MACE Grouper at Brown University

James Cramton

March 12, 2008

Topics

- What is MACE Grouper
- Business problem
- Brown's solution
- Grouper Demo
- Lessons Learned
- Next steps
- Access Management Survey

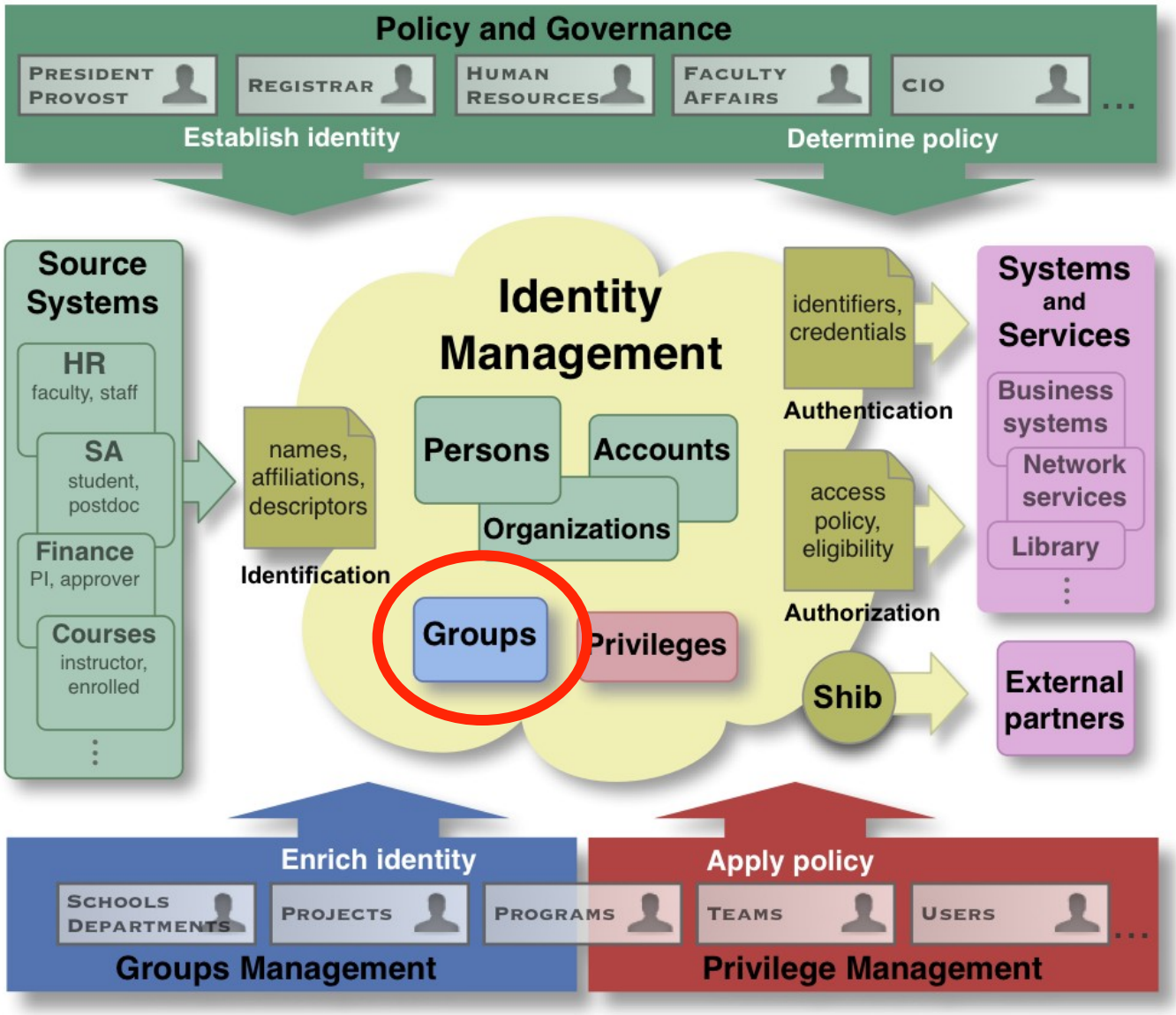
BROWN

Introducing MACE Grouper

- Open source group management toolkit sponsored by Internet2 MACE
- Java API and UI for managing groups
- Web service to be released mid-2008
- Allows automated group provisioning from multiple sources (RDBMS, flat files, LDAP)
- Allows delegated group management
- Allows automated group provisioning to multiple destinations (LDAP, RDBMS)

