ITAC Meeting

Date: August 9, 2012    Time: 8:30-10:00

GSC, Rm: 2605

Meeting Leader: Adam Mikeal    Recorder: Lori O’Bannon

Attendees: Andy Bland, Becky Carr, Erick Beck, Fred Fisher, Mark Harris, Tom Lyster, Adam Mikeal, John Norton, Jim Rosser, Ron Szabo, David Sweeney, Allison Oslund, Michelle Osterholm, Willis Marti

Guest Attendees: Dr. Deborah Dandridge, Cheryl Cato, Dr. Trez Jones, Tom Golson. Dr. Marchbanks

Item 1: Approval of Minutes: Minutes approved unanimously

Item 2: New IT Trends

Topic: David Sweeney brings up topic of Common Alerting Protocol (C.A.P.)

Relays trending: Emergency Notifications opportunities for disseminating information to faculty, staff and students (clients).

- Emergency Notification Clients: C.A.P. encompasses major categories of emergencies: Weather, Public Safety, etc.
- David Sweeney asks does anyone use C.A.P. notifications; if so, is your dept./unit utilizing Code Maroon relative to the Emergency Notifications. Charley Clark’s desire is that there is broad distribution for emergency notifications.
  - Willis Marti: States C.A.P. has different versions, and each version has unique challenges. Willis encourages the ITAC committee to utilize C.A.P., get emergency messages out to all clients.
  - Willis advises the committee members, if you have C.A.P. compliant questions, contact Judith Lewis for assistance.
- David Sweeney asks is CIS the group that sponsors the program.
- Dr. Marchbanks replies that Dr. Cantrell runs the students C.A.P. portion, and Charley Clarke runs the faculty and staff C.A.P. portion.
  - David follows up with latest C.A.P. version is 1.2 and was updated in 2010. It is very different than 1.0. &1.1 which has contributed to inconsistencies across the board.
- Adam Mikeal inquired “How is it distributed?” answered through XML container.
  - Willis Marti explains the two different interpretations, pose difficulties for transmission.

Topic: Marti Willis: stated “Wired” publication reported- Gmail account was hacked and compromised while customer was executing on line purchases through Amazon and Apple stores.

- Adam Mikeal relayed the hacker wiped the victim’s IPhone, I Pad, and Mac book. All devices chained together. Once one device was compromised, the next apparatus was backed up and the password or email was chained to each device. The hacker did not have to even guess a password.
Topic: Marti Willis: stated “Wired” publication reported- Gmail account was hacked   cont.

- All occurred through social engineering: The attacker used the target’s last 4 digits of credit card and home address; from that small bit of information Amazon allowed the hacker to add info to the accounts.
- Additionally, the attacker used that info to remove original email info from Amazon account and crafting social engineering, accessed Apple and apple id.
- Since incident: Amazon and Apple have changed policies.(Still holes in procedures)

Topic: Willis Marti parlayed recent interpretations regarding FERPA data in "The cloud."

- If you put FERPA data in the cloud, must have “Direct Control,” of the cloud.
- David Sweeney states need to tell the stories to customers; however, in doing so, also need to offer solutions.
- David Sweeney states he likes Internet 2 as a network solution- probably too expensive for the University. David poses a question: Are we at the point that we have to decide, Is the solution that is distributed by centralized IT effective, or is each individual shop going to have purchase its own solution? Presently, there is not an integrated shared solution offered.
- A Rick Young point out this predicament is not unique. The needs of people within unit/depts. always out paces what can be provided? Historically, it has not been economically feasible to purchase campus centrally provided services? For example a researcher in his dept. wants a terabyte that is not available from the campus centralized IT. Until it is both economically viable and available, the problem continues.
- Fred Fisher states Pete can provide a terabyte of storage cheaper than “he can,” Pete states,” If more folks come on, the cost lowers.”
- Dr. Marchbanks stated if you go to Dr. Cantrell and say, “I need this amount of storage space, and I have this amount of money available to fund…” Collectively, that process can aide a campus-wide solution. (Help Dr. Cantrell mitigate funding risk for a campus solution)
  - David Sweeney states not just storage space, also a need for a cloud base model. Have to address funding issue. Users already have access to “the cloud.”

