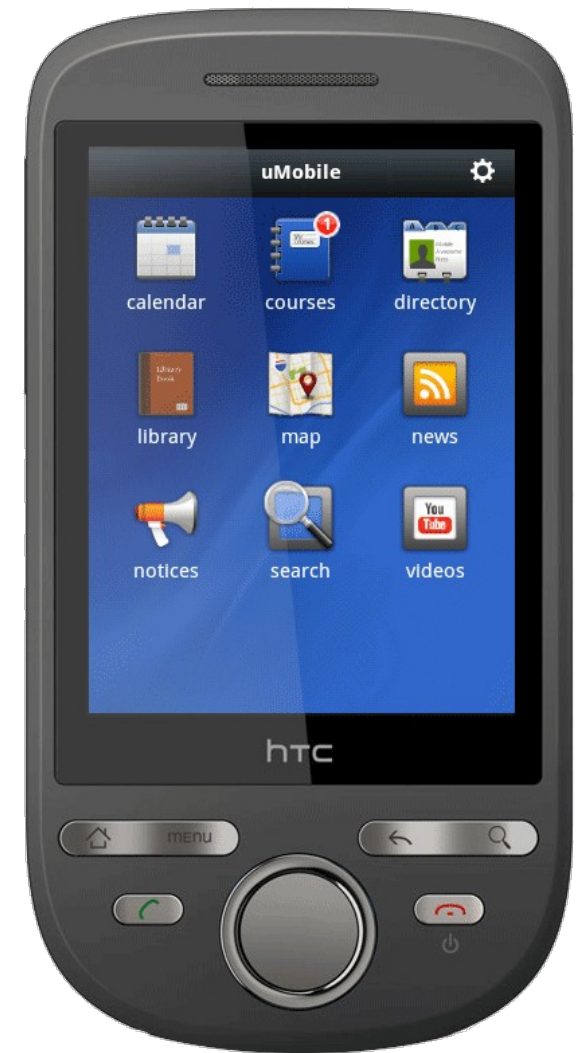


# uMobile and Identity

# Jasig uMobile Project

- Native mobile apps
  - Android and iOS
- Mobile web site
- Personalized experience
- Using uPortal infrastructure for back-end services
- Using CAS for SSO
- Just used for Jasig Conference
  - <http://umobile.unicon.net>



# Mobile Identity Challenges

- Same challenges as any enterprise application
  - Authentication, Authorization, Access Control, Directory Access, etc.
- Authentication is the most “Affected”

# Authentication Challenges

- Mobile users expect to log in just once. Ever.
- Credentials should be persisted and reused until user elects to signout.
- Need persistent uPortal authentication while accommodating Proxy CAS.
- Might need to support CAS ClearPass (password replay).
- Also need to support anonymous / guest view.

# Possible Authentication Strategies

- Local Cached Credentials
- CAS OAuth
- CAS “Remember Me”

# Locally Cached Credentials

- Store credentials locally in application database/preference.
- Need to be able to retrieve cleartext version for reuse.
- Advantages:
  - Would enable ClearPass and Proxy CAS.
  - Easy to implement
- Disadvantages:
  - Obviously security vulnerabilities.

# CAS OAuth

- Standards-based
- Current mobile app “Best practice”
- Authenticate to CAS once and then retain long-term delegated authentication.
- Advantages:
  - Eliminates local storage of actual user credentials.
- Disadvantages:
  - Breaks ClearPass.

# CAS “