BROWN

IdM Landscape



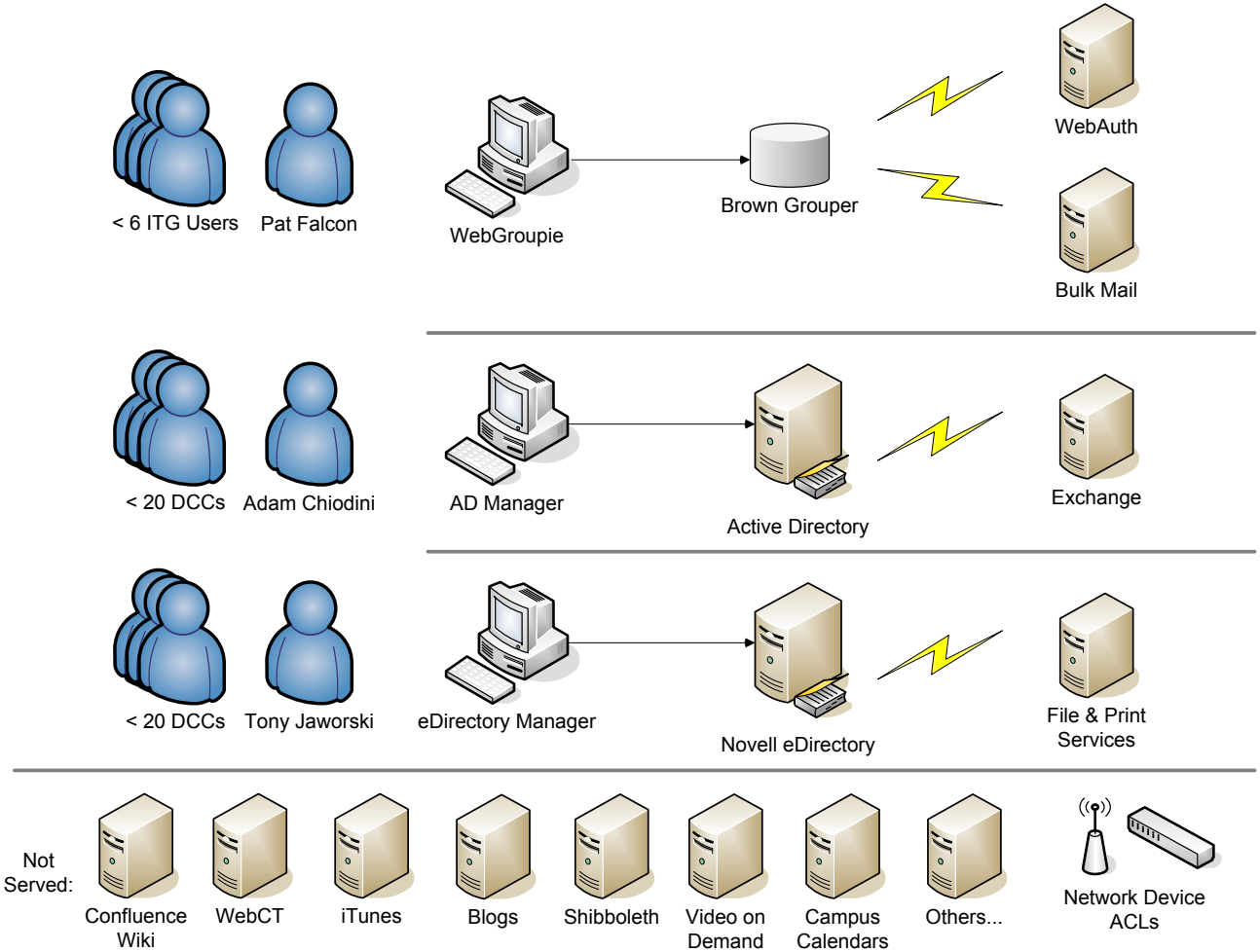
BROWN

Motivating Assumptions

- A growing suite of applications use groups
- Application authorization requirements are growing more complex and fine grained
- Need to delegate group management to scale
- Growing demand for federated access to Brown applications and services
- Together, these represent a vastly expanded use of groups and attributes