Item 3: Dr. Trez Jones addresses ITAC committee brief overview: ID Management, present services offered and long term goals:

- In Feb 2012 ID Management Office began operations: The services were an evolution of CIS’ Account Services’ Office.
  - Account Services: Create UIN in special situations: For example extensions and pre-provisioning net ids in unusual circumstances: Includes J1 scholars, contractors, visiting researchers, etc.
  - If you have faculty members leaving, ID management office can de-affiliate faculty member using payroll feed, ID office can work with units, staff and/or faculty while the faculty member is completing business with the University.
Item 3: Dr. Trez Jones addresses ITAC committee brief overview: ID Management Office  
cont.

- ID Management Office can Provision BBP, in cooperation with Willis and OAL’s Line of 
  Business, and assign special guest accounts to VPN, Wireless, and Open Access Labs’ 
  machines.
- Proxy Management; example: libray@tamu.edu; assists organizations to grant access to services 
  at proxy.netapplication.
- Can facilitate special password reset
- ID Management Office provides proactive security management of the campus Net IDs 
  credentials:
  - Look at how people are using net ids. Try and put compromised accounts out of 
    commission before something, “bad happens.”
- Basically ID Management office can support helping folks with any kind of bizarre question/ 
  concern. Trez relays the ID Management office “Takes pride in assuming ownership of the 
  problem, and bringing it to a resolution.” Contact info: 2-4300, and identity@tamu.edu

Future Goal: Trying to federating” Identity Agents,” across the campus:

- Presently, folks have to come to main campus, present IDs. No other way to verify identity 
  unless individual comes into the ID office in person
- Currently have a Beta group program running with ADMI and PITO for read only access to 
  administrative LDAP data and password reset services.
  - Using that information from applicant Pool-Admissions Beta program, seeing how they 
    use that service; hopefully, very soon the ID Management Office will be able to roll out 
    the ability to provision guest accounts in a limited capacity to “Identity Agents.”
  - The catalyst behind this concept is the ID Management office’s desire is to work 
    cooperatively with depts. /and units across campus – Frankly, “Departments and units 
    know their user base.” (Really, no reasons pass folks to ID office).
- Using the information gained from the beta program, The ID Management office will establish 
  an “Identity Agent” protocol:
  - A process will be determined and a code of conduct of responsible standards of use will 
    be agreed upon for Federated “Identity Agents.”
  - The ID Management Office will work cooperatively with Units and Departments- In doing so; improve the quality of life for your IT professionals and your user base.
  - The desire is for more groups to participate in the program.
- The “Identity Agent”: As the program is formalized, the authorizing ID Management agent will 
  work similar to compass’ primary authorizing agent, and PAAA for your LOB., authorizer
- Currently, aggregate 26 data feeds to come up with enterprise directory.
- Testing: Incorporating small fees; make sure odd groups have access, and requested services 
  provided. Unique individuals come to TAMU and request net ids and resources, etc. The ID 
  Management office will also work with library to facilitate the individual appropriately. Gather 
  the validating information, and provide them appropriate access.
Future Goal: Trying to federating” Identity Agents,”  

- Individuals are looking to “you” to provide services. The goal of the ID Management Office and the theory behind “Identify Agents,” is to make services easier for everyone involved.

**Future Goal:** Biometrix – Dr. Cantrell would like Kiosks on campus to provision some services.

- Once hardware installed there will be a lot of opportunity for integrated services for all of our lines of business.
  o Partner with library, federate agents, leverage some of their infrastructure.
  o For example: Imagine a student/parent doesn’t know the location of their next class, or meeting.
    ▪ Go to kiosk, and obtain a map indicating exact building.
    ▪ This program is part of an integrated shared services initiative from Dr. Cantrell.

**Future Goal:** Making things easier for part 02 user base to integrate passwords for SSO and net ids:

  o Function SSO and CAS are different, but all lead up to Dr. Cantrell.
  o ID Management Office is meeting with SAGO rep to begin the dialogue.
  o Cooperatively working on integrating security efforts that incorporate net ids’ use to sign e signatures.
  o Will continue Policy outreach on SAP initiation and revisions.

- David Sweeney states his department has a unified active directory in his division. What would it look like for his dept. to give ID management password reset, while he maintains the security group level access for his users?
  ▪ Trez responded, The ID Management Office would manage password reset at the dept. level, using University standards.
  ▪ David Sweeney affirmed he would like more information on the Identity Management Agents. How do we integrate active directory into the ID Management Office?

