

Attendees:

Reidar Bornholdt, Manny Gonzalez, Hristo Mihovski, Charlotte Nichols, Brent Powers, Soumitra Sengupta, Bob Sideli, Fedor Syagin, Max Ulitskiy, Bill Wozniak, John Zimmerman

Guest speaker and presenter:

Rama Balasubramanian

Opening Remarks and Discussions

- Robert Sideli, Chief Information Officer, CUMC IT, shared with the group an interesting piece about a website called “Realage” that would entice viewers to key in personal information to arrive at a “real” health age vs. “calendar” age. As users are asked to leave behind their e-mail addresses, the information so collected may be used by drug companies to send out promotions.
- John Zimmerman from the Dental School of Medicine informed the group one of their departments recently asked for workstations to be set up within a day after they arrived. Such requests are hard to fulfill as they come without any pre-planning. So he mentioned that Purchasing now requires a project plan to be in place so that planning is done ahead, before systems are purchased. A couple of other such examples for quick set up were cited: Charlotte Nichols about iPhones and Dr Sideli on Russ Berrie’s request to put up a system on the network right away. Dr Sengupta, Chief Security Officer, CUMC IT said it has been a practice over the years that a department would buy systems and ask them to be quickly set up after they are received without planning with IT.

Identity and Access Management: Presentation and Discussion

- Rama Balasubramanian, Director, Identity and Access Management, CUIT was introduced to the attendees by Charlotte Nichols, Asst. Vice-President, CUMC IT.
- Rama Balasubramanian made a presentation on Identity and Access Management (IAM) implementation in CUIT. The presentation was discussed extensively immediately after opening remarks. (For a soft copy of the presentation, please [click here](#)).
 - Rama Balasubramanian opened his presentation with the IAM group’s mission statement about managing identities in CUIT so that the university and its constituents can have a consistent, timely, secure, seamless, and reliable access to electronic and physical assets.
 - He gave an overview of the Lenel security system recently implemented in CUIT. Lenel manages cameras and controls access points in the campuses, housing and dining facilities, ID centers, and fitness centers in CUIT.
 - Dr Sengupta added that NYP is on Lenel and they may be using Identipass.
 - Rama Balasubramanian stated that IAM manages provisioning and access lifecycle from the creation of UNI very well. Thru IAM real-time identity enrolment is possible by DIAs and the ID cards use contact less technology.
 - Charlotte Nichols asked if IAM would support print page quota level functionality for students. Rama Balasubramanian replied in the affirmative and said IAM can support passing queries from the ID card to a database to define how many pages can be printed or cannot be printed.
 - John Zimmerman spoke about the issues in defining what affiliations have to be used for provisioning. He said sometimes affiliations could run into tens or even more than a hundred. Rama Balasubramanian clarified that thru IAM affiliations can be built into groups and the IAM service can work on group querying to mitigate issues in defining affiliations. Rama Balasubramanian also clarified later in the presentation that the WIND upgrade does not truncate affiliations, even if they are more than one hundred.
 - Dr Sengupta wanted to know what component in IAM manages identities. Rama Balasubramanian gave an architectural overview and stated that SIS and PeopleSoft are the primary systems that feed into IAM.

- In one of the points around IAM, Rama Balasubramanian shared with the group that the system failed over within 300 seconds and it was very impressive. This statement generated a few points for discussion:
 - For a question from Dr Sengupta on where the servers were located, Rama Balasubramanian informed that they were located in their Computers and Philosophy departments.
 - Bill Wozniak, Network Design Manager, CUMC Dean's Office, wondered if the servers failed what effect it would have for example on accessing doors here in CUMC. For this the presenter clarified that the system in such a scenario returns to what the default definitions are – default definitions being those laid out by Public Safety on a case by case basis.
- Another point highlighted by Rama Balasubramanian was that the new upgrade of Lenel supports usage of energy and cost efficient Point of Ethernet (POE) readers.
 - Bill Powers, Manager, Pathology outlined that these readers may cost about \$15,000 a piece.
- Rama Balasubramanian gave a structural overview of how Shibboleth, the protocol behind IAM, works. He said IAM supports scalability and supports federation. He said for example, CUMC could have five different disparate applications each calling for usernames and passwords. Someone for example from Rutgers can access these applications using their Rutgers credentials. He explained in detail the concept of Service Provider and Identity Provider in a Federation. He said the Service Provider talks to the Identity Provider to grant access to services.
- This interaction between the Service Provider and Identity Provider was illustrated with an example: Let us say a user Dr Ginsberg wants access to CTSA Wiki. CTSA, the Service Provider would like to know his affiliations. When Dr Ginsberg chooses Columbia on CTSA Wiki, the Service Provider (in this case CTSA Wiki) will talk to the Identity Provider (in this case Columbia) through Shibboleth protocol. Based on the affiliations returned by the Identity Provider (in this case Columbia) the Service Provider (in this case CTSA Wiki) grants access to the requestor (in this case Dr Ginsberg) trusting the Identity Provider (in Columbia's case Wind authentication).
 - Manny Gonzalez, Director, Core Resources questioned if audit trail reports can be obtained from the Service Provider on what the requestor actually did. Rama Balasubramanian informed that this functionality is outside of the scope of IAM. He elaborated that in the IAM framework, the Service Provider deals with authorization while authentication is managed by the Identify Provider. For example, authorization defines what areas the user can access while authentication defines who the user is.
 - Dr Sengupta wanted to know how IAM would address authentication issues when systems are outsourced. The presenter outlined that as long as the vendor supports Shibboleth, this is not an issue and IAM would support vendor access quite easily.
- Rama Balasubramanian said that OAD (formerly UDAR) went thru UNI activation without SSN using IAM. He said that IAM simplified password resets by matching a series of questions. This does not call for the user calling the help desk for password resets.
- He also said that IAM can be configured to send automatic DIA expiration notifications.
- He also mentioned that Departmental Administrators in IAM are those who have access to managed self services in PeopleSoft. Charlotte Nichols brought up the question that someone who has access to a cost code can see everything about a department. This question was left open with a thought from the attendees that PeopleSoft needs to be used to better define divisions.
- Rama Balasubramanian stated in detail other features like submitting photos from the web, and disabling IDs from the web, Kerberos and Active Server UNI synchronizations supported through IAM.
- Dr Sengupta and Dr Sideli thanked the guest for the presentation.

Closing Remarks:

- Dr Sideli asked the group to submit topics for the next meeting, (date for which is yet to be decided).