

Why TIER?

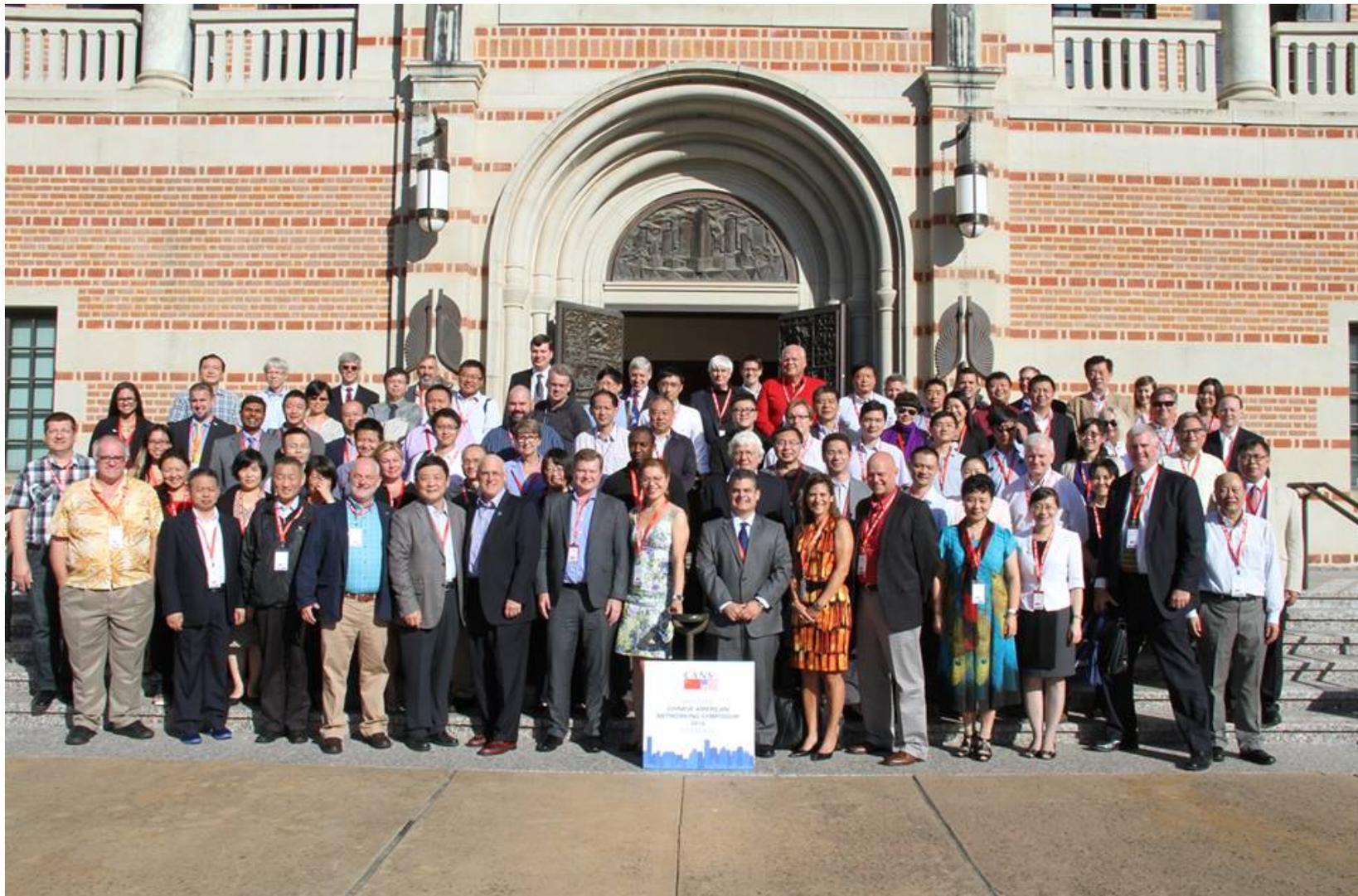
Dean Lane

*Manager of Identity and Access
Management*

Rice University, Houston, Texas, USA



RICE



About Rice

- William Marsh Rice was founded in 1912
- Research University located in Houston, Texas, USA
- About 15,000 active accounts
- 4,000 undergraduate students
- 2,700 graduate students
- 665 faculty
- 2,700 staff
- 870 visitors



Who am I?

- My name is Dean Lane
- Graduated with a BS in Computer Science from the University of South Carolina in 1990
- Jobs in the Oil & Gas industry doing software development and Unix/Linux system administration
- Started working at Rice in 1998
- Designed and developed our Identity Management System
- Became the Manager of our new Identity and Access Management group in 2015



RICE

IAM Group

- Staff of 5 people (myself included)
- Varied skills and abilities
 - Software development
 - Systems Integration
 - Cloud Systems Management
 - Linux Administration
 - Active Directory Administration
 - Database Administration
 - Door Access System Management
- Responsibilities
 - Directory Services (389 Directory Server and Active Directory)
 - Authentication & Authorization Services (Single Sign On - SAML & CAS)
 - Groups Service (Grouper)
 - Certificate Service (InCommon Certificate Manager)
 - Provisioning & Deprovisioning (local accounts & cloud services)
 - Cloud Service Management (Google, Box)
 - Physical Door Access & ID Card System (CBORD)



