A virtual laboratory for decision support in viral disease treatment

A Security Infrastructure for MOCCA Component Environment

http://virolab.cyfronet.pl

1. Objective
Concept and development of a new security system for H2O and MOCCA

2. Target environment
• H2O
  - Middleware platform for distributed computing
  - Providers setup H2O kernel (container)
  - Allowed parties can deploy pluglets (components)
• MOCCA
  - Distributed, CCA-compliant component framework
  - Build on top of H2O, uses its security mechanisms

3. Authentication in H2O
• Extensible, pluggable architecture
  - Tunneled
  - Chain of authenticators
  - Based on message exchange
  - Similar to Pluggable Authentication Modules
  - Returns Subject object – for JAAS authorization
• Only basic Password Authenticator by default
  - Low level of security
  - Simple to intercept
  - Careless users...

4. Concept and implementation
• H2O-applicable authenticator
  - based on PKI and X.509
  - providing delegation based on proxy certificates
• Compliant with GSI
  - Single Sign-On and delegation using proxy certificates
  - Widely deployed on production infrastructures (EGEE)

Authentication steps:
• Identity introduction – with (proxy) certificate
  - Kernel verifies validity and checks if the issuing CA is trusted
• Identity confirmation – simple challenge-response algorithm:
  - Kernel encrypts a nonce and sends it to the client
  - Client decrypts and signs the nonce and sends back to the kernel
• Credential delegation:

5. Performance
• Authenticators comparison
• SSL/TLS and server authentication overhead

Authors
Michał Dyrda (1), Maciej Malawski (1), Syed Naqvi (3), Marian Bubak (1,2)
(1) Institute of Computer Science, AGH, al. Mickiewicza 30, 30-059, Kraków, Poland
(2) Academic Computer Center CYFRONET, ul. Nawojki 11, 30-950 Kraków, Poland
(3) CETIC, Rue des Freres Wright 29/3, B-6041 Charleroi, Belgium

References
Maciej Malawski, Dawid Kurzyńiec, Vaidy Sunderam: MOCCA – Towards a Distributed CCA Framework for Metacomputing, IPDPS 2005