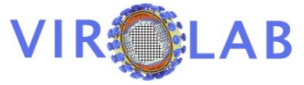
AGH University of Science and Technology



Security in Component Grid Systems

Michal Dyrda

Master of Science Thesis

Faculty of Electrical Engineering, Automatics, Computer Science and Electronics
Institute of Computer Science

Krakow, June 2008

AGH

Outline

- Introduction
  - MSc Thesis Goals, Target Environment
- Security Concepts in (Component) Grid Systems on Example of H2O
  - Overview, Authentication in H2O
- Concept of GSI Authenticator
- Authenticator Validation
  - Performed Tests, Threat Analysis, Performance Analysis and Discussion
- Work status
  - Summary of Work Done, Future Work

VIROLAB CoreGRID

AGH

MSc Thesis Goals

- Identification and analysis of security architecture and shortages in H2O
- Overview of available solutions for H2O security enhancements
- Concept and development of a security solution for H2O and MOCCA that would answer the presented shortcomings
- Proof of correctness and usefulness of the created solution
- Build, configuration and usage description
- Identification of future work

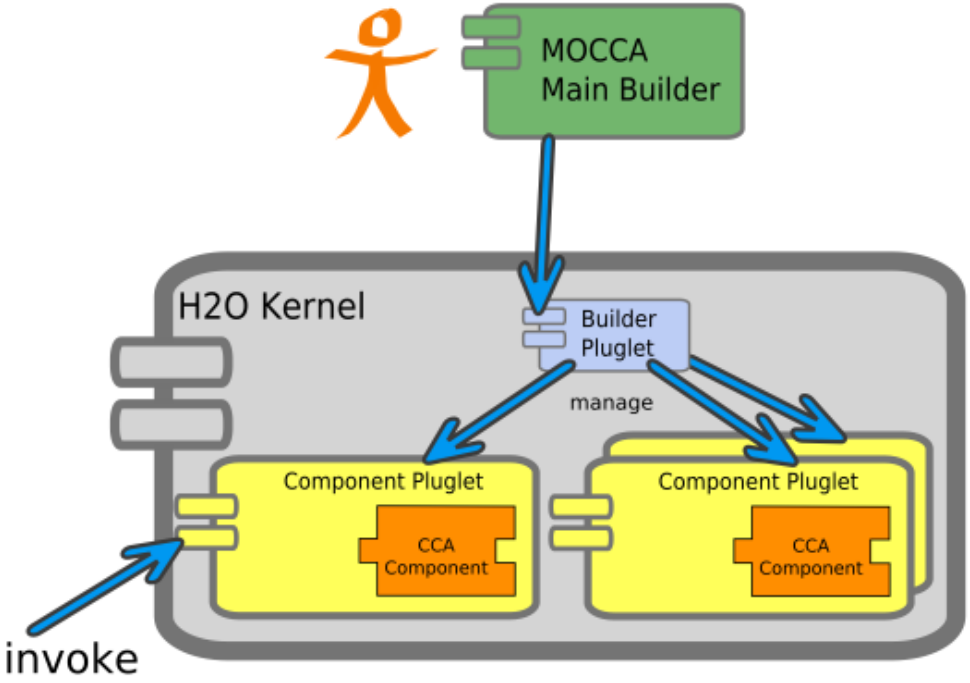
AGH

Target Environment

- H2O
  - Middleware platform for distributed computing
  - Providers setup H2O kernel (container)
  - Allowed parties can deploy pluglets (components)
- MOCCA
  - Distributed component framework
  - CCA-compliant
  - Build on top of H2O platform
  - Uses H2O security mechanisms

H2O / MOCCA structure

- CCA components mapped to H2O Component Pluglets and deployed in H2O Kernel
- MOCCA Main Builder and Builder Pluglets used for managing and combining deployed pluglets



Security Concepts in (Component) Grid Systems on Example of H2O

- Authentication
  - Described soon…
- Authorization
  - JAAS; based on authentication 'Subject'
- Communication security
  - Message integrity and confidentiality
  - RMIX framework, TLS / SSL
- Single Sign-On and delegation
- Sandboxing
- Accounting, Audit, …

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
  - Not applicable for SSO and delegation
  - Hardly possible to manage validity lifetime
  - Careless users…

Our Challenge !

