# ShibbolizedWireless

## UT System Public Wireless Network Sign-on

It's a fair statement to say that a majority of guests to the UT System Administration complex are affiliated with other UT System institutions. We host a variety of system-level meetings, project/virtual teams, special-interest groups, etc. We've had a public wireless network available to these guests for some time, but it used a set of rotating, yet widely-known, shared group names and passwords. Thanks to a recent upgrade of the wireless network, we're now able to offer a shibboleth-based option for sign-on to the public wireless network and eliminate the security hole from widely-known "secrets".

First of all, I'd be remiss if I didn't point out that this is a hack. It works, it's transparent to the users, and I don't know of anything wrong with doing things this way (if you do, please let me in on it – pcaskey@utsystem.edu). It will not work for an 802.1x environment and is not viewed as a long-term solution to the challenge of federated wireless networking. For information on (and to contribute to) potential long-term solutions to the federated network authentication challenge, visit the Internet2 SALSA-FWNA (Federated Wireless Network Authentication) Working Sub-Group and the eduroam site. It was just a novel way of using Shibboleth to solve a business problem and may have application in other areas.

This one application has helped us achieve greater progress with federated identity management within the UT System than almost anything else we've done. As representatives from the various UT System institutions come for meetings, some executives from UT System Federation member institutions are able to login to the wireless network with their home credentials using Shibboleth and benefit from full privileges and more bandwidth, while those who are not yet running Shibboleth IdP servers, are required to register as a guest with reduced privileges and bandwidth. Peer pressure at that level can sometimes be very persuasive.

First of all, the key enablers for this solution were

- a wireless network that supports external web authentication and AAA Override from RADIUS (vendor-specific attributes) – we're using Airespace (now Cisco), but several vendors offer these features – it works just like internet access in hotels with browser redirects and
- a RADIUS server that could employ a hierarchy of data sources, with one of those sources being a SQL database (we're using Cisco ACS, but several have this feature).

The wireless network sign-on process is as follows:

1. The user associates freely to the wireless network and requests a web page in their browser.
2. The user is redirected to an external web page on one of our web servers.
3. This page presents the user with a choice to either login using Shibboleth through the UT System Federation or login through the guest access system (regular form-based login and not discussed further).
4. After choosing a shibboleth login, the user is redirected to the UT System WAYF, then to their HS/SSO, then on to the wireless sign-on application (there is a pre-auth ACL on the wireless network that specifies federation WAYF and IdP servers as allowed traffic). *Editor's note: Paul has noted thought's been given to allowing this network access to untrusted users: "What are they going to do, DoS us from an 802.11?"*
5. The wireless sign-on system first checks to see if an eduPersonPrincipalName (ePPN) (and soon affiliation too) was released and if not, does nothing and displays an error page.
6. Assuming a valid ePPN (today, we're just looking for any value, but we're evaluating needs to possibly filter some of these based on level of assurance or something similar), the system grabs the session ID from the shibboleth cookie and writes the ePPN and session ID to a SQL database that is front-ended by our RADIUS server (the ePPN becomes the user's username and the session ID becomes the password).
7. Along with the username and password that is written to the SQL database, a RADIUS group is written for the user, based on their identity. We are currently only differentiating between guests and federation members (with the latter receiving no bandwidth or network protocol restrictions), but easily have the ability to base policy decisions off of affiliation or any other asserted attribute.
8. Assuming all went well, the user sees a message telling them that they have authenticated successfully and displays the standard disclaimer about being subject to monitoring and asks them to acknowledge by pressing a Continue button.
9. When the user presses the Continue button, their browser does an HTTP POST of the "username" (ePPN) and "password" (Shibb session ID) back to the wireless network switch, which in turn, verifies the posted username and password with the RADIUS server (which doesn't find the user in it's primary data source and then checks the SQL table).
10. Based on the group set in the database for the user, the RADIUS server will use AAA Override (also called vendor-specific attributes – VSAs) to tell the wireless network what level of QoS and what ACL to place on the user's session.
11. The user is then redirected to the page they initially requested (i.e. their home page).
12. Periodically, there is a stored procedure in the database that kicks off and wipes out older records in the user table for the RADIUS server.

*Questions/Comments?* They are, of course, always welcome! Send them to pcaskey@utsystem.edu

– PaulCaskey - 21 Jul 2005