Enhancing Data Turbine with GSI

Chris Wilk,
Matt Miller,
Pawel Plaszczak

www.gridwisetech.com
{pawel,chris}@gridwisetech.com
www.creare.com
mjm@creare.com

gridwise technologies

About this presentation

- This presentation is a result of cooperation between Gridwise Technologies and Creare, Inc.
- Please find the most recent version of the material at: www.gridwisetech.com/resources

Plan of this presentation pt. 1

1. Introduction
   - Authentication
   - Authorization
   - GSS & GSI
2. Data Turbine in brief
   - Data Turbine overview
   - Messaging middleware
   - NEESgrid overview
   - NEESgrid overview ctd.
   - NEESgrid usage of Data Turbine
   - NEESgrid security

Plan of this presentation pt. 2

3. Data Turbine and GSI
   - GSI authentication
   - GSI authorization (grid map)
   - GSI authorization (CAS)
4. Conclusions
   - Our work in wider context
   - Non-intrusive grid-enabling

Part 1

Introduction

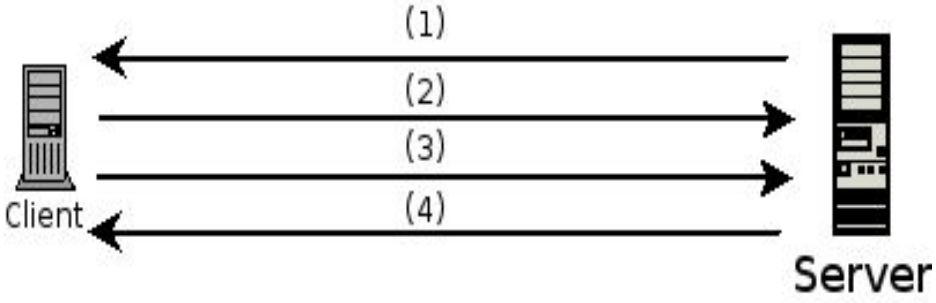
Plan of Part 1: Introduction

- Authentication
- Authorization
- GSS & GSI

Authentication

- Client- server approach (server authenticates client)
- Grid context:

  Mutual authentication



(1) client auth request
(2) client auth response - success
(3) server auth request
(4) server auth response - success

Authorization

- Client- server approach (server authorizes client)
- Grid context:

  Fine- grained and distributed authorization

  Delegation of authority (impersonation)

GSI

- **GSI** (Globus Security Infrastructure) – Globus Toolkit's implementation of GSS and more
- **GSS** (Generic Security Services) – APIs and standards
- **Grid certificates** = X.509 certificates
- **Proxy certificates** – delegation of authority