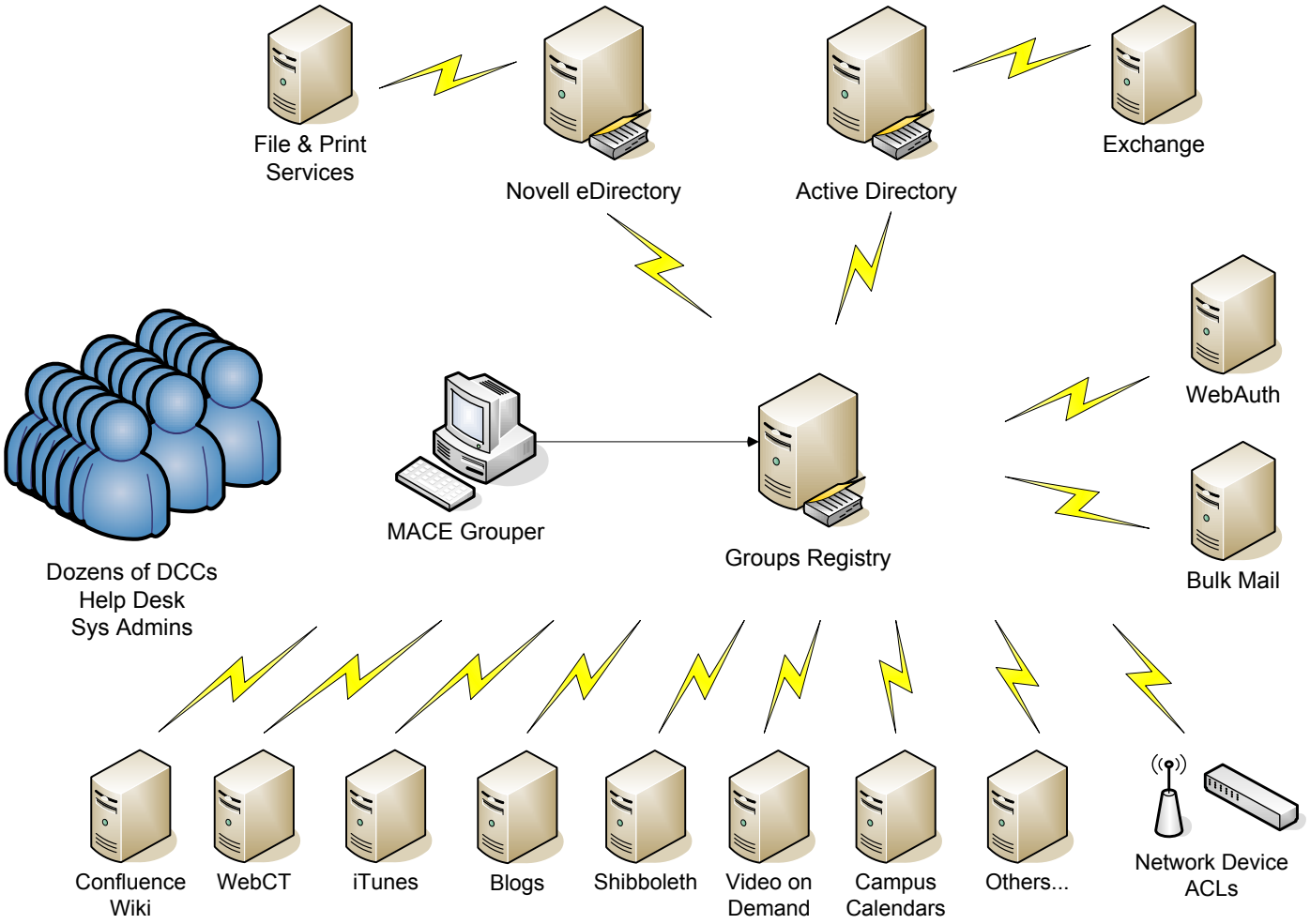
BROWN

Problem System



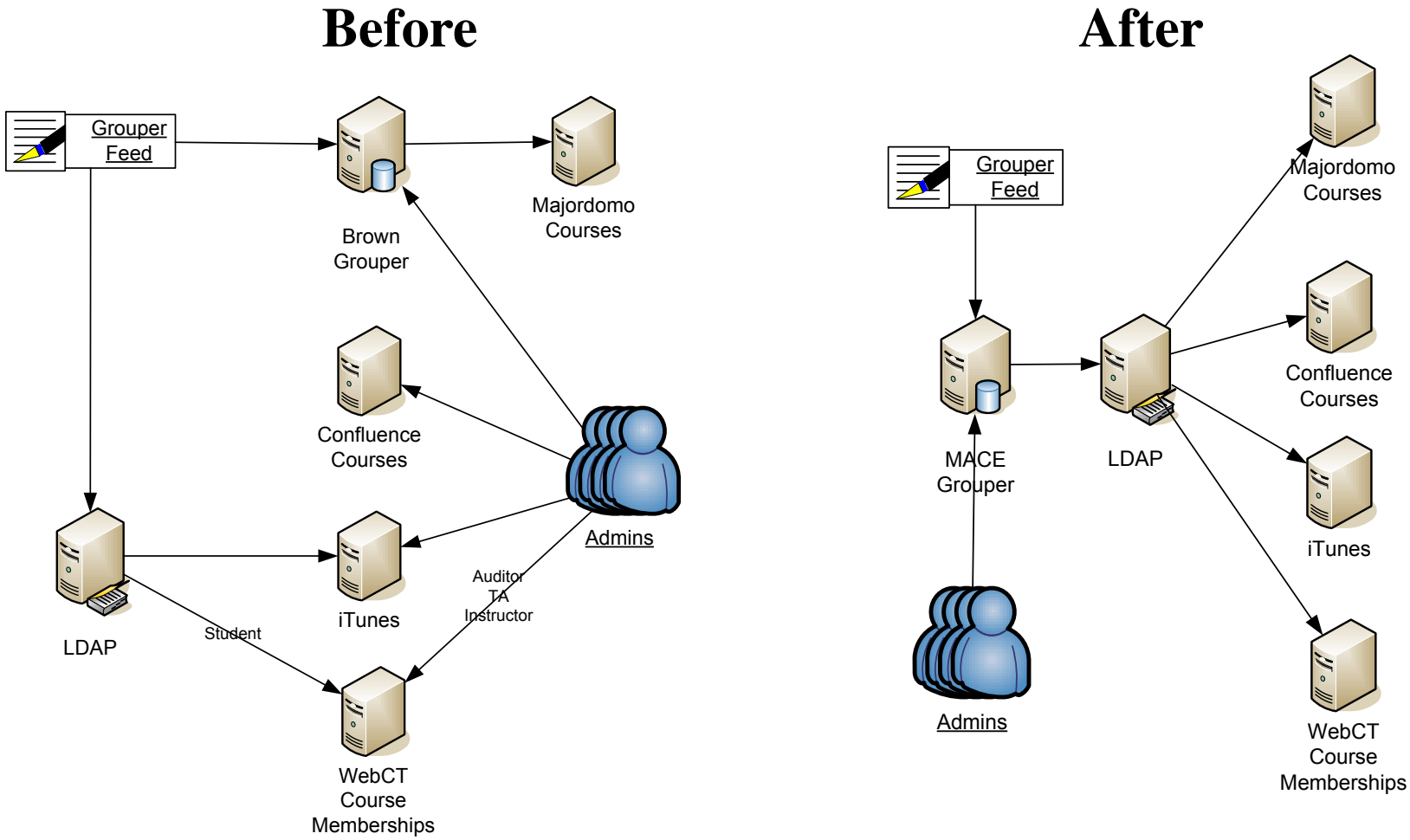
BROWN

The Solution



BROWN

Scope of Initial Phase



BROWN

Brown's Group Statistics

- Production launch at start of Fall semester 2007
- Limited to course groups
  - 2,500 'real' courses; 4,500 with independent study
  - 14 groups per section → 60,000 course groups
- Nightly provisioning takes 2 – 3 hours
- LDAP provisioning takes 15 minutes – 1 hour
  - Runs continuously after nightly provisioning
  - Replicates ad-hoc changes in near-time (15 minutes)
  - Still working to implement real-time LDAP group updates
- Demographic groups using legacy Brown Grouper

