



PERTH LINUX USERS' GROUP

April 2010 Seminar

Title: A new approach to restricting applications, and why traditional approaches to security are no longer adequate (FBAC-LSM)

When: Tuesday, 13th April 2010, 7:30pm - 9:00pm.

Where: ['Futuresphere'](#), Christ Church Grammar School, Queenslea Drive, Claremont

Presenter: Z. Cliffe Schreuders

Linux, like most operating systems, typically allows programs to act with all the authority of the user. However, this approach is inadequate in the current threat climate as basing security decisions on the identity of the user does not protect against processes which act maliciously due to software vulnerabilities or malware. Security systems exist which can restrict the actions of individual applications on Linux, although generally they are very hard to use. FBAC-LSM is a new scheme for restricting applications based on the functionalities they provide. It is designed to be easier to use than previous systems.

In this talk I will describe why the traditional approaches to security are no longer adequate, and I will describe FBAC-LSM. Last year a usability study was conducted (with a number of PLUG members participating) which compared SELinux, AppArmor and FBAC-LSM. I will give an overview of the results of the usability study. I will also give a live demo of using FBAC-LSM to confine a Trojan horse.

I am currently recruiting collaborators to help develop FBAC-LSM further. I will give a quick overview of how FBAC-LSM is designed for anyone interested in becoming involved.

FBAC-LSM is in development and is available as free open source software: <http://schreuders.org/FBAC-LSM>

Z. Cliffe Schreuders is a PhD candidate and casual lecturer at Murdoch University, Western Australia. Recently Cliffe has presented at academic and Linux conferences in England, Portugal, New Zealand and Australia. His current research aims to provide more useable application restrictions.