Discussion of Available Solutions

Globus Security Infrastructure

- Official specification for safe communication in grid environment
- Widely deployed on production infrastructures (EGEE)
- Based on existing mechanisms:
  - Public Key Cryptography, Public Key Infrastructure, X.509, TLS
- Single Sign-On and delegation using proxy certificates:
  - based on a new key pair
  - digitally signed by the owner of the original certificate
  - with limited lifetime

MyProxy - software for managing security credentials

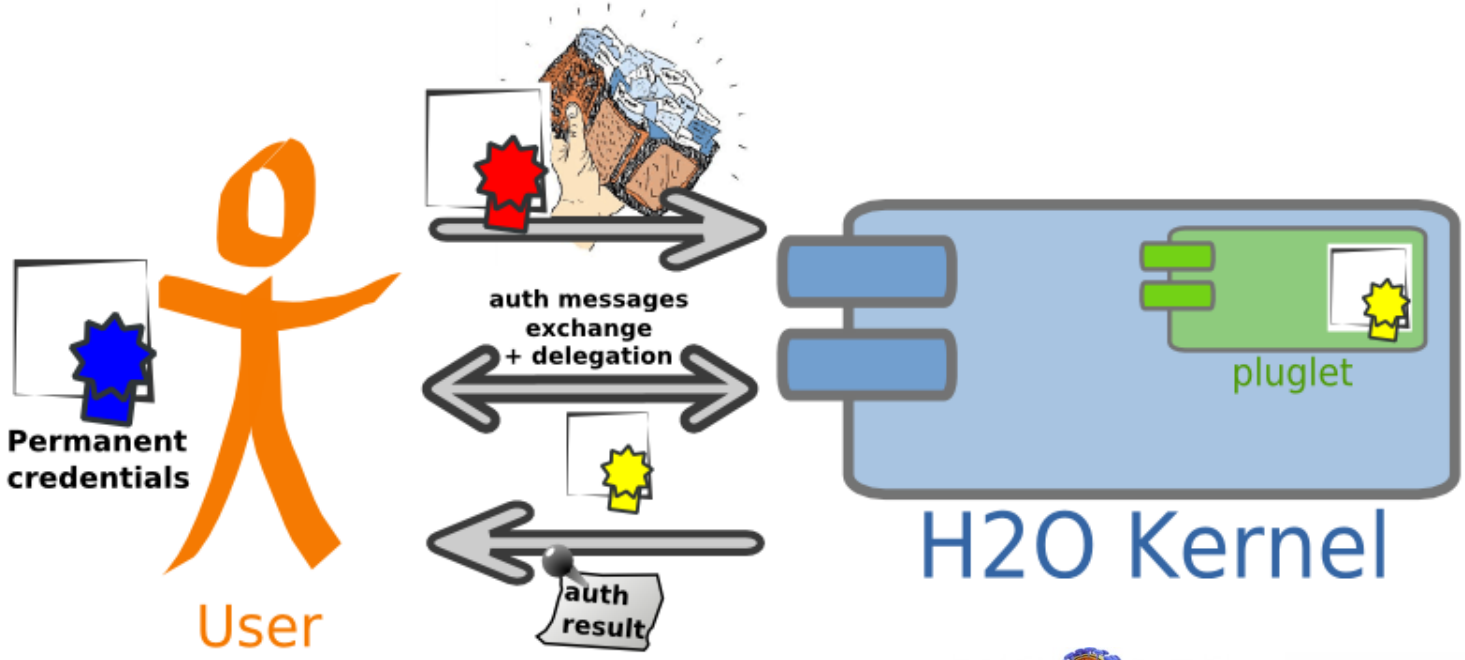
- release from the location of our permanent credentials
- use grid services from different locations and terminals

