meritorious service to the intelligence community in 2008 and is now the lead writer at http://ctovision.com and is the CTO of Crucial Point LLC, an IT consultancy. Contact Bob at bob@bobgourley.com