Part 2

Data Turbine in brief

Plan of Part 2:
Data Turbine in brief

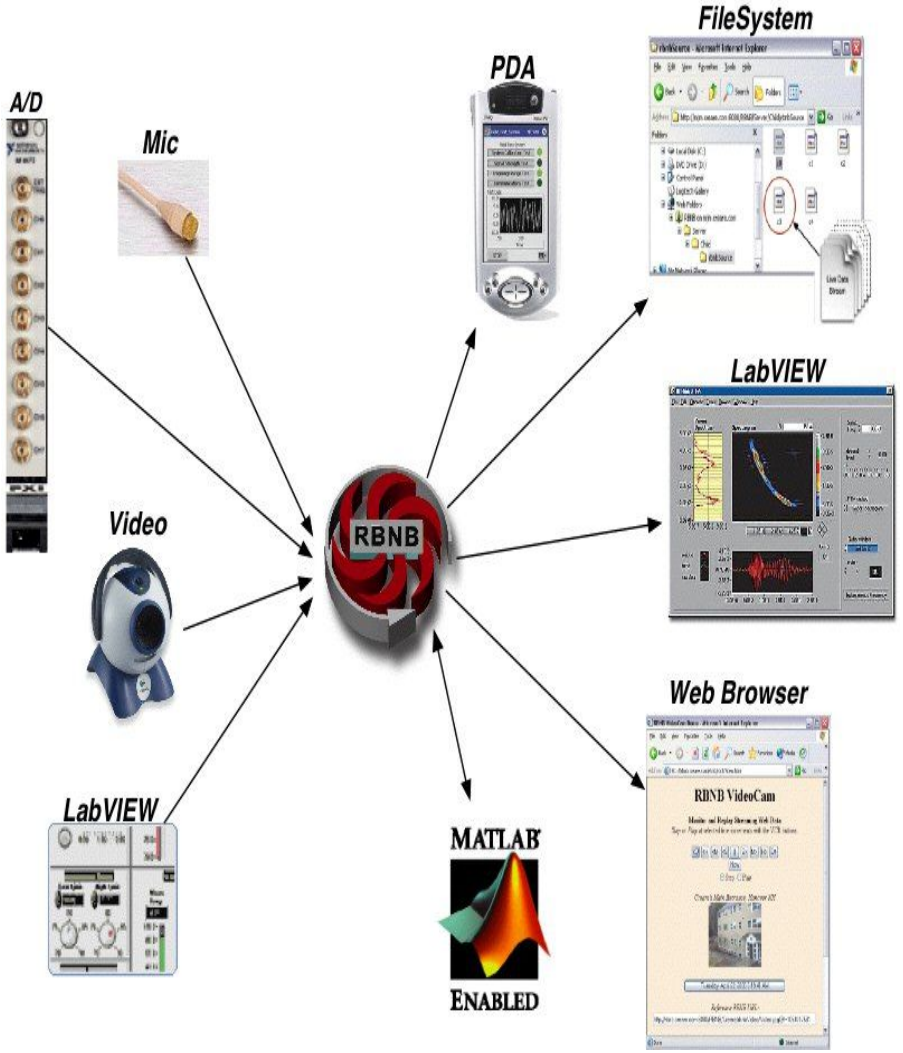
- Data Turbine overview
- Messaging middleware
- Data Turbine messaging
- NEESgrid overview
- NEESgrid overview ctd.
- NEESgrid usage of Data Turbine
- NEESgrid security

Data Turbine overview

- Created by Creare Inc.
- Called Ring Buffered Network Bus (RBNB) Data Turbine
- Provides flexible and robust solution for:
  - data management
  - data routing
  - data archival
- Described as '**messaging middleware**'

