



Project Document Cover Sheet

Project Information			
Project Acronym	SPIDER		
Project Title	Self-Protecting Information for De-perimeterised Electronic Relationships		
Start Date	1 st March 2008	End Date	31 st March 2009
Lead Institution	Cardiff University		
Project Director	Jeremy Hilton		
Project Manager & contact details	Jeremy Hilton (jeremy.hilton@cs.cardiff.ac.uk)		
Partner Institutions	None		
Project Web URL	http://spider.wesc.ac.uk		
Programme Name (and number)	e-Infrastructure		
Programme Manager	James Farnhill		

Document Name			
Document Title	<i>Project Plan, Progress Report, etc</i>		
Reporting Period	<i>for progress reports only</i>		
Author(s) & project role			
Date		Filename	
URL	<i>if document is posted on project web site</i>		
Access	<input type="checkbox"/> Project and JISC internal		<input type="checkbox"/> General dissemination

Document History		
Version	Date	Comments



JISC Project Plan

Overview of Project

1. Background

Collaborative working between multiple organisations will always require some level of information sharing and exchange. A significant amount of information belonging to an organisation will have an associated value for which appropriate protection mechanisms must be put in place in order to prevent the exposure or loss of that information. The emergence of Grid computing and Service-Oriented Architectures have led to the increasing adoption of dynamically formed, collaborative working groups known as Virtual Organisations (VOs). These Virtual Organisations (VOs), as defined in [FoKe03]¹ and [FoKT01]², provide strong motivation for investigation into the infrastructure, and in particular the security necessary to protect the information and resources shared within a VO, both while resident on local machines and when allowed to move beyond the secure boundary of a local organisational network perimeter and into the realm of the distributed VO.

Previous research in the area of access control approaches to shared information to date such as VOMS, PERMIS, ShARPE and iRODS have focused on the protection of information resources as an entity within the secure system boundary, for example, an entire classified document; access is either granted or denied using system-level access controls, or Digital Rights Management (DRM) techniques on the entity. This approach often has two major drawbacks:

- It hinders information sharing to some extent due to its limited granularity. That is, information sharing, and as a result collaborative working, is not being allowed to reach its maximum potential because large amounts of information cannot be shared due to small amounts of higher-level sensitive content within the resource raising the overall classification of the resource.
- With current DRM and system-level controls that can control access to information to some extent *after* the information has been allowed to move beyond an organisation's access control perimeter, the access control policy is permanent and cannot be modified by the owner of the information. However, there may be a change in the controls required to protect a resource, for example, the VO working group may disperse or the VO community may be changed, thus wishing to deny access to information previously shared.

This project aims to address both drawbacks by first of all designing and implementing an approach to access control which removes the fixed boundaries around the whole information resource, and places boundaries just around the sensitive content within the resource, thereby putting part of the access control policy within the information itself, and allowing the access restrictions to apply to not only the entire resource (as currently achieved), but also the content within. This has the potential to allow the sensitive content to be strictly controlled, while the rest of the information in the resource can be made publicly available. Different views of a resource can be created for varying levels of access control.

¹ [FoKe03] Foster, I., Kesselman, C., The Grid 2: blueprint for a new computing infrastructure, 2nd Ed, San Francisco, Calif.: Morgan Kaufman, 2003

² [FoKT01] Foster, I., Kesselman, C. Tuecke, S., The Anatomy of the Grid, Enabling Scalable Virtual Organisations. Intl J. Supercomputer Applications, 15(3), 2001

The second phase of the project addresses the implementation of modifiable policy, even on resources that have been stored on media outside the control of the system access control perimeter. The proposed work will review and build on current and emerging standards/approaches to Information Security that define policy and place access control restriction criteria with the information resource itself, instead of the common approach which relies on centrally controlled access to information contained within a finite perimeter (e.g. a company network).