RICE

Our Issues

- Small staff
- Home grown system that was built 12-15 years ago
- Has been expanded multiple times with various technologies: perl, PHP, Java
- Business logic is spread out over multiple components
- In some cases different implementations of the same business logic exists that produces different results
- System has become fragile and complex as it has been extended over time
- It is now difficult to handle new situations, new populations, new work flows
- System is slower than we would like due to it's heavy reliance on polling
- Due to constant maintenance, we lack the time for the proper development of a new system

TIER to the rescue

- TIER, Trust and Identity in Education and Research
- Internet2 started the TIER project in 2015 but it includes and consolidates work that has been going on in Internet2 for over a decade
- The project is focused on two areas:
 - producing an open-source, community-developed identity and access management suite
 - on the practices, standards and community alignment that comes from adopting a common approach to identity and access management



TIER Major Components

- **Entity Registry**
 - COmanage
 - Midpoint
- **Authentication & Federation Services**
 - [Shibboleth](#) (SAML)
 - OAuth
 - Consent Service
- **Groups Service**
 - [Grouper](#)
- **Provisioning Service**
- **Integration Services**
 - used to tie all of the components together
 - enables event based processing
 - REST based API to each of the above components

* [Blue](#) - currently using the stand alone package

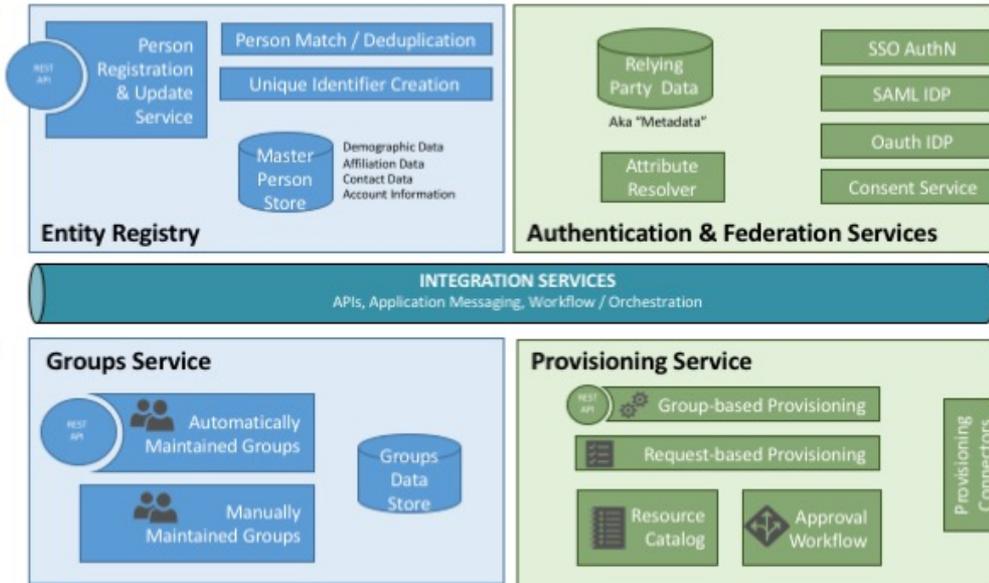


RICE

Identity Sources



The TIER Architecture



Identity Consumers



TIER Advantages

- Modular architecture, where parts can be replaced as needs change
- Best practices common with other institutions
- Event driven, near real time changes
- Ability to leverage components built and tested at other institutions
- Ability to develop components that can be shared with other institutions
- Ability to consolidate business logic flexibly through groups
- Improved monitoring and metrics
- Better scalability
- Because the components are loosely coupled, it will be easier to add enhanced functionality

TIER Campus Success Program

This summer TIER introduced the TIER Campus Success Program.

The TIER Campus Success Program will include a diverse group of higher education institutions committed to adopting and deploying the TIER software components and helping to accelerate adoption for the rest of the trust and identity community.

The goals of the program include:

- **assisting campuses in the successful deployment** of one or more TIER-packaged components to address one or more campus need(s)
- **accelerating local adoption** of TIER components so the community has guidance more quickly
- **providing lessons learned** about the local challenges and solutions and developing the first deployment guidance and advice for later adopters in the form of presentations, project reports, and locally produced TIER-related artifacts
- **informing the TIER program** about issues encountered in production implementation and provide data for

TIER Major Components at Rice

- **Entity Registry**
 - COmanage
 - **Midpoint**
 - **Authentication & Federation Services**
 - **Shibboleth** (SAML)
 - OAuth
 - **Consent Service**
 - **Groups Service**
 - **Grouper**
 - **Provisioning Service**
 - **Integration Services**
 - used to tie all of the components together
 - enables event based processing
 - REST based API to each of the above components
- * **Blue** - currently using; but will transition to the TIER package
- * **Red** - new TIER components to replace or enhance existing parts of our system

Rice and TIER

Through the TIER Campus Success Program, Rice hopes to not only replace our aging infrastructure but to also move to a more standard scalable solution that will enable us to answer the needs of the future.

We are very excited that through this process, we will be able to give back to the community and help other institutions that will come along later. And as we move forward, any integrations or components that we add to the architecture will be more easily shared back to the community thereby helping everyone.

More Information

- TIER - <https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/>
- TIER Software and practice components - <https://www.internet2.edu/vision-initiatives/initiatives/trust-identity-education-research/tier-components/>
- TIER Campus Success Program - <https://spaces.internet2.edu/x/oQrABg>
- TIER Grouper Deployment Guide - <https://spaces.internet2.edu/x/PpmTBg>
- TIER Reference Architecture - <https://spaces.internet2.edu/x/VgvcBQ>