CIC Guest Wireless Report and Recommendation

C·I·C COMMITTEE ON INSTITUTIONAL COOPERATION
www.cic.net

1819 South Neil Street, Suite D
Champaign, IL 61820-7271
217.333.8475
www.cic.net

September 2010

Contents

Project Participants

Rahul Doshi ♦ Indiana University

Mike Grady ♦ University of Illinois at Urbana-Champaign

Jim Green ♦ Michigan State University

Keith Hazelton ♦ University of Wisconsin - Madison

Neil Johnson ♦ University of Iowa

Jason Mueller ♦ Indiana University

Gary Rogers ♦ University of Iowa

Jeff Utter ♦ Michigan State University

Alan Walsh ♦ Indiana University

1 Background

In August of 2009, the CIC Identity Management Task Force recommended to the CIC CIO's three Identity Management (IdM) projects designed to improve the ability of CIC institutions to collaborate. Among those projects was Guest Wireless. From the August 20 report:

> ***"As wireless networks have proliferated across the landscape of the CIC institutions, so have the complex means of obtaining access to them. Every CIC institution provides a different mechanism for obtaining access to the system, ranging from totally open to short-lived paper-based credential provisioning schemes. As all of the CIC institutions have agreed to join InCommon and are working toward using Shibboleth for federated access to institutional resources, it is our belief that "Shibbolizing" the guest wireless services at our respective institutions is the proper course to follow.***
>
> ***Identity and Access Management (IAM) focused problem statement: It is the goal of this project to allow CIC constituents to leverage their home institutions' Identity Providers to gain access to guest wireless services at the institution they're visiting. That is, a Faculty member from the University of Minnesota should be able to connect to the guest wireless service at the University of Iowa using his/her UMN Internet ID and Password. This will allow ease of access to the network, while still providing an acceptable amount of accountability and security to the provisioning process."***
>
> *[https://cicme.cic.net/sites/cicit/idmgmt/Documents/Reports/Project%20Proposal%20for%20CIOs.docx]*

2 Activities

Since August, the CIC Wireless Group has assessed the feasibility of the proposed solution, (i.e. using federated web application access standards, profiles (SAML, Shibboleth) and software to meet our requirements. Alternative solutions have also been examined.

Specific activities:

1. Met with the University of Wisconsin-Madison Networking and Middleware teams to assess the feasibility of a SAML/Shibboleth-based solution.

2. Attended CIC wireless networking and network directors meetings in Chicago to present the project and solicit feedback. *(November 2009)*

3. Attended a webinar on eduroam that resulted from conversations at a previous Research University CIO Conclave (RUCC) meeting. [https://connect.case.edu/p12686352/] *(November 2009)*

4. Contacted Louisiana State University regarding their experience with eduroam. [https://cicme.cic.net/sites/cicit/idmgmt/IdM%20Wiki/20100120%20-%20Conversation%20with%20LSU.aspx]. *(January 2010)*

5. Participated in regular conference calls with U.S. eduroam participants and InCommon to discuss administrative and technical issues related to deploying eduroam in the U.S. The current goal of this effort is to create a proposal and business case that will convince InCommon to take on the organizational and administrative duties necessary to make eduroam a viable service for U.S. institutions.

   Those participating include:
   - John Borne – Louisiana State University
   - Hector Rios - Louisiana State University
   - Mike Grady – University of Illinois
   - Michael Corn - University of Illinois
   - Jeffery Gumpf – Case Western Reserve University
   - Philippe Hanset – University of Tennessee-Knoxville
   - David Worth - University of Tennessee-Knoxville
   - Paul Caskey – University of Texas System
   - Keith Hazelton – University of Wisconsin-Madison (chair)
   - Steve Devoti – University of Wisconsin-Madison
   - Ed Kiefer – Cornell University
   - John Krienke - InCommon
   - Dean Woodbeck - InCommon
   - RL Morgan – MACE, InCommon TAC
   - Ken Klingenstein – Internet2

6. The University of Illinois has piloted eduroam (now in beta). Please see the following information provided by Mike Grady: [https://cicme.cic.net/sites/cicit/idmgmt/IdM%20Wiki/Notes%20on%20eduroam%20deployment%20at%20University%20of%20Illinois%20at%20Urbana-Champaign.aspx]

3 Findings

The feedback from the CIC Wireless group and individual campus meetings with network engineering and IdM teams has been generally negative towards a SAML/Shibboleth-based solution. Here are the specific findings of the group:

1. With the current technology available to us, a SAML/Shibboleth-based solution requires the use of a captive portal. Most have indicated a strong desire to eliminate or greatly reduce the use of captive portals for network authentication.

