ORNL technology may better detect cyber security attacks (w/ Podcast)

March 3 2010

A system that can more effectively detect possible cyber security attacks within large organizations - including government agencies -- is being developed with the assistance of the Department of Energy's Oak Ridge National Laboratory.

Justin Beaver of ORNL's Computational Sciences and Engineering Division is leading the technology's development team.

"One of the problems with existing intrusion technologies is that they alert so frequently that an operator or analyst has a very difficult time determining which alerts they should most concerned with," Beaver said. "What we've got is an engine that analyses that data for you. The computer does the work of filtering out the signal from the noise."

Beaver said the Oak Ridge system enables security personnel to more accurately detect actual cyber attacks.

"The typical set-up for a cyber defense is that you have a collection of tools that you put together for any kind of large organization," Beaver said. "They always set up some kind of cyber defense that is comprised of many niche tools. All of these things pipe into one channel. There is a huge amount of data that has to be handled, analyzed and processed.

Provided by Oak Ridge National Laboratory