A Security Solution for GridSpace2 Platform

Jan Mezner(1), Eryk Ciepiele(1), Piotr Nowakowski(1), Joanna Kocot(1), Maciej Malawski(2), Marian Bubak(1,2,3)

(1) AGH University of Science and Technology, ACC Cyfronet AGH, Krakow, Poland
(2) AGH University of Science and Technology, Department of Computer Science, Krakow, Poland
(3) Informatics Institute, University of Amsterdam, The Netherlands

Objectives
- advanced security system for GridSpace [1], going beyond Shibboleth, GSI and Linux-PAM protected resources [2,3]
- enables secure access to heterogeneous computing and data storage resources as well as sharing experiments while protecting confidential data [4]

Security modules

EW AuthNZ password-based authentication; secure SSH connection to the EH with PL-Grid account credentials

Local Wallet – a tool allowing storage of confidential data (e.g. credentials) in protected files (UNIX permissions)

Remote Wallet (ReCeW) – a UNIX daemon for secure storage of confidential data accessible to EH users via RESTful remote API from many locations (EH, external machines, e-Infrastructures), employing AES-256 encryption. Features a plugin mechanism enabling easy development of new extensions

ReCeW / Local Wallet Clients – enable management of wallet contents in the EW and permit use of secure data in scripts (for access to external services, data sources etc.)

Architecture

Example of usage
- access the whole platform by logging into the Experiment Workbench using any Experiment Host account (e.g. PL-Grid account)
- submit jobs to computing clusters from EW without additional security-related effort
- store, manage and access arbitrary confidential data in a secure manner with high-grade encryption algorithms
- use custom credentials to access external services – databases, Grids, Clouds, custom Web/REST services etc.

Future work
- new ReCeW plugins (new modules, streamlined remote API)
- enable ReCeW to be hosted in the Cloud (Security-as-a-Service model)

References