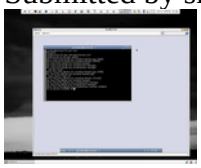
Intent Is The Problem

By *srlinuxx*
Created *06/12/2009 - 11:18pm*
Submitted by srlinuxx on Sunday 6th of December 2009 11:18:50 PM Filed under OS [1]



Of late, I keep banging into the problem that people want systems to be ?secure by default?: they don?t want to pester the user about security. They want the system to just do the right thing. The problem is, this just isn?t possible. One example I like to give is ?rm -rf *?. Clearly this command is sometimes a very bad idea, and sometimes exactly what you want to do. If some piece of code I mistakenly trusted runs that command on my behalf, I might be very sad about it. Therefore, any system that wants to be ?secure? has to somehow know that when I move to some directory and type rm -rf * I mean it, and when I run a piece of code I?m expecting to (say) edit some text, I don?t mean it, and it should not be allowed to do it.

How can the system discover this? Clearly it must be through some user action. The user must behave differently in some way in the two cases, so that the system can discover his intent. Therefore it is impossible to be ?secure? without, in some way, consulting the user about his intent.

Rest Here

OS

Links:
[1] http://www.tuxmachines.org/taxonomy/term/37