Shibboleth and SPNEGO auto login

Abstract

This report briefly looks at incorporating SPNEGO auto login support for Shibboleth. This would enable auto-login to any University systems protected by Shibboleth. This report aims to detail the steps required to develop a SPNEGO Handler for Shibboleth. This report also details the progress we have made thus far with regards to providing SPNEGO auto-login to Shibboleth 2.1.

1.1 Introduction

When considering use cases for Shibboleth which are internal to an institute automatic login or "true single sign on" for users becomes a very desirable feature. An illustrative use case of this are student facing institutional portals. The usability and user acceptance of portals is much enhanced when on campus users, who have already logged into their computer, are automatically logged into a web based portal rather than having to log in again. The desirability of this feature has been discussed at length on Shibboleth mailing lists and in single sign on discussions at internet2 conferences. It has been identified here in Newcastle University as a prerequisite to a rich personalised portal deployment. The convenience of auto login combined with Shibboleth's ability to gather a rich set of attributes from diverse institutional data stores enables a compelling set of portal personalisation and information targeting scenarios.

Newcastle University, as part of the GFIVO (http://gfivo.ncl.ac.uk/) project, looked at the feasibility of incorporating this functionality into Shibboleth. The core objective of this work was to look at the feasibility of developing a SPNEGO Authentication Handler for Shibboleth. This would enable "out of the box" auto log-in into any systems protected by Shibboleth. This would greatly enhance the desirability of Shibboleth to large sections of the HE community. SPNEGO is functionality present in most modern browsers that allows Kerberos tickets on the users computer to be communicated to a web server allowing the web server to seamlessly login the user.

As a starting point we looked at CAS (http://www.ja-sig.org/products/cas) as it is a WebISO system that provides SPNEGO support. One of the benefit of CAS is that it's architecture has a flexible series of authentication handlers and those handlers have been developed in a modular way. The CAS distribution contains modular authentication handlers for LDAP, Kerberos + SPNEGO and a variety of other techniques.

While Shibboleth can be deployed with CAS to provide the login and SPNEGO support it would be desirable for this functionality to be integrated into Shibboleth directly as a login handler. There are two reasons for this. Firstly many sites new to Shibboleth seem to find the need to research, choose and deploy a WebISO system like CAS a step too far, packaging a fully functional login handler with Shibboleth would remove a barrier to take up. Secondly the new login flows available in Shibboleth 2.1 would benefit from having the log on system integrated into Shibboleth directly.

Newcastle uses Microsoft's Active Directory as a username and password store and Kerberos Domain controller. The ubiquity of Active Directory in UK HE and FE sites means that lessons learned in Newcastle have value to the rest of the community. Also since the Active Directory in this case acts as a Kerberos domain controller the lessons learned have direct applicability to alternative sites that use other Kerberos implementations and password stores (openLDAP, SunONE etc) .

1.2 Leveraging CAS SPNEGO code

The source code for the CAS SPNEGO handler can be found in the CAS 3.2.1 server distribution at **cas-server-3.2.1\cas-server-support-spnego\src\main\java\org\jasig\cas\support\spnego** Note: the latest CAS 3.3 does not seem to build so 3.2.1 is the best version to work with.

CAS itself uses the SPNEGO implementation code from the JCIFS sub project of the samba organisation (http://jcifs.samba.org/). JCIFS is a Java implementation of Window's CIFS/SMB networking protocol. The CAS SPNEGO module integrates the SPNEGO support provided by JCIFS into CAS via the Spring Framework. This framework is also used by Shibboleth 2. The modular nature of CAS authentication plugins means that the SPNEGO support of CAS is separated from the rest of the CAS server codebase which should make it easy to identify and repurpose.

Licence issues should not be an impediment, JCIFS is distributed under the GNU Lesser General Public Licence (LGPL) so Shibboleth 2 should be able to incorporate it's libraries without altering Shibboleth's Apache 2.0 licence. CAS itself is distributed under the permissive JA_SIG licence. It is therefore likely that the CAS SPNEGO authentication handler is an excellent candidate to be easily ported over to the Shibboleth code base and should be used as a template for the development of a Shibboleth SPNEGO authentication handler.

It is clear from reading the CAS and Shibboleth Development guides that Spring development knowledge is required. A guide on developing Shibboleth extensions can be found at https://spaces.internet2.edu/display/SHIB2/DevelopmentDocs Unfortunately, we in Newcastle University do not have the necessary expertise in Spring to develop a Shibboleth SPNEGO Handler so can't undertake this work.

1.3 Conclusions

SPNEGO auto login support would be a very desirable feature to add to Shibboleth 2.2 indeed it is marked as "desired, will be included if there is time" on the roadmap https://spaces.internet2.edu/display/SHIB2/Shibboleth+2.2+Roadmap . It is the opinion of the GFIVO project that prioritisation of this feature would be highly desirable, indeed we recommend that JISC look at funding a small project to add this functionality. It is a feature that if it were available would drive the deployment of Shibboleth as an internal institutional sign on system as well as just a external federated sign on system. The ability for Shibboleth 2 to integrate directly out of the box with Active directory to provide class leading auto login. This would be of massive benefit to the high proportion of institutes in the UK federation who use the Active Directory as their username and password store. While we can’t say exactly how much work would be involved without doing the actual integration, the initial scoping carried out by the GFIVO project and outline in this document strongly suggests that the existing CAS SPNEGO codebase would be a excellent starting point.