Shibboleth - Federated Web Single Sign-On framework

- no user certificates
- login requests are redirected to user's home organization
- attribute-based access control
- used mainly for integrating Web resources of educational institutions

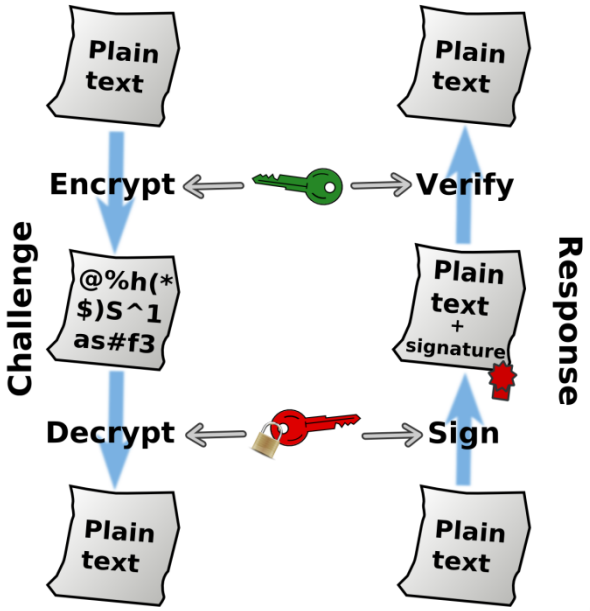
Concept of GSI Authenticator

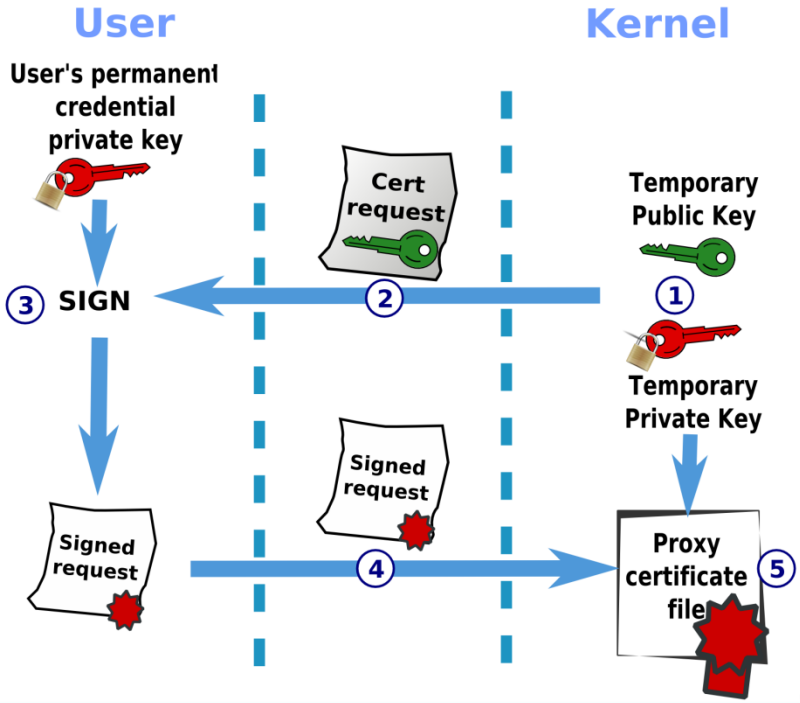
- H2O-applicable authenticator
  - based on PKI and X.509
  - compliant with GSI
  - providing delegation based on proxy certificates