- Trez replies: He would address the “Identity Agent” question and defer to Tom Golson to address the technical concerns.

- Beta testing Allows “ID Agents” to flag a password or account for password reset. Using the same tools that senior support staff have at help desk central in the Operations Division:
  o Such as: gateway.tamu.edu the “Identity Agents,” would continue the process.
  o The “ID Agents” are given access to the same tools ID Management Office uses.
  o Present internal tools, are not; “idiot proof,”
  o The desire is to roll out less technically inclined applications.

- Trez quantified presently in the information gathering phase. (Using ADMI’s feedback)
  Establishing needs of the “Identify Agents,” without compromising security.

- Weighing security implications. Want to enable IT consumers and IT end-users and not compromise security: Too much security, no accessibility; too much accessibility, users do what they want.
**Future Goal:** Making things easier for part 02 user base to integrate passwords for SSO and net ids:

- Over the next semester the SAP should be written, Identify Management’s duties will be codified by December.

**One Way Federation**

- Tom Golson states the goal to use Identity Management is to enable services once you have a handle on identities of individuals. At that point, then you can address service delivery in a “granular fashion.”
- ID Management is not just password reset. Shibboleth and federated identity provider is part of being a federated in common provider
  - National Institutes of Health claims to save a million and half of dollars- getting out of password reset business
- Tom Golson asserts to offload the burden of password resets, really is redistributing a financial cost. Perhaps you do not have the burden of password reset but, you still have customer service issues.
- Presently, have audit requirements:
  - Have to look for comprised shared accounts, perform security locks
  - Password changes on people.
  - If that person is your customer, then in Tom’s opinion, it becomes an unsatisfying customer service experience. (Therefore a Negative incentivize shared authentication model).
  - ID Agents’ problem designed to overcome those problems. Tom declares, the IT professional sees the benefits of a shared authentication model. However, what is harder to see is what might incur, that could be perceived as “Service Negatives.”
- David Sweeney declared that is already happening now.
  - David Sweeney feels his customers would feel the opposite, He sees the benefits to a shared service ID Management model.
- Tom Golson: states: Initially it sounds great, until people will be locked. Tom agrees Suggest “Shared Service Authentication” is a huge win for the University. However, there will be problems people do not see.
  - Seeing a lot of failed log-ins due to shared log-ins. That is a clear/ present danger to the University.
  - Unfortunately, the person at the computer, trying to log in may not know, “Why am I locked out? “
- Tom Golson recommends until quality customer service, up and down the chain, can be guaranteed, there is no merit to setting aside resources, people and time in depts. across the campus. There is value to offloading password resets. However, your customers, will not like it when they have been locked and they call you, “Call CIS.”
- Need to build better tools? Continue to provide support to get departments out of the password reset business.
Tom Golson explains: Authentication Services for all people in the active directory, your customers, can be provided today. You will be in business of managing security groups.

- David Sweeney responds that is what we want.
- A Tom Golson question is that? It is not convenient. As credentials are monitoring Centralized Authentication, One –way Federation manages threats for compromised accounts and password reset.
- Ultimate Credential Source is centralized. Manage a password for 6 months or Manage 10,000 failed Log-in failures. (Separate problem space) Applies more value to customers.
- Tom Golson states will be able to use pass phrases by the end of Sept.
- Tom pleads with ITAC committee to please champion SAP, policies so can proceed to administer procedures; in absence of policy, enforcement is currently problematic.

- **David Sweeney: Summarizes Tom Golson’s Concerns:**
  - Level Customer of Service is not present, when we move to centralized passwords, an answer of “Contact CIS, “is a bad solution.
  - **Answer:** Solution Create Identity Agents: Local agents in our area have access to the same tools HDC folks, ability reset passwords. Sounds great. In the process of defining roles of those folks. Administratively, allows the IT dept./units to support solution
  - **Technical side:** AD Authentication- difference global and local security groups.
    - Tom Golson wants dept./units to continue to support security groups in their own areas, and Tom Golson states has no desire to manage those security groups from a centralized state.
    - Tom Golson agrees
  - David Sweeney: Issue technical limitations; have to sort them out before we move forward.