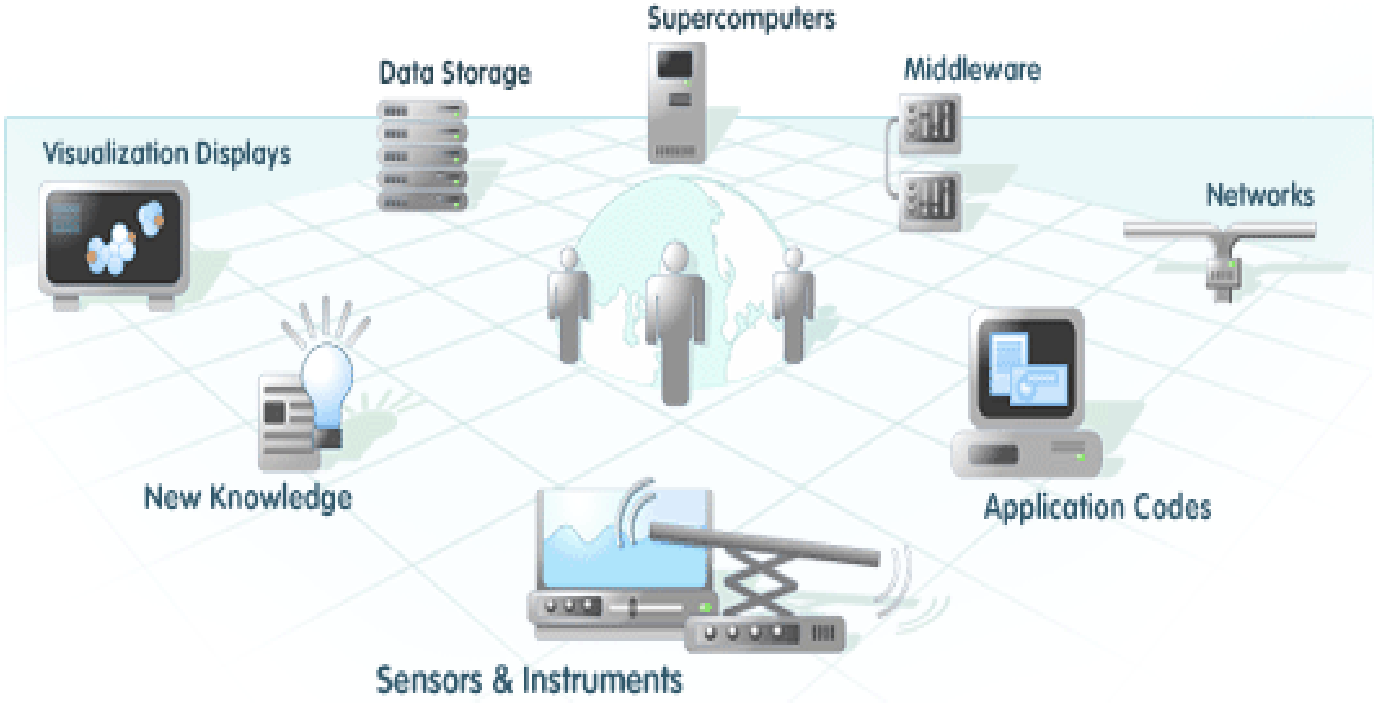
Messaging middleware

- Various data sources
- Various data destinations (sinks)
- Supported asynchronous transfers (data stored for later retrieval)



NEESgrid overview

- **NEES** – Network for Earthquake Engineering Simulation

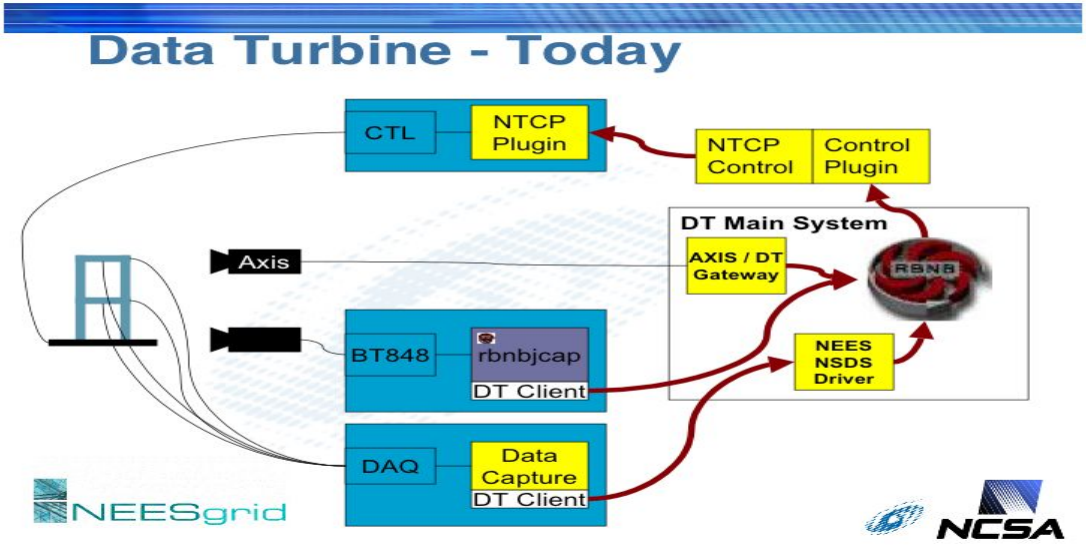


Provided by NEES

NEESgrid overview

- Links 15 laboratories across the US
- Enables collaborative engineering research
- Deploys specialised, expensive, experimental equipment
- Facilitates real-time data transfers and huge data archival
- More information at: http://it.nees.org

NEESgrid usage of Data Turbine



- Actuators controlled with NTCP plugin
- Cameras controlled with AXIS/ DT Gateway or RBNB Java Frame Capture
- Data received by DAQ with NSDS driver

