IAM Committee
Meeting Notes
03/12/2018

Attending: Dash Ballarta, Cam Beasley, CW Belcher, Michael Bos, Ed Horowitz, Felipe Lee, Ty Lehman, Darin Mattke, Jason Mayhew, Chris Owan, Steve Rung

Absent: Graham Chapman, Tim Fackler, Cesar de la Garza, Alison Lee, Mike McIntosh, Shelley Powers, Dustin Slater, Charles Soto

IAM Team Members Present: Michele Graham, Joel Guajardo, Justin Hill, Marta Lang, Mario Leal, Reece Price, Aaron Reiser, Autumn Shields

1. UTLogin Stability Roadmap Progress – Update (Marta Lang)
   Reference Handout
   • Completed re-baseline of project plan
   • Team is working on configuration of the TEST environment
   • Re-baselined completion date for this phase is May 11, 2018.

2. IAM Workday Readiness Coordination – Update (Marta Lang)
   • Number of different IAM systems impacted by Workday Go-live
   • DY Module (Workday mainframe data replication) testing coming up
     o Documented DY testing scenarios needed for IAM systems
   • For TIM, Apollo, OHSC, ID Card System, DPUSER:
     o All changes completed except for ID Card System changes, which are in TEST and QUAL
   • SailPoint - Workday Integration Testing
     o Round 3 wrapping up in next week
     o End to end testing in May
     o Regression testing will take place when Workday has next release this summer

3. SailPoint IdentityIQ 7.2 Upgrade – Update (Autumn Shields)
   • Goal is to update in QUAL before Workday end-to-end testing
   • Version 7.0 to 7.2 upgrade requires an upgrade first from 7.0 to 7.1, then 7.1 to 7.2
     o 7.1 upgrade requires some development work. On-track to finish this week. Testing next week.
     o 7.2 will also require some development because of API changes.

   Reference Handout
   • Answer questions from last time:
     o All users who do not have an updated password hash on file will need to change their passwords.
       ▪ The IAM team will execute a communications campaign for affected users.
• After password rule changes have been implemented, a series of notifications will be sent to affected users to let them know they need to change their passwords.

• High Level Plan
  o Implement password rule changes in summer 2018
  o Start communication process end of summer, beginning with staff and then moving on to faculty and students

Q: Will new rules work with old OS versions? Q: Will this affect AD administrator accounts?
A: by Cam Beasley: This could affect AD administrator accounts.

Q: Faculty and staff are cautious about responding to emails that refer to passwords after ISO phishing exercise. How will you address this?
A: The team will take this into account in the design of the communication campaign.

Request: Notify technical contacts within the departments so they can communicate with employees about the change. Let staff know about new password rules so they may change it on their own.

Q: How will you handle populations that have a need for password expiration?
A: The team will work directly with groups that have these requirements.

Comment by Cam Beasley: NIST password standards assume 2FA is in place, so the university recommendations are more strict because universal two factor is not in place.

Joel Guajardo: We will meet with FAS Communications to develop communication plan.

• Feedback from the committee on the proposed password rules is due by March 26th

5. Other Initiatives/Updates
   a. IAM Team Staffing (Mario Leal)
      o Caroline Taylor has resigned - Last day is March 23.
      o 4 vacancies open:
         ▪ SSDA – Reclassifying position to SDA to widen pool
         ▪ SE – On-site interviews scheduled for next week
         ▪ BA/QA – On hold
         ▪ IT Manager – Developing posting

   b. IAM Integrations (Justin Hill)

      Reference Handout

      o In an effort to better support the UTLogin V2 project some integration engineers are being reassigned to UTLogin V2 work. Work on new integrations may be delayed.

   c. Apollo and OHSC Roadmaps (Michele Graham)
      o OHSC – Expect to have OHSC roadmap drafted by end of Month.
      o Apollo – The Apollo roadmap has been drafted. Will send communication to the IT community about the Apollo and OHSC roadmaps at the same time.
UTLogin Stability Roadmap Status
IAM Committee
Monday, March 12, 2018

UTLogin Roadmap Status

Action 1: Stabilize Current UTLogin Environment (Complete) - As of June 8, 2017, the IAM team disabled the self-service Realm Policy Agent and put the existing UTLogin environment in a “critical fix only” mode. Efforts will now focus on Action 2.

Action 2: Simplify & Standardize UTLogin Environment (In Progress) - The rebaseline of the “Build TEST Environment” phase is complete with the new Planned Finish dates reflected below. The team is now currently working to complete the environment configurations for the Build TEST Environment phase, which will be completed in May 2018. The team completed the configuration of the User Interface (UI) pages and the integration with Duo. We are now focused on the configuration of OAuth, SAML, monitoring, and the whitelist filter. Planning for following phases will be completed in April 2018.