2. Aims and Objectives

The aim of this project is to produce a mechanism for the secure sharing of information at a finer level of granularity than is currently possible. As such, this will create a contribution of understanding and solution to both the academic and commercial research and development and collaborative working communities in line with the e-Research Federated Tools and services theme of the JISC call, meeting the anticipated outcomes of a broader and more effective understanding and use of e-Infrastructure with enhanced security. Being a Welsh establishment it is also important to us that we assist in the promotion of research capacity and development of technologies for e-Research as defined by the Welsh Assembly Government's strategy for the HE sector.

The first objective is to research and analyse the associated risks for information sharing in collaborative distributed environments using some sample medical research data made available from the initial research of the CU led PET Scanner project, scheduled to be completed in 2009. Only by understanding the risk can there be a suggestion of the controls required to manage the risk, and from there the technical controls necessary can be implemented. While aiming to redefine the security requirements for VO environments, the project team are not new to the domain and are aware that technologies such as VOMS, PERMIS, ShARPE and iRODS for access control enforcement, Shibboleth for federated access management, and standards such as XACML and SAML for policy definition and decision are already available from previous research. Rather than re-inventing the wheel, the planned research and analysis will consist of an evaluation of current access control methods, technologies and standards in relation to the risk assessment carried out on the collaborative medical research environment, creating a set of requirements where current controls are lacking in comparison to the identified risks and can be built upon to improve e-Infrastructure security.

The second objective is then to take the set of requirements and implement a solution that considers these requirements, using stable open standards where appropriate, in order to provide a solution that better suits the widely distributed, expanding perimeter environments that are rapidly emerging through the adoption of VOs and collaborative working. The resulting work will provide a development to e-Infrastructure security that will allow much finer grained control over their information security and allow greater collaboration potential by increasing the amount of information that can be shared. Where previously research results or company reports were unable to be shared because they contained a small amount of information that was too sensitive to be made public, the sensitive information will be able to be classified and restricted while the rest of the information is publicly accessible.

A third objective is to improve the understanding of the collaborative working community as to how information exchange could be greatly improved by providing much finer grained access controls. The case study of testing the infrastructure with medical research data will provide a clear understanding of the technology and a use case for data access management that can be disseminated to the research communities through workshops and requests for comment to give them a better understanding of the gain in collaborative research potential that this level of fine grained control over their research information can provide. For future sustainability this solution can be built upon to production level and integrated into existing commercial enterprise architectures.

During CU's previous JISC funded projects, a high degree of time and energy has been given to collaboration with other projects and the community at large, with project staff attending JISC project meetings and attending and often speaking at both national and international events. This is important

to us in our effort to establish ourselves within the relevant research domain and to share research views with other likeminded organisations. This project will aim to continue in this vein.

3. Overall Approach

The approach will take the form of a bottom up system design from requirements capture and analysis to system implementation.

The initial risk assessment of the PET scanner project in which sensitive information is shared in a collaborative environment will provide a range of potential vulnerabilities and threats for which a set of requirements for information assurance in collaborative environments can be derived.

Following this initial step, it is important to determine what support is currently available to information managers in Information systems. By mapping the support currently available in methods and tools against the requirements derived in the earlier step, a gap analysis will be produced for which a modified model and architecture can be developed.

Using open standards and tools where available, a system architecture and application will be developed to suit the gap analysis.

4. Project Outputs

The project output will be:

- Requirements specification for access control technology in VO research environments
- Policy notation document
- Policy enforcement requirements specification
- Information classification scheme requirements and definition document
- Access control policy requirements and definition document
- VO security system architecture
- Report on usability, quality and effectiveness of the security system
- Conference paper on application of the information classification scheme and related controls to medical research information
- Conference paper on the system architecture and comparison to existing architectures that do not meet the requirements of collaborative VO information sharing to such a fine granularity.
- Software implementation of the proposed system architecture for demonstration and dissemination.
- Journal paper on the complete solution to include the initial research, analysis and risk assessment of VO research environments, information classification scheme and policy notation, and software implementation
- Release (under licence) of the first version of the software including documentation
- Presentation/Demonstration of the software internally at CU, to UCISA, to the Jericho Forum members, and to ENISA.
- Report on future development requirements and bugs
- Final Project Report
- Conference and Journal papers, once published will be published on the project web site
- Publication of all related work to website (ongoing)

5. Project Outcomes

The major outcome of this project will come from the structure of its work packages. It is a bottom-up approach to a solution that takes an existing collaborative research scenario and conducts a risk assessment, analysis and requirements definition prior to the development of technical controls. This generates a belief of defensibility to any statements or requirements stated in the solution and the various reports and papers.

