



THE WHITE ROSE GRID e-Science Centre

COLAB: CROWN-C

“The COLAB collaboration is developing a new Grid Middleware System with a focus on facilitating the development of highly dependable, high-assurance service-oriented Grids, called CROWN-C.”

Introduction

Beginning in the summer of 2005, the University of Leeds (UK) and Beihang University (China) have been collaborating together to integrate the White Rose Grid (a virtual organisation which comprises partners from the three Yorkshire Universities of Leeds, York, and Sheffield) with the CROWN Grid system in China, and to develop new Grid technologies. This collaboration is called *COLAB* (Collaboration between Leeds and Beihang universities), and is co-led by Profs. J. Xu (Leeds) and J. Huai (Beihang), and managed by the EPSRC WRG e-Science Centre.

CROWN-C

The COLAB collaboration is developing a new Grid Middleware System with a focus on facilitating the development of highly dependable, high-assurance service-oriented Grids, called CROWN-C. CROWN-C is based on the CROWN (China Research environment Over Wide-area Network) Grid middleware system developed at Beihang University in Beijing, China, which itself is based upon the Globus Toolkit.

The major differentiators between the Globus Toolkit and CROWN are that CROWN places more emphasis on Grid resource management and dynamic management mechanisms at the design stage, and provides a new security architecture with distributed access control mechanisms and trust management mechanisms.

Furthermore, CROWN features integrated provenance recording capabilities; the provenance of a piece of

data is the documentation of the process that led to a given data element's creation. For CROWN-C, the following areas were targeted for improvement:

- Fault-injection based assessment facilities
- Fault-tolerance support tools
- Advanced multi-party authentication tools
- Automated trust negotiation tools

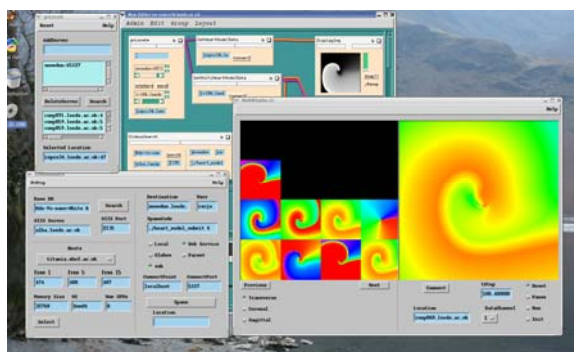
The specific technologies integrated into CROWN to address such issues are *FT-Grid* to support fault-tolerance, *CROWN-FIT* to support fault-injection based assessment, *GRID-MPA* to address multi-party authentication issues, and *ATNService* to provide automated trust negotiation. An overall architecture of CROWN-C is shown overleaf, with dependability enhancements shaded yellow.

FT-GRID

Multi-Version Design (MVD) is software fault-tolerance technique based on the principle of adjudicating the outputs of multiple redundant, diverse designs. The FT-Grid tool, developed at the University of Leeds facilitates the provision of topology-aware MVD fault-tolerant systems in a service-oriented Grid context. This is achieved through the analysis of provenance data (stored automatically by CROWN-C) to derive information about live system workflows, and perform weighted voting on MVD channels based on historical knowledge, inter-service dependence, etc.

CROWN-FIT

Fault Injection Technology (FIT) is the University of Leeds network level fault injector framework designed to work with middleware systems in order to address the dependability assessment issues. FIT contains a Fault Injection Engine (FIE) that



g-Viz running on CROWN-C

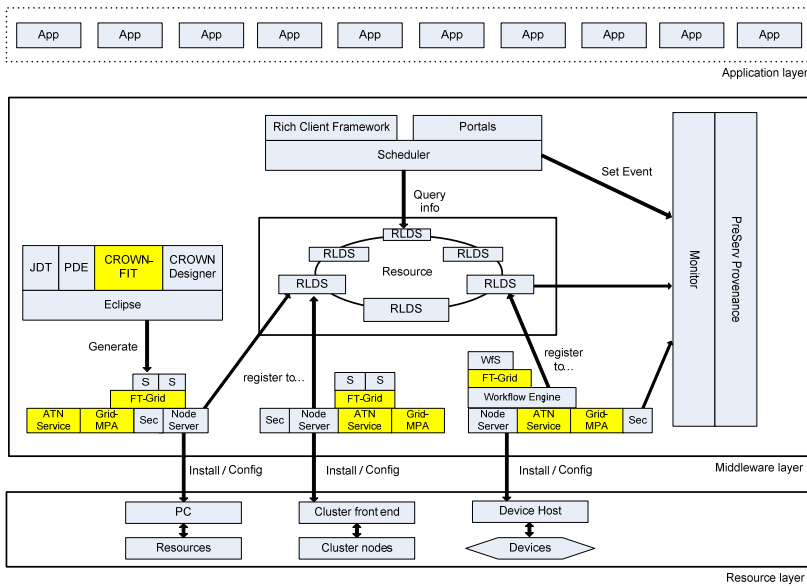


is implemented in such a way that different middleware message formats can be handled, including both text and binary. CROWN-FIT is a specific tailoring of the FIT framework, integrated into CROWN-C. CROWN-FIT is implemented as a plug-in for Eclipse, which is a platform independent framework for developing applications, and works alongside a Grid service development plug-in known as CROWN Designer.

boundary for business sessions that allows only trusted principals to join a business session; it also allows the identity of session partners to be verified through cryptographic methods. Therefore, collaborating instances within a business session can authenticate with each other by simply using their session memberships.

ATNService

Dynamically building mutual trust relationships between service requesters and service providers from different security realms is a fundamental problem, especially when considering the need to preserve their privacy. To address these issues, COLAB has developed an ATNService that supports the *automated trust negotiation* approach to enhance the Grid security infrastructure, thereby allowing flexible negotiation between strangers from different security realms. This service has been successfully implemented into CROWN-C, and complements existing Grid security infrastructures when trust is needed between unknown parties.



CROWN-C Architecture

The major innovation of CROWN-FIT is a novel fault injection mechanism that allows network-level fault injection to be used to simulate Code Insertion fault injection, whilst circumventing the need for modifications to service source code.

GRID-MPA

Dynamic authentication between organisations can be highly complex and time-consuming if some intermediate authentication paths have to be created and credentials have to be converted. Therefore, when there is no existing direct authentication relationship in place between two security realms, it is practically difficult for a system to enable any secure collaboration between services from the two security realms in a just-in-time fashion. In order to address heterogeneous cross-realm authentication issues in service-based business sessions, COLAB has developed a new authentication system entitled Grid-MPA. Grid-MPA generates a security

Current and Future Work

Work on the CROWN-C system is ongoing as part of the COLAB project; future work includes more rigorous testing of the CROWN-C system, using a wide variety of Grid applications, such as the g-Viz visualization service and the Advanced Regional Eta-coordinate Model (AREM) weather prediction tool.

Further Information

Contact:
 Dr Paul Townend (pt@comp.leeds.ac.uk)
<http://colab.crown.org.cn/>