Data Security on the National Fusion Grid*

J.R. Burruss,[1] T.W. Fredian,[2] M.R. Thompson[3]

[1]*General Atomics, P.O. Box 85608, San Diego, California 92126-5608 USA*
[2]*Massachusetts Institute of Technology, Cambridge, Massachusetts, USA*
[3]*Lawrence Berkeley National Laboratory, Berkeley, California, USA*

Corresponding author. burruss@fusion.gat.com

The National Fusion Collaboratory is developing and deploying new distributed computing and remote collaboration technologies with the goal of advancing magnetic fusion energy research. This work has led to the development of the National Fusion Grid (FusionGrid), a computational grid composed of compute and data resources from the three large U.S. fusion research facilities and with users both in the U.S. and in Europe. Critical to the development of FusionGrid was the creation and deployment of technologies to ensure data security in a heterogeneous environment. These solutions to the problems of authentication, authorization, data transfer, and secure data storage, as well as the lessons learned during the development of these solutions, may be applied outside of FusionGrid and scale to future computing infrastructures such as those for next-generation devices like ITER.

Collaboratory workers have adapted secure communication and authentication technologies from the Globus Security Infrastructure (GSI) to the popular MDSplus scientific data management system to create a GSI-enabled version of MDSplus. GSI is an extension to the Transport Layer Security (TLS) protocol in wide use for secure Web transactions; it provides secure and mutually authenticated communication using proven encryption technologies and public key certificates. A centralized credential manager based on the Grid middleware MyProxy server was deployed to provide the fusion scientists a convenient and secure way to manage their public key credentials. These components create a data management system capable of robust authentication and secure data transfer in a computational grid.

An authorization system appropriate for computational grids was developed to meet the security needs of computational resource stakeholders such as site security staff, systems administrators, and the scientists that develop, share, and maintain the codes and data made available through FusionGrid services. This system, known as the Resource Oriented Authorization Manager (ROAM), consists of an authorization database and easy-to-use web interface. ROAM works with GSI-enabled MDSplus or any client capable of communicating via HTTPS, and is general enough to be applied to other distributed computational environments.

TOPIC: Database Techniques and Data Handling;
Remote Participation Techniques and their Application
PREFERENCE: Oral + Poster presentation
JOURNAL PUBLICATION: Yes

*This work was funded by the SciDAC project, U.S. Department of Energy under contract number DE-FG02-01ER25455 and cooperative agreement number DE-FC02-04ER54698, and by the Director, Office of Science, Office of Advanced Science, Mathematical, Information and Computation Sciences of the U.S. Department of Energy under contract number DE-AC03-76SF00098.