Meeting with Dr. Simon Grange, University of Southampton
Georgetown University, Wednesday, 10 March 2010

Dr. Grange is a member of the "research staff (Visiting Researcher) in Learning Societies Lab School of Electronics and Computer Science, University of Southampton."

He writes: "Having trained as a Doctor, and then as an Orthopaedic Surgeon in the UK, with various fellowships and opportunities studying abroad, it is apparent to me that we can do much to enhance the traditional medical environment for research, education and clinical practice. I have developed an interest in surgical simulation and my thesis explored the subject of embedding such technologies into virtual learning environments".[1] He is principal investigator on several JISC projects.

Dr. Grange had expressed an interest in the security of networked communications that involves universities and hospital and medical center information.[2] The focus of the discussion turned to further development and implementation of authentication and authorization. Dr. Grange had expressed an interest in using Shibboleth authentication. The UK universities now use Shibboleth authentication for access to journals. Authorization is assumed for anyone who has a university-issued credential. Dr. Grange would prefer to extend this infrastructure rather than create "yet-one-more" security system.

Because of Georgetown University's participation in the development and implementation of Shibboleth—including pilot projects with the U.S. National Institutes of Health and National Science Foundation—and in distributed computing, this meeting was scheduled with University Information Services staff. The meeting with Dr. Grange included Principal Technologist Charlie Leonhardt, staff in his Scholarly Systems Group Arnie Miles, Grid Middleware Architect, Brent Putman, Middleware Systems Analyst, and Jim Farmer, Coordinator.

The Challenge

Projects that Dr. Grange leads often include several universities, hospitals, and medical centers. These collaborations, crossing institutional boundaries, require a nuanced authorization scheme more complex than available from current permissions software as implemented for institutional use. The security system must also support "overrides"—access to a patient's records during a medical emergency. The security system must also comply with all privacy laws, regulations and accepted practices for personal and medical data, and protect the institution. To facilitate management security systems should be able to exchange security data across networks as well as institutions.

Dr. Grange is currently a principal researcher for the VRE 3 project VRIC - Virtual Research Integration Collaboration. "The aim of the project is to build a framework for the integration of basic science and clinical research to manage research lifecycles and allow for integration of

---

[1] From Dr. Grange's biography at www.ecs.soton.ac.uk/people/sg01v.
[2] From his discussion with Frederique van Till, Programme Manager, e-Research, for the Joint Information Systems Committee (JISC) following the VRE Meeting, 24 February 2010 at the University of London.

scientific approaches throughout these lifecycles into the everyday work practice of the consortia that manage translational clinical research."[3]

The Discussion

Dr. Grange began the discussion by listing needs for network security in terms of use cases. These included a researcher participating in clinic trials, an emergency room physician with a critically injured patient, and a researcher needing access to a computing service or data available on a grid (distributed computing). The discussion can be summarized:[4]

1. Authentication using different systems – Arnie Miles commented access computing services or data on another network is needed. Although Shibboleth serves a major share of the higher (tertiary) education, some use other methods of authentication. Similarly hospitals, medical centers, and other networks may use other methods.

    Miles said his Thebes distributed computing network was developing software to exchange the SAML assertions from one source into the SAML assertions needed by another. This includes the exchange of Shibboleth assertions to public key certificate assertions. Miles said so far they have been able to change among all of the most frequently used methods of assertion. This means a user would not need to have another "account" to use a computing service or data that required SAML assertions for other protocols.

2. Joint authorizations – Dr. Grange said often hospitals and medical centers, for compliance and liability concerns, want to approve authorizations for project staff to have access to their records (which may include patient records). That is, the project must identify the user and authorize access subject to approval (second authorization) by the hospital or medical center. The discussion suggested this could be a function of the authorization software: certain authorizations would require an authorization from a third party. The authorization software would have to seek this additional authorization. This could be incorporated in a SAML assertion in the response of the original authorization engine. The source of computing services or data would require both authorizing assertions to permit access

3. Overrides – There was general agreement this would have to be a special authorization that both authorized access and recording by the required computing service or data of the identity of both the requester and the records accessed. Some review of how this authorization is done is current patient records system, or systems with similar security requirements, could yield a "best practice" than could be incorporated.

4. Data security – Some datasets have limited distribution. The issue is how to incorporate this into data archiving software or repository. Putman said RDF (Resource Description Frameworf\k) has this capability of linking data sets to the association restrictions

---

[3] From the project description "VRIC - Virtual Research Integration Collaboration" [www.jisc.ac.uk/whatwedo/programmes/vre/vric.aspx].
[4] The order of the discussion topics have be changed to improve presentation.

(authorization requirements). He further said RDF metadata is supported by the Fedora open source repository.

5. HPC (High performance computing) – Arnie described the HPC technology that had been incorporated into the Thebes network. This included security—Shiboleth, SAML2, and Web Services—that will be extended to function for administrative applications.

Other Objectives

In addition to responding to these specific use cases, there was general agreement the use of Shibboleth for research in the U.K. would increase the use and strengthen Shibboleth infrastructure in the U.K. At the same time it would reduce the costs of development and implementation in the environment Dr. Grange described.

Principal Technologist Charlie Leonhart said developing and implementing the proposed network would also benefit the InCommon federation through additional users. The number of users is important since the value of a network is proportional to the square of the number of users. [5]

Reflections

As directed by Dr. Grange, the discussion focused on identifying, integrating, and implementing technology from current VRE (virtual research environment) and other JISC Projects. These are principal objectives of the JISC (Joint Information Systems Committee UK) VRE Phase 3 projects. The goal is to provide researchers with a more productive environment in an era of openness, collaboration, and vast digital resources.

---

[5] See Metcalfe, Robert. (1996: 30 May). Metcalfe's Law recurses down the long tail of social networking, VCMike's Blog. Waltham, Massachusetts USA: Polaris Venture Partners. See also Metcalfe, Robert. (1996: 30 May). The Internet After the Fad: Remarks of Dr. Robert Metcalfe at the University of Virginia. Washington DC, VA USA: Monticello Memoirs, The Smithsonian Institution.