Return to Advance CAMP wiki

Advance CAMP Wednesday, Sept. 28, 2016

4:30pm-5:20pm

Dupont Room

Guest Identities: Account Minting and Identity Promotion

CONVENERS:
Michael Domingues, University of Iowa
Billy Cook - Clemson University

MAIN SCRIBE: Eric Goodman

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 36

Russell Beall -- University of Southern California
Jon Miner - UW-Madison
Jan Tax -- UNC Chapel Hill
Celeste Copeland -- UNC Chapel Hill
Kerry Havens - University of Colorado Boulder
Vaibhav Narula - University of Utah
Subhasish Mitra - University of Utah
Jill Gemmill - Clemson University
Billy Cook - Clemson University
Jeff Bate - Clemson University

DISCUSSION:

There are guest accounts on campus, in general not done well. Several distinct systems containing them, with varying levels of accuracy (vetting, etc). Looking at creating a single “source of truth” for guest identities. Many have tenuous connection to the campus.

Specific desire is promoting the guest identities to “full identity”.

Question of scope:
Is it:

- anyone can create an account
- Only one guest account system exists
- Accounts for people who aren’t in your central identity system
- Is it guest credentials or guest identities

[Editor’s editorial: the term “guest account” is being used by many people to mean “a credentialed account with no or few authorizations”. It’s somewhat conflated with guest/external credentials, and implementations that maintain separate repositories for guest/“low authorization” accounts vs. “member” accounts for faculty and staff.]

Are wireless accounts unique enough that they should be handled differently? UWisc can host even wireless only accounts in their central person repository. (Though they also maintain a separate account system that is used too). In many use cases (multiple campuses commented) those wireless accounts get promoted to being full users, so separate wireless can be an issue.

There are tools that can authenticate social credential (or account) and allow temporary access to wireless. Could be extended to desktop support (identity less). Debate on whether every credential (even temporary ones) require identities. Those that spoke seem to fall out about 2:5 no:yes. Further discussion detailed cases where people actively put entries in the identity store vs. just using the name of the credential. Some locations also keep track of data that was associated with a guest account WITHOUT creating an identity (in the standard identity registry) for it. E.g., maintain a gmail account record without entering

Indiana only has of one identity flow that promotes “low loa” accounts (applicants) to full fledged accounts. Are there others?

Also, consider that there are naming issues; temp account names (and frequently identities) are often random looking and students are frequently given first.last type names, so consider the rename process.

If someone has a credential, that's a matching factor, if they have trusted identity data, that's a matching factor..

Became clear through discussion that there is a large variance among people in the room about the meaning of “guest”, “guest account”, “affiliate” and other keywords in this space (even among ACAMP vets!)

Some vague attempt at capturing the table that I was hand waving during the discussion.

	Incidental (Implicit) Access (Wireless access)	Significant affiliation access
Guest Credential	optional	required
Full Credential	good idea	required

When MUST an identity be added to the identity store

Minnesota has "guest" and "sponsor" where "guest" is self-asserted and "sponsor" is brought by a campus department. They manually maintain connecting people by swapping the ID to the "real" identity when a "sponsor" entry transitions.

ACTIVITIES GOING FORWARD / NEXT STEPS: