Kepler - Bug #3072

Security issues with distributed execution

01/16/2008 02:58 PM - Chad Berkley

Status:	Resolved	**Start date:**	01/16/2008
Priority:	Normal	**Due date:**	
Assignee:	jianwu jianwu	**% Done:**	0%
Category:	distributed execution	**Estimated time:**	0.00 hour
Target version:	master-slave-2.0.0	**Spent time:**	0.00 hour
Bugzilla-Id:	3072		

Description

See bug 3071. basically, the issues are that arbitrary code can be executed on the slaves so the utmost care needs to be take wrt security. kar files need to be signed, workflows should also possibly be signed. the command line and scripting actors might need additional security built into them. This basically breaks the java sandbox.

History

#1 - 01/28/2008 03:52 PM - Christopher Brooks

Ptolemy is reasonably well set up to use the Java sandbox, see $PTII/doc/sandbox.htm for details.

The sandbox has fairly fine granularity, by default the execution
of subprocesses is probably disabled.

See $PTII/bin/sandbox.policy for what is enabled.

Perhaps remote kepler processes should be started up in a sandbox in the default,
with the command line and scripting actors defacto disabled?

#2 - 01/28/2008 04:24 PM - Matt Jones

Its the ability to use the command line actor (for access to various custom simulation models) and the scripting actors like the RExpression actor (to do various custom data processing tasks) that would make distributed execution useful. Eliminating these from the actors available essentially eliminates a vast majority of workflows that a scientist would want to run in a distributed environment. This is a major security/capability dilemma.

#3 - 01/28/2010 10:07 AM - jianwu jianwu

It can be configured by permission policy file at slave side. Users who start slave will know their requirements and do the corresponding configuration. How to change policy file to permit and forbid ExternalExe and Python actor has been tested. Matlab and R scripting actors are also being tested.

#4 - 05/20/2010 09:20 PM - jianwu jianwu

It is fixed at version 24539. When a slave is started using startWithExecutionPolicy command, it will use master-slave.policy file to run in a secure sandbox.

By default, it will not allow 'External Execution', 'Python', 'Matlab', 'R'
actors to be executed at the slave side, since there may be malicious codes embedded in these actors.

By configuration this file, the allowance for the above actors can be configured.

#5 - 03/27/2013 02:22 PM - Redmine Admin

Original Bugzilla ID was 3072