- Ron Szabo stated completed one way federated trust with students and in the process of implementing changes with Lawrence research lab, transitioned groups; effort was enforced at Bush School.
  - Accounts provide AD, still manage population and security. One way trust; have to take measures to authorize trusts.

- David Sweeney declares “Not seeing the downside.”
  - Adam Mikeal: replies to David, the problem is you do not have faculty. Very difficult to get faculty to change behavior.

If anyone has any question about ID Management contact Trez Jones: 862-4300 or identity@tamu.edu

If have questions about I way trust- contact Tom Golson: 458-4373 or tgolson@tamu.edu
**Item 5: Next Steps: Retreat review:**

- **Shared Services**
- **Funding Model - Focusing Centralized Funding**
- **Leading in Innovation: Broad Areas**: Need to come up with some measurable goals
  - Ideally thought about a subcommittee to work SMART Goals. Put on hold for now.
    - David Sweeney asks the committees to work the SMART Template and complete and submit to Executive Steering Committee (E.S.C.), or ITAC listserv. E.S.C. will codify all info received.
    - Shared Services Goals: Identify Shared Services: The 2 previously, Identified ID Management, Email, Fred Fisher asks to add “Cloud Services.”
- **Adam Mikael** requests completion of Goals, please enumerate, prioritize areas for Shared Services
  - Adam asks committee members to work with the E.S.C. to flush out initiatives, and help identify “Next Steps.”
  - Adam asks the Committee members to complete the SMART Template and provide to Executive Steering Committee.
  - David Sweeney asserts he will come to meeting prepared to discuss SMART Goals info received.
  - Adam Mikael cautioned the first round of discussions will only be as effective as feedback received.
  - Eric Beck adds please make sure take into consideration reports the chancellor has should put out, and frame the documents form that narrative.
- **Funding Model**: Collect Information regarding Email comparative email costs. How do we access cost of email? David Sweeney will put together a Qual-Tech survey and send out to ITAC members.

**White Board Notes**: Flushing out input from committee to determine Shared Services Funding. David Sweeney will be sending out info to committee members. Be prepared mid Sept: Below captured discussion: White board Notes:

<table>
<thead>
<tr>
<th><strong>Groupware Email Cost</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personnel: % FTE</strong></td>
</tr>
<tr>
<td>Admin: Manage, Restore, Training</td>
</tr>
<tr>
<td>Service desk: Tickets, Provision, Setting up Mobile, Training</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
</tr>
<tr>
<td>Servers, Redundancy</td>
</tr>
<tr>
<td>Storage</td>
</tr>
<tr>
<td>Back up (SW, Media)</td>
</tr>
<tr>
<td><strong>Network</strong></td>
</tr>
<tr>
<td><strong>Facilities</strong></td>
</tr>
<tr>
<td>Rack Rental</td>
</tr>
</tbody>
</table>
White Board Notes  cont.

<table>
<thead>
<tr>
<th>Power/ Cooling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generators</td>
</tr>
</tbody>
</table>

**Software**

<table>
<thead>
<tr>
<th>Servers, Desktops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage, Back up (mentioned, but not annotated)</td>
</tr>
</tbody>
</table>

**Level Of Service**

<table>
<thead>
<tr>
<th>Identify services (calculate email contacts, im quote)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery time</td>
</tr>
<tr>
<td>Downtime a year, (school, in schedule)</td>
</tr>
<tr>
<td>Geographic List</td>
</tr>
<tr>
<td>DAG replication</td>
</tr>
<tr>
<td>Can you recover from loss of stack- due to fire, hurricane</td>
</tr>
<tr>
<td>Catastrophic loss? Time?</td>
</tr>
</tbody>
</table>

**Announcements:**

- David Sweeney: Appointment letters going out Deans and Vice Presidents
- Conversation with Dr. Snell: LMS identified at retreat. (Info sheet distributed to committee)
  - Perhaps have liaison member for ITS
  - (Next meeting discuss what the relation ITAC will have with ITS dept.)
  - What is appropriate, etc. Dr. Balfour has some ideas on this issue
- Article will be sent to David Sweeney: “Making Central and Decentralized IT work together.” Author from Utah State University.
  - David Sweeney will send out to the ITAC committee and will be discussed as possible IT Trend