BROWN

Brown Course Group Schema

- Course : [Subject] : [Number] : [Term] : [Section]
  - All
    - **Administrator**
      - **Instructor** (Provisioned)
      - **TeachingAssistant**
      - **Manager**
    - Contributor
      - **ContentDeveloper**
      - **Mentor**
    - **Learner**
      - Student (Provisioned)
      - Auditor
      - Vagabond

[brackets] indicate dynamic data
Bold indicates eduCourse/IMS compatible role

- Schema is flattened to provision LDAP
  - 12 groups per course provision hasMember attribute in Groups ou
  - Person objects get isMemberOf pointers to groups

BROWN

MACE Grouper Demo

BROWN

Lessons Learned—Integration

- Write good documentation
  - 40 pages of concepts, role mapping, plus Grouper and application tasks
- Test with the most representative data possible
  - Mid-term data not always representative—too little change
  - Beginning of term data causes more change—and longer run time
  - Be prepared for a lengthy support cycle after launch
- Application 'support' for external groups is variable
  - Some integrate directly with LDAP ~ natively (iTunes, Majordomo)
  - Some use separate provisioning scripts (WebCT)
  - Some suffer loss of usability with thousands of groups (Confluence)
  - None pay any attention to group ACLs—use single bind dn
- Application needs vary by course or group
  - Some need section-specific course groups
  - Some need multi-section course groups
- Few performance problems in the Grouper UI
- LDAPpc provisioning needs performance and feature improvements
- Provisioning LDAP from group attribs would allow more flexibility

BROWN

Lessons Learned—Group Management

- Limit initial release audience to manageable, trusted group
- Demographic groups are a big challenge
  - 10 years of legacy demographic group evolution is a mess
  - Legacy demographic groups have redundancy and transparency problems
  - Can't clean up part of the legacy data without addressing all groups
- Demographic group resolution gating factor in deploying applications
  - WebAuth
  - Wifi
  - Bulk Email
- Naming conventions take a long time to define
  - Accurately representing existing uses of groups
  - Maintaining standards compatibility (eduCourse/IMS)
  - Catch-all group important in course schema
- Widespread use will require exposure of implications of actions
  - Lay users will need a clear understanding of how changes impact apps
  - GUI troubleshooting tool awaits in Nirvana

BROWN

Lessons Learned—Requirements

- Involve the stakeholders early and often
- Real-time provisioning is critical to user experience
- Distributed MACE Grouper UI is ‘too full-featured’
- Need to provide group, privilege, and service management app to Brown community (‘Gateway’)
- Support multiple semesters
- Balance is the key to design and policy
  - Complexity vs. features
  - Central group definitions vs. custom group privileges per app
  - Conceptual shift from “Confluence Groups” to “Just Groups”

BROWN

Next Steps for Brown

- Identify who manages groups
- Allow lay people to manage their groups & privileges
  - Must convey implications of group & privilege changes across apps
  - Developing a ‘services portal’ to automatically activate selected services for specific groups—by lay people
  - Both imply more granular control of privileges
- Message-based provisioning
  - Provide real-time change availability
    1. From Grouper to LDAP—may require grouper web service
    2. From HR or course management systems to Grouper
- Enforcement of group ACLs from within applications
  - Apps should not expose existence or membership of some groups
  - Have yet to see an application support this
  - Probably can be achieved by removing capabilities from apps
  - May require exposure of privilege management to community

BROWN

Discussion

- Presentation and other materials available in session notes at educause.edu

  http://www.educause.edu/NC08/Program/139211?PRODUCT_CODE=NC08/SESS3

- But wait, there's more…
  Internet2 MACE's Access Management Survey

BROWN

Access Management Survey

- Organized by Internet2 MACE
- A self-assessment tool, not a competition
- 2 questionnaires
- 8 universities
  - comprehensive research institutions
  - public and private
  - 7,000 – 51,000 students, faculty and staff
- Respondents asked to include a small campus group to answer questions

BROWN

Questionnaire #1

- Open-ended questions about
  - Respondents' access management initiatives
  - Drivers that led to the launch of the initiative
  - Steps taken to address the drivers
  - New capabilities that will exist at the end of the initiative
  - Knowing when it is time to consider access management initiatives

