IAM Committee

Meeting Notes

3/9/2014

Attendees: Greg Baker, Mark Barber, CW Belcher, Michael Bos, Cesar de la Garza, Ed Horowitz, Ty Lehman, Darin Mattke

Absent: Cam Beasley, David Burns, John Chambers, Fred Gilmore, Roy Ruiz, Steve Rung, Charles Soto, Kim Taylor, Raul Villa, Jason Wang

IAM Team Members: Marta Lang, Aaron Reiser, Dustin Slater

1. ForgeRock Meeting Recap

This meeting was attended by five ForgeRock representatives (four in person and one via phone) in order to hear the concerns of users of UTLogin. The representatives talked about what they have been doing in order to improve their processes, address issues that the UT community has encountered, and get a better understanding of what is important to the UT community and how ForgeRock can help improve things on their end.

Approximately 17 UTLogin customers were in attendance. Meeting minutes were sent out for comment on Friday and feedback was requested from the attendees in order to ensure that future sessions are informative and useful for all parties involved.

Q: Is there any information available regarding tracking numbers for enhancement requests made to ForgeRock during this meeting?
A: The meeting yielded no specific new feature requests, mostly process improvements. Typically, feature request are submitted by the UTLogin team. ForgeRock has a public JIRA site (https://bugster.forgerock.org/jira/browse/OPENAM) where customers may view the status of issues, though these are not broken out by UT Austin requests. The UTLogin team does have a list of issues submitted by UT Austin which they monitor regularly.

One of the main items discussed during the meeting was about how ForgeRock is changing how they manage their engineering teams, breaking them out into a core team and a WPA team. They have heard that support has been uneven so they will be focusing on consistency going forward.

Q: What was the most interesting feature announced for OpenAM 12 that would benefit the university?
A: The addition of social network login capabilities and the addition of new API capabilities.

2. UTLogin & UT Power Outage – Update

During the recent university power outage there were approximately 42 minutes of downtime for UTLogin. A fully summary of the outage, including the root causes analysis, can be found at https://wikis.utexas.edu/x/jQuKBQ .

Q: What steps are the UTLogin team taking to account for the networking change in UDC-B on 3/14?
A: The UTLogin team is proactively bringing the UTLogin servers down gracefully during the maintenance in order to prevent any issues.

Q: How long did it take to detect UTLogin was down and, from there, how long did it take to triage the system?
A: The exact timeline is available on the wiki page linked above, however due to a number of resulting issues (e.g. power outages in the office, power outages affecting cell service and resulting in poor data coverage, and the overburdening of close-by off-campus wireless access points) caused what would have been a 5 minute outage to turn into a 40 minute outage.

Suggestion: In the event of a similar outage, staff should move to UDC-B and, if that data center is down, staff should move to UDC-C as a backup.

3. IAM Roadmap – Update

Reference handout (soft copy to be sent to the committee via email).

The most significant change is that several initiatives having to do with IAM modernization have been consolidated in the IAM Modernization Program (IAMMP) section and broken down into three phases based on feedback from SailPoint. The IAMMP team is currently working on developing the statement of work to hire an integrator. The first phase on IAMMP will include the deployment of the SailPoint technical architecture and system environments, development of the detailed data and interface transition strategy, and implementation of group and role management functionality. Identity administration and provisioning, password and credential management, and other items currently handled by the uTexas Identity Manager (TIM) will be implemented in phase two. Phase three will deal with access and approval management, access recertification, and enterprise authorization reporting. More details will be available when the project plan is finalized.

Q: When will information on transitioning be available to owners of systems consuming identity data?
A: It will depend on the data. The IAM Team will be working with the owners of each source system to schedule transitions, which will include the creation of bridges if the respective deployment schedules are not aligned. For new functionality such as group and role management, the IAM Team will identify early adopters to prove out functionality, with expanded campus adoption proceeding in future phases. When changeovers begin in each phase, information will be developed for customers including information on what they will need to do.

In the Identity Assurance and Authentication section of the roadmap, there is a line for Lightweight Authentication. That project has kicked off and the first meeting of the steering committee took place last week.

The CARE project plan is currently being finalized and the project kickoff meeting will happen in the next few weeks.

The next enhancement in the pipeline for Two Factor Authentication is the implementation of hard tokens. Toopher is ready for the IAM Team to being their testing. The IAM Team will be coming to the IAM Committee to for input on policies surrounding hard tokens, such as eligibility, replacement, cost, etc.

Q: Is there a pilot group for hard tokens?
A: Not yet.

Q: Is there an estimate for how many individuals will need hard tokens?
A: The number is unclear, but it should not be more than a few hundred individuals. It may make sense to include individuals who are having significant difficult using the existing Printable One Time Password (POTP) functionality.

Q: What will the provisioning process for hard tokens look like?
A: It will be a manual process involving a physical provisioning step.

The team anticipates that after the IAMMP integrator is selected and initial phase one detail is put together that there will be adjustments to the IAM Roadmap. That information should be available in time for the next IAM Roadmap review in the summer.

4. Other Initiative Updates

a. Two Factor Authentication

The IAM team is working with ITS Systems and ITS Networking to ensure a cohesive, collaborative approach for implementing the UT System two factor authentication mandate on campus. The proposal for this initiative will be going out soon.

Q: Will the mandate result in the blocking of remote desktop to personal machines?
A: That would need to be addressed by the Information Security Office.

Action Item: Share with the IAM Committee ITS Networking's plans regarding the expansion of VPN capabilities to support the two factor authentication mandate.

b. CARE Project

The project plan is currently under review. The kickoff email to the customer steering committee should be going out within the next several weeks. The plan is to approach the project in phases with Shibboleth and TED handled first, followed by UTLogin.

c. Lightweight Authentication & BYOId

The Customer Steering Committee kicked off their first meeting last week. Autumn Shields is currently gathering requirements from and interviewing key stakeholders around campus to identify use cases. Requirements gathering will take place over the next six weeks with a goal of presenting the requirements to the IAM Committee in early May.

d. IAM Modernization Program

The team is currently developing the statement of work for the SailPoint implementation partner. The statement of work is expected to be released in April.

e. Identity Assurance Framework

Work on the framework has been rescheduled to align with the Lightweight Authentication project. One of the deliverables of that project is to create guidelines for developers on campus who want to use lightweight authentication, which will be provided via the Identity Assurance Framework.

f. TADS Security / IAM SME Group

There was an FYI presentation last week covering product selection for the new technical architecture. The IAM Team will be working with the TADS team to complete an in-depth review of each selected product