The nature of the project is that it has a final software deliverable which is a practical outcome that can be demonstrated to the academic and commercial communities through CU's various connections. Further outcomes from this will be a contribution to the electronic access control research field and a sustainable development plan for integrating the resulting solution into existing tools and services.

Apart from the conference and journal papers that are produced in the work plans, CU has links to the UCISA, ENISA and Jericho Forum board. The project results and related software will be demonstrated to the each organisation, with particular interest to the Jericho Forum whose members are generally CIO level from large organisations. There has been previous interest from some members in the kind of solution proposed in this work and when results are demonstrated, it is expected that interest will rise and future research and commercial integration may occur.

6. Stakeholder Analysis

Stakeholder	Interest / stake	Importance
Cardiff University	Project Facilitator	High
JISC	Project Funder	High
Academic Community	Similar research areas	Medium
Jericho Forum	Working group in area of research	Medium

7. Risk Analysis

Risk	Probability (1-5)	Severity (1-5)	Score (P x S)	Action to Prevent/Manage Risk
Loss of core project staff	1	2	2	The CU research team have strength in depth and any loss of contribution from core project staff could be distributed to other capable staff.
Failure to get papers published	2	1	2	This is a contemporary and interesting area of research and should be relevant to upcoming conferences and journal publications. If not, the research will be disseminated through demonstration to ENISA, Jericho Forum and other interested parties, and case study reports.
Failure to find use case for proof-of-concept	1	3	3	The failure to find a use case would impact the credibility of the work as proof-of-concept could not

				be demonstrated. However, CU has its own internal information management infrastructure which could be used for demonstration should the failure occur
Failure to deliver suitable technical solution	1	4	4	The project would be a failure if a technical solution were not produced but regular project progress meetings and the deadlines set for publication of progressive work, along with the technical expertise and experience at CU should ensure that the deadline is adhered to and a solution produced

8. Standards

Name of standard or specification	Version	Notes
None defined as yet		

9. Technical Development

Technical development will be informed by the earlier assessment and analysis of the problem space. The risk assessment of the medical healthcare information sharing environment, followed by the requirements analysis and existing systems analysis will create a specific set of requirements that the technical development should fulfil.

The development of a technical solution will follow a modular approach in order to test and implement each requirement a stage at a time, and to enable traceability and scalability of implementation in future development.

Standards will be used where appropriate, particularly in the development of security policy and software testing.

10. Intellectual Property Rights

The published research will be available for use by the further and higher education community. Software will be released for evaluation and further research use by the further and higher education.

Project Resources

11. Project Partners

None

12. Project Management

Though this is an internal CU project, it is cross-disciplinary and as we wish to implement the results, the approach developed must be capable of implementation within the CU infrastructure. Consequently we will establish a steering committee with members from Corporate Compliance, Information Services and Computer Science. Due to the anticipated benefit to UCISA, a UCISA expert

Project Acronym: SPIDER
Version:0.1
Contact:p.burnap@cs.cardiff.ac.uk
Date:01 June 2008

will also be invited to join the Steering Committee. We would also seek an appropriate input from JISC in an advisory capacity, or as a member of the steering committee.

The Steering Committee will meet at the beginning and end of the project, as well as at suitable milestones to be decided at the beginning of the project. Appropriate documentation in accordance with PRINCE 2 will be developed; the minimum being product descriptions and a full project plan, to be agreed at the first Steering Committee meeting.

Jeremy Hilton – Principal Investigator
Jeremy.hilton@cs.cardiff.ac.uk

Pete Burnap – Lead Researcher
p.burnap@cs.cardiff.ac.uk

Anas Tawileh – Researcher
anas@tawileh.net

Rhys Smith – Researcher
r.o.smith@cs.cardiff.ac.uk

13. Programme Support

It would be very useful to be informed of any related research, conferences and future funding or dissemination opportunities that JISC becoming aware of.

14. Budget

See Appendix A

Detailed Project Planning

15. Workpackages

See SPIDER-WP-Detail

16. Evaluation Plan

Timing	Factor to Evaluate	Questions to Address	Method(s)	Measure of Success
Sep 08	Requirements specification	Were the requirements accurate and complete	Report on usability, quality and effectiveness of the security system	Whether the security system fulfils some of the flaws/shortcomings with current information security
Sep 08	Information Classification Scheme	Was the scheme usable, flexible and verbose enough?		Whether it was usable within the security system with several different information sources
Jan 09	Software Implementation	Is the software usable and does it fulfil the requirements spec	Presentation/Demonstration of the software internally at CU, to UCISA, to the Jericho Forum members, and to ENISA.	Should be able to demonstrate a fulfilment of the initial requirements

17. Quality Plan

Output	Quality criteria	QA method(s)	Evidence of compliance	Quality responsibilities	Quality tools (if applicable)
March 2008	Software fit for demonstration	Test and evaluation by project team and associates at Cardiff	Test Results	PB, AT	None

18. Dissemination Plan

Timing	Dissemination Activity	Audience	Purpose	Key Message
Sep 08	Conference paper on application of the information classification scheme and related controls to medical research information	Information Security Researchers/Developers	To publish the concepts of the research	Information Classification requirements
Dec 08	Conference paper on the system architecture and comparison to existing architectures that do need meet the requirements of collaborative VO information sharing to such a fine granularity.	Information Security Researchers/Developers	To publish the concepts of the research	Gap in existing VO security
Jan/Feb 09	Journal paper on the complete solution to include the initial research, analysis and risk assessment of VO research environments, information classification scheme and policy notation, and software implementation	Information Security Researchers/Developers	To publish the concepts and results of the research	Solutions to gaps in existing VO security
Feb 09	Presentation/Demonstration of the software internally at CU, to UCISA, to the Jericho Forum members, and to ENISA.	CU, UCISA, Jericho Forum, ENISA	To disseminate the solution in its practical entirety	These are our project results. Feedback.

19. Exit and Sustainability Plans

Project Outputs	Action for Take-up & Embedding	Action for Exit
Requirements specification for access control technology in VO research environments	Publish papers and join related working groups to enhance community thinking and involvement	Continue contact with working groups
VO security system	Publish papers and join related	Continue contact with working

architecture	working groups to enhance community thinking and involvement	groups
Software implementation of the proposed system architecture demonstration for and dissemination.	Publish papers and join related working groups to enhance community thinking and involvement	Fully document software. Look for further funding to develop further software functionality and implement in new domains

Project Outputs	Why Sustainable	Scenarios for Taking Forward	Issues to Address
Software deliverable	Can be developed further, modified, and applied in new domains	Further funding. New requirements analysis. Ongoing emerging risk analysis	How to keep up with new issues in information security

Appendixes

Appendix A. Project Budget

			Year 2007/08	Year 2008/09	Full Cost of Project	Requested Funding
Directly Incurred Costs						
Staff Costs			3482.08	38302.92	41785	34785
Travel & Sub. UK			83.33	916.67	1000	1000
Travel & Sub.OS			250	2750	3000	3000
New Equipment			3000	0	3000	3000
Recruitment/Advertising			0	0	0	0
Consumables			0	0	0	0
Other Costs			0	0	0	0
Audit Fees			0	0	0	0
Sub - Contract			1100	12100	13200	13200
Directly Allocated Costs						
Investigators Costs			844.33	9287.67	10132	10132
Advance Research Computing			0	0	0	0
Use of School Equipment			0	0	0	0
Estates Costs			917.67	10094.33	11012	11012
Other DA Costs			0	0	0	0
Indirect Costs			2814.17	30955.83	33770	33770
Exceptions			0	0	0	0
Staff Project Studentship			0	0	0	0
Other Costs			0	0	0	0
TOTALS			12491.58	104407.42	116899	109899