Blog Export: c0t0d0s0.org, http://www.c0t0d0s0.org/

Tuesday, May 30. 2006

Application Containment by OS Virtualisatiion

When you test an application you have to ask yourself, if the application is trustworthy. After reading this article about ultra-fast creation of Solaris Container, the following idea came into my mind:
Imagine a wrapper that clones for every application you want to use a container, executes the programm in this containers and destroys the application after the exit of the application. Obviously you would use an shared filesystem for data storage (like /export/home/), but any modification outside the home dir would disappear immediately after executing. Furthermore when the application opens an backdoor and uses an root exploit, the backdoor and the exploit is contained against other users, other applications and other systems.
Or to take it to an extreme: everytime when a users logs into the system a containment container will be created and destroyed. I will think about this idea a little more ...

Posted by Joerg Moellenkamp in English, Solaris at 22:02

In addition, the shared storage (which in the case of a home directory would be zfs as well) is set to a new snapshot.
Did I mention that I love zones and zfs?
Anonymous on May 30 2006, 23:04

No, you didn´t but this is pretty obvious
Anonymous on May 31 2006, 06:32