Implementation of GSI Authenticator

- 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



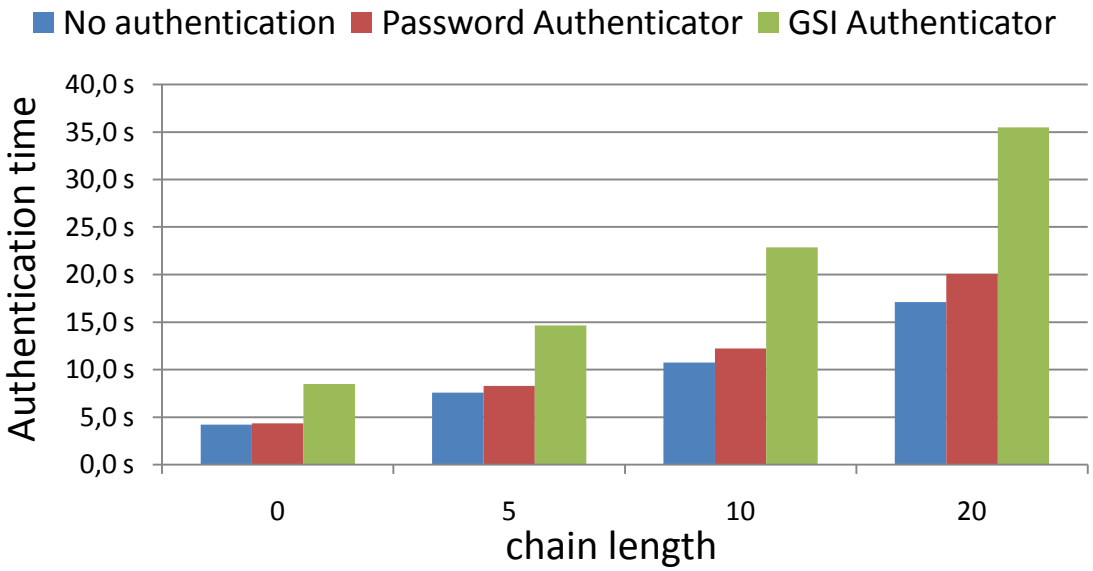


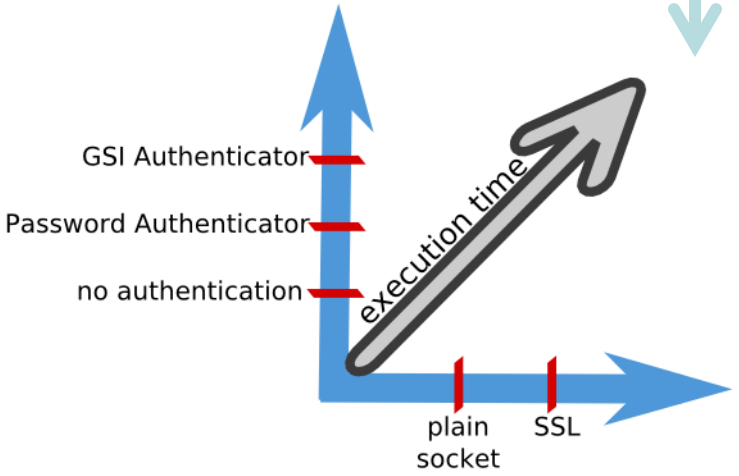
Authenticator Validation

- Verified cases:
  - Valid credentials — correct
  - The lifetime of the proxy is over — incorrect
  - The subject is unknown to the kernel — incorrect
  - The issuer is not trusted by the kernel — incorrect
  - The certificate is revoked — incorrect
- Threat analysis
  - Attacks on the system
    - Cryptanalysis attacks, network eavesdropping, session hijacking, man-in-the-middle attack
  - Attacks on the authenticator

Performance Analysis and Discussion (1/2)