NEESgrid security

- End-user access to NEESgrid provided by CHEF web portal
- CHEF performs user authentication and authorization
- Need for augmenting other NEESgrid tools with security
- Gridwise Technologies improved Data Turbine in terms of security

Part 3

Data Turbine and GSI

Plan of Part 2:
Data Turbine and GSI

- Data encryption
- Data integrity
- GSI authentication
- GSI authorization (grid map)
- GSI authorization (CAS)

Data encryption

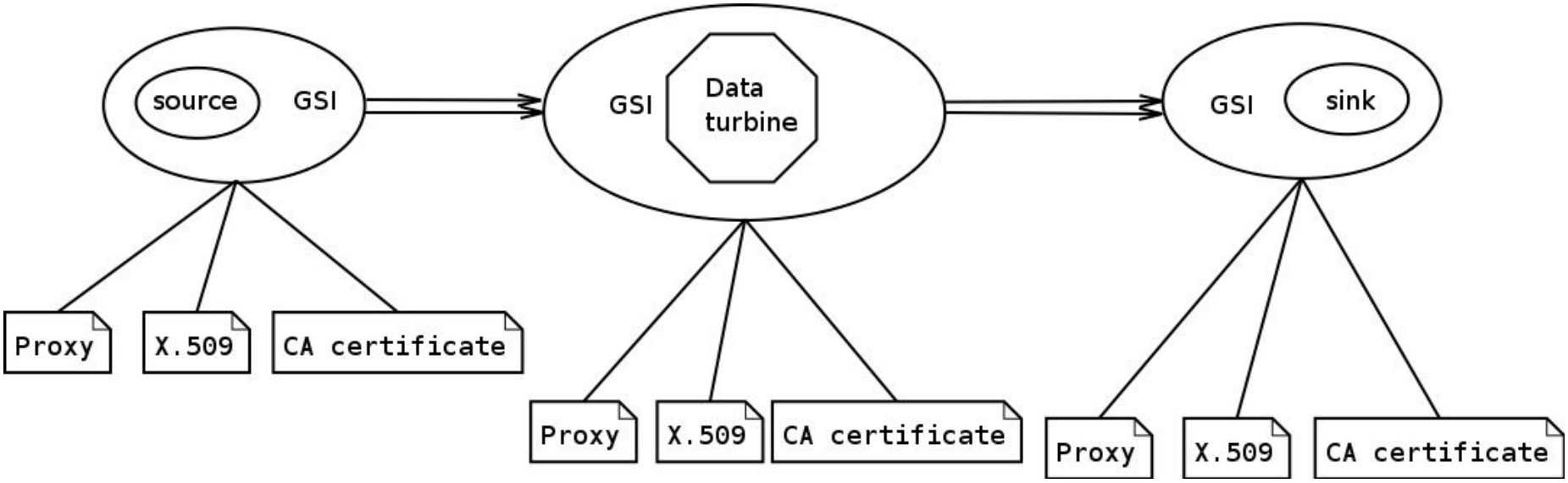
- Encryption – scrambling data using encryption key
- Data cannot be descrambled without matching decryption key
- Encryption provides confidentiality of data

Data integrity

- Message digest – one- way checksum function
- Digital signature – encrypted message digest attached to the message
- Encryption with digital signatures provides data integrity

GSI authentication

- All parties have X.509 certificates
- All X.509 certificates issued by common CA
- All parties have grid proxies
- GSI establishes encrypted communication channels



GSI authentication detailed

- Authentication disabled by default – legacy applications
- Our work delivered as security plugin
- Possibility to deploy non- GSI authentication schemes

GSI authentication detailed contd.