2. Even if a captive portal solution were deemed acceptable, two or three firewall rules would need to be maintained for each federation partner to allow outbound access to the partner's IdP and login page.

3. The University of Wisconsin investigated using URL filtering (e.g. allow all outbound to .edu). Their network engineers do not believe that currently available solutions can support required throughput.

4. A simple solution would be to provide open wireless on parts or all of our campuses. Currently, Michigan State and Minnesota provide varying degrees of open wireless. Wisconsin is investigating open wireless as part of their wireless infrastructure upgrade project. Though open wireless would technically meet the CIC Guest Wireless objectives it is clear that researchers in particular will need access to VPNs and other secure networks. Open wireless will not address this issue.

5. Though the drawbacks of a SAML/Shibboleth-based solution might be addressed within the CIC, thus allowing us to meet our stated objectives, it is unlikely such a solution will be adopted by all those we wish to federate with.

6. We could support visitors to our campuses as long as their home institutions were members of InCommon. This would work well for visitors with U.S. home institutions but not for international visitors.

7. When our affiliates travel to institutions outside of the CIC, if the institution does not support authentication via SAML/Shibboleth (likely case), our users will not automatically gain access.

8. Eduroam is the solution of choice for federated network access in Europe, Australia and Asia; has momentum in Canada and is gaining traction in the U.S. Obstacles to eduroam adoption in the CIC (and the U.S.) are its requirement that the institution have in place an 802.1x compliant

infrastructure and the lack of U.S. administrative and operational structures. [http://www.eduroam.org/]

9. Many institutions already have some or all 802.1x capable hardware deployed though they may still be using a captive portal. Others, e.g. Wisconsin, are in the process of upgrading their hardware and have plans to move to 802.1x for authentication.

10. Eduroam has appeared on the radar of InCommon and has been discussed at the Steering Committee and Technical Advisory Committee. We are optimistic that InCommon will agree to provide the administrative functions necessary to make eduroam a reality in the U.S.

4 Recommendations

1. All CIC institutions review their stance on open wireless and pursue opening some or their entire wireless network as feasible.

2. Commit, in the next few months, to eventually supporting eduroam. Specifically:

    a. Gain and document commitment from appropriate leadership at your campus.

    b. Contact the University of Tennessee-Knoxville and express interest in joining eduroam U.S. It seems reasonable to conclude that the more interest expressed the more likely it is that InCommon will take this on. http://www.eduroamus.org/eduroam_us_institutions

3. Engage your network and/or IdM groups and set up an eduroam beta. As Mike Grady has relayed, technically this is very straightforward and does not require a large expenditure of resources.

    a. http://www.eduroamus.org/peering_request

    b. Discuss with your networking and/or IdM groups your current RADIUS infrastructure's support for RadSec. Though it is unclear whether RadSec will be required, optional or not part of U.S. eduroam, it is the stated direction for eduroam Europe and could provide significant benefits. Institutions with RadSec capabilities will be well positioned for whatever course U.S. eduroam takes.

4. If you have an 802.1x compliant infrastructure, commit to full eduroam participation by fall 2011.

5. Institutions that will not have 802.1x capabilities in the timeframe necessary to meet our deadline may at their option, protect their captive portals with Shibboleth to support federated login by affiliates of other CIC institutions.

6. Produce a standard document that can be deployed as a web page describing how visitors can access wireless. Each institution would post in an area easily accessible from their home page (e.g. many/most/all of us have a “Visiting Campus” or “Visitors” link off our home page). A composite document might be deployed at the www.cic.net.