Action 3: Measure & Report Progress (Ongoing) - KPIs have been identified and are being published on a weekly basis (See: http://iamservices.utexas.edu/projects/utlogin-stability-report/). Monthly status updates will be provided outlining incidents, KPI’s, and project status.

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Budget Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project</td>
<td>Planned Start</td>
</tr>
<tr>
<td>IAM Project - UTLogin Stability Roadmap</td>
<td></td>
</tr>
<tr>
<td>Simplify and Standardize - Planning</td>
<td>6/5/2017</td>
</tr>
<tr>
<td>Simplify and Standardize - Requirements</td>
<td>6/5/2017</td>
</tr>
<tr>
<td>Simplify and Standardize - Procurement</td>
<td>6/19/2017</td>
</tr>
<tr>
<td>Simplify and Standardize - Design</td>
<td>6/26/2017</td>
</tr>
</tbody>
</table>
**UTLogin Availability**

This graph represents UTLogin’s overall availability since November 9, 2017 along with UTLogin’s published SLO of 99.42%. This data shows that since UTLogin was put into critical/fix only mode on June 8, 2017, the number of service disruptions has decreased. There were no service disruptions for the month of February.

Historical data and other Key Performance Indicators (KPI’s) which reflect the stability of UTLogin are published every Friday. The weekly report is viewable here: [https://iamservices.utexas.edu/projects/utlogin-stability-report/](https://iamservices.utexas.edu/projects/utlogin-stability-report/).
BACKGROUND
The National Institute of Standards and Technology (NIST) recently issued revised guidelines for digital identity management, including authentication management (see https://doi.org/10.6028/NIST.SP.800-63b). While UT Austin is not required to follow NIST identity management guidelines, they are well-respected in the identity management community as recommended best practices.

REVIEW OF PERSON EID PASSWORD RULES
The IAM team has reviewed the new version of NIST 800-63B to assess the alignment of UT Austin’s current password management rules for Person EIDs with NIST’s recommended practices. Notably, NIST has removed their prior recommendation that users be required to periodically change their passwords, which aligns with UT Austin’s current EID password rules. NIST also recommends that many commonly used password content requirements be removed or relaxed to reduce the burden on users.

RECOMMENDATION
The IAM team recommends that the Person EID password rules be modified to allow the use of passphrases (a series of words with spaces in between) that are easier for users to remember but more difficult for other humans or machines to guess. The team also recommends simplifying other EID password rules in alignment with NIST recommendations, as shown in the table below.

<table>
<thead>
<tr>
<th>Password Rule</th>
<th>Current Guest Class</th>
<th>Current Member/Affiliate Class</th>
<th>Proposed Guest Class</th>
<th>Proposed Member/Affiliate Class</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length</td>
<td>8 characters</td>
<td>8 characters</td>
<td>8 characters</td>
<td>12 characters</td>
<td>ISO recommendation</td>
</tr>
<tr>
<td>Maximum length</td>
<td>20 characters</td>
<td>20 characters</td>
<td>32 characters (or longer if downstream systems can support)</td>
<td>32 characters (or longer if downstream systems can support)</td>
<td>Lengthen to support passphrases</td>
</tr>
<tr>
<td>Biographical info in password</td>
<td>Cannot use EID, birthdate (any format) or name (first, middle, last)</td>
<td>Cannot use EID, birthdate (any format) or name (first, middle, or last)</td>
<td>Cannot use EID, birthdate (any format) or name (first, middle, or last)</td>
<td>Cannot use EID, birthdate (any format) or name (first, middle, or last)</td>
<td>Avoid common social engineering risk</td>
</tr>
<tr>
<td>Spaces allowed?</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Support passphrases</td>
</tr>
<tr>
<td>Character census</td>
<td>Cannot be all letters or all numbers</td>
<td>Must have at least one letter, number, and special character</td>
<td>Cannot be all letters, all numbers, or all special characters (Must have 2 out of 3 character types)</td>
<td>Cannot be all letters, all numbers, or all special characters (Must have 2 out of 3 character types)</td>
<td>ISO recommendation</td>
</tr>
<tr>
<td>Cracker dictionary check</td>
<td>None</td>
<td>Dictionary check for words of 4 or more characters</td>
<td>None</td>
<td>Limited dictionary check</td>
<td>ISO recommendation</td>
</tr>
<tr>
<td>Password expiration</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None globally but some populations may need password expiration</td>
<td>NIST 800-63B recommendation</td>
</tr>
<tr>
<td>Previous password re-use</td>
<td>Cannot re-use last 10 passwords</td>
<td>Cannot re-use last 10 passwords</td>
<td>No restriction</td>
<td>No restriction</td>
<td>Avoids storing old password hashes</td>
</tr>
<tr>
<td>Password hint allowed?</td>
<td>Yes</td>
<td>No</td>
<td>Yes (but remove once password management moved to SailPoint IIQ)</td>
<td>No</td>
<td>NIST 800-63B recommendation</td>
</tr>
</tbody>
</table>