- Our work relies on Globus Toolkit 3.2 GSI:
  - SUN's Java Cryptography Extension (JCE) framework
  - Cryptix implementation of JCE
  - PureTLS implementation of SSL

GSI authorization (grid map)

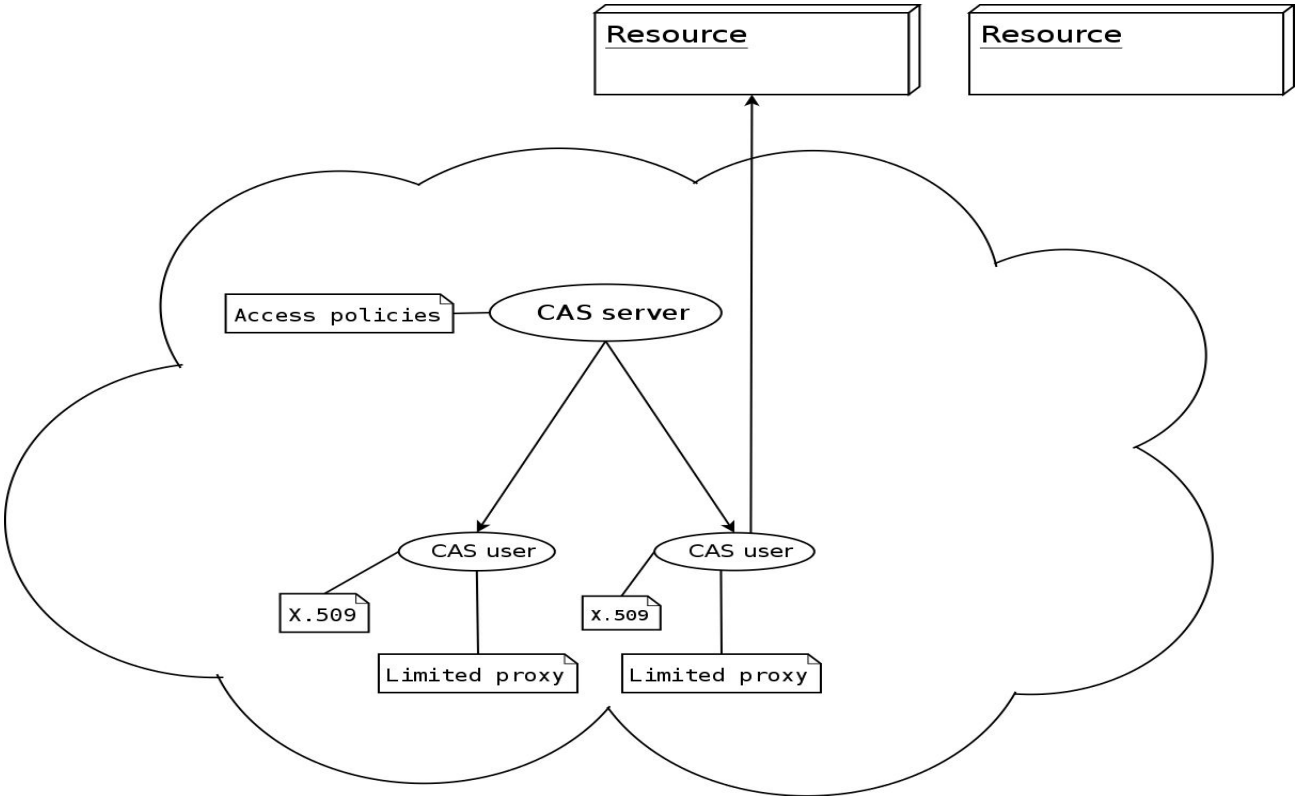
- Proof-of-concept feature
- Following GSI authentication
- **Grid map**

  simplest authorization

  list of allowed certificate subjects

GSI authorization (CAS)

- Potential future extension
- **CAS** – Community Authorization Service



Part 4

Conclusions

Our work in wider context

- We have implemented a secure, robust transport on the Grid – an alternative to GridFTP for those who do not transfer terabytes but still need security
- Security enhancements to a non-Grid product – a way to gain widespread acceptance through "Grid compliance"

Non- intrusive grid- enabling

- Conforming to open standards pays back:
  - Reusal of existing software components
  - Common interfaces help to achieve interoperability with other software solutions
- Plugin approach – non- GSI schemes possible

Thank you

- Reference materials to this project: www.gridwisetech.com/resources

- Questions, feedback are welcome: *pawel@gridwisetech.com*