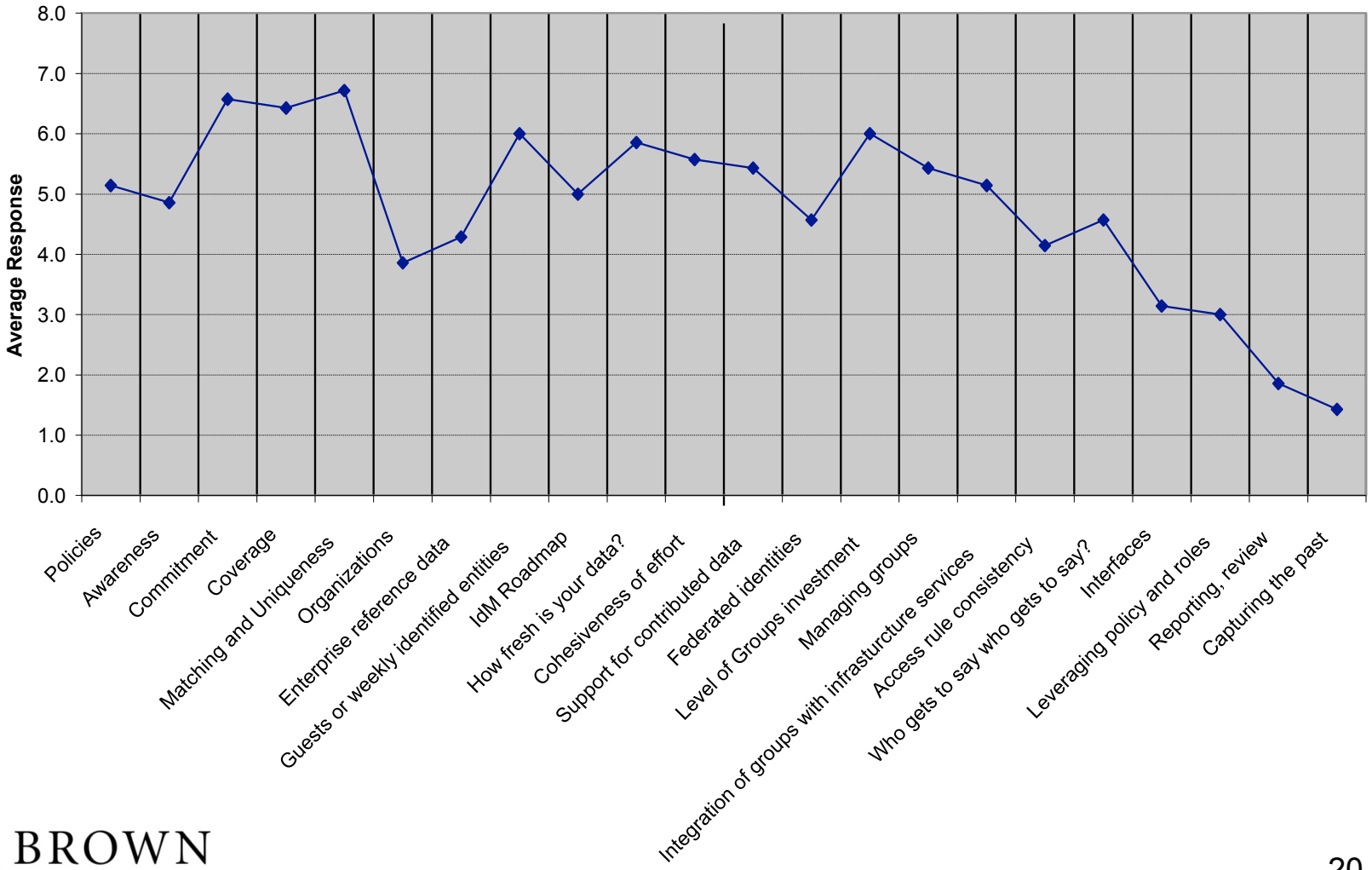
BROWN

Questionnaire #2

- Maturity of current policy, infrastructure, and operational practices related to access management
  - Data stewardship, sharing & re-use
  - Who's in our IdM systems
  - IdM roadmap, operations & auditing
  - Groups & basic access management
  - Roles & privilege management