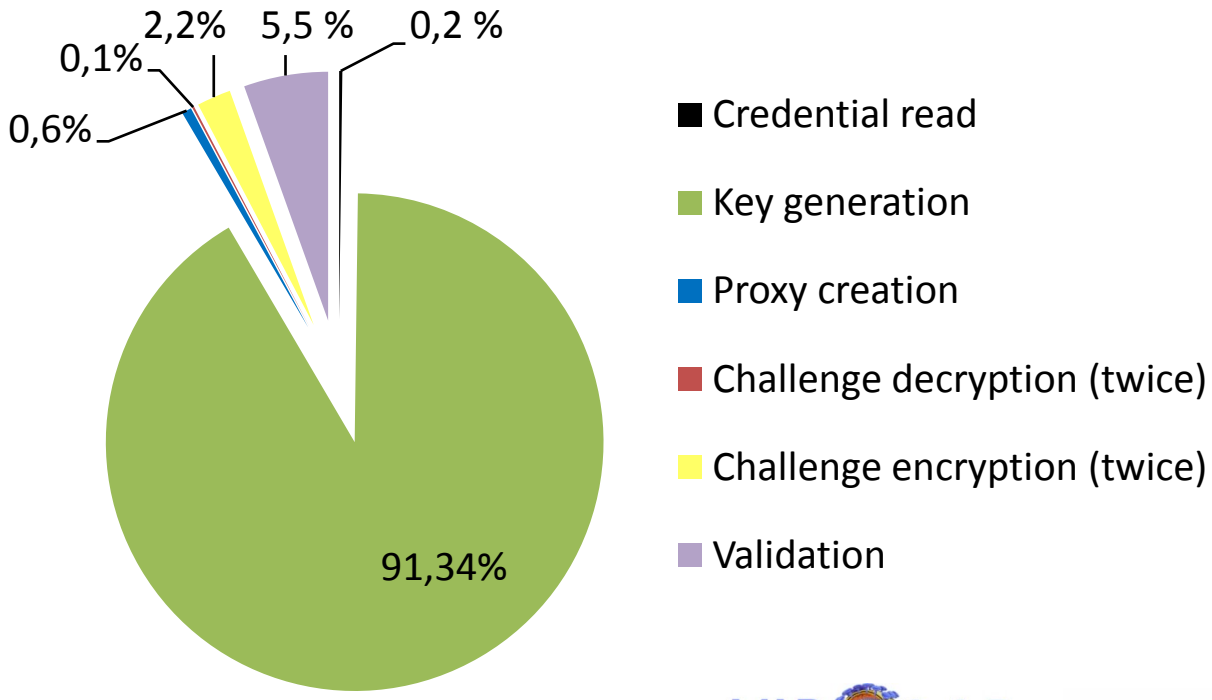
- Authentication mechanism analysis:
  - Authenticators comparison
  - SSL/TLS and server authentication overhead
  - Risk analysis
    - How much performance can we gain?
    - How much security are we ready we loose?





Performance Analysis and Discussion (2/2)

- GSI Authenticator analysis
  - Chain validation time
  - Execution time of particular elements



Summary of Work Done

- Identification and analysis of security architecture and shortages in H2O
  - ✓ **performed**
- Overview of available solutions for H2O security enhancements
  - ✓ **GSI-based solution selected**
- Concept and development of a security solution for H2O and MOCCA that would answer the presented shortcomings
  - ✓ **GSI Authenticator created, integrated with H2O**
- Proof of correctness and usefulness of the created solution
  - ✓ **performance and usage tests, threat analysis, usage examples for both H2O and MOCCA performed**
- Build, configuration and usage description
  - ✓ **provided in MSc Thesis**
- Identification of future work
  - ✓ **see next page**

AGH

Future Work

- Delegation of trust anchors
- CRL update and the Online Certificate Status Protocol (OSCP) for certificate revocation verification
- MyProxy for credentials storage
- More sophisticated authorization mechanisms

VIROLAB CoreGRID

GSI Authenticator

Please visit the following websites:

- H2O : *http://dcl.mathcs.emory.edu/h2o*
- MOCCA : *http://mocca.icsr.agh.edu.pl*
- VIROLAB : *http://virolab.cyfronet.pl*