c|net NEWS.COM http://www.news.com/

Linux guru warns on security of open-source code

By Richard Thurston
http://news.com.com/Linux+guru+warns+on+security+of+open-source+code/2100-1002_3-6129835.html

Story last modified Thu Oct 26 12:47:45 PDT 2006

Alan Cox, one of the most respected figures in the U.K. open-source community, has warned about complacency over the security of open-source projects.

Speaking to delegates at London's LinuxWorld conference on Wednesday, he emphasized that considerable sums of money were being spent in attempting to hack into open-source systems.

And he cautioned that many open-source projects were far from secure.


Alan Cox
Linux developer

"There is a lot of money going into security, but the situation is worse, because there is a lot of money going into breaking security. People are being paid to work breaking down software systems," Cox, who is employed by Linux seller Red Hat, told delegates.

"Things appear in the media, like 'open-source software is more secure, more reliable and there are less bugs.' Those are very dangerous statements," Cox said.

Cox said that analysis looks only at well-known projects. An analysis of 150 projects from SourceForge, a repository for open-source code, would not result in the same high marks that the Linux kernel would get, he noted. "High-quality only applies to some projects--those with good code review and those with good authors," Cox said.

"The debate of Microsoft saying 'Look how secure we are' versus Linux saying 'We're more secure' is not looking at the important points," he added.

Cox, who has been closely involved with the development of the Linux kernel for many years, also took the opportunity to take a swing at a newly launched project that promises to measure the quality of open-source code.

The Software Quality Observatory for Open Source Software (SQO-OSS), funded by the European Commission, was launched on Monday. Cox told delegates that metrics must not become targets.

"It is good to build metrics, and SQO-OSS has great potential," he said. "But there are problems with this, and there are risks associated with that kind of methodology.

"If you are working with metrics and you have 14 bugs, you fix the 13 easy ones, and the one hard one

can wait. That happens in the security world, but it becomes inefficient."

Richard Thurston reported for ZDNet UK in London.