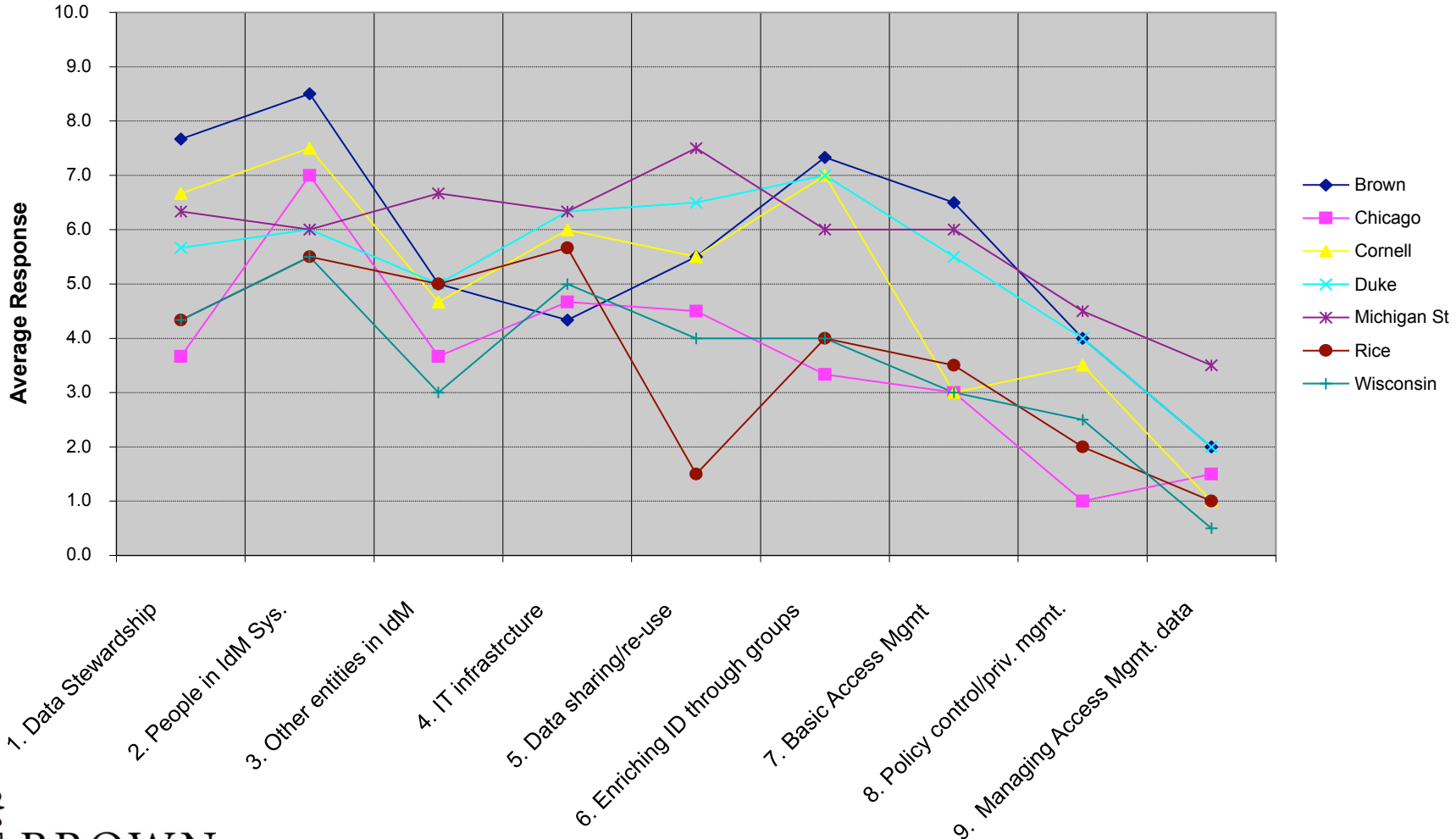
BROWN

Campus Average Responses



BROWN

Overall Section Scores



BROWN

Key Points from Survey

- Extremely useful self-help questionnaires
- Each institution has self-identified strengths and weaknesses
- Most campuses are weak in:
  - External entities in IdM
  - Policy, control & privilege management
  - Managing access management data
- Full results posted to session notes at
  http://www.educause.edu/NC08/Program/139211?PRODUCT_CODE=NC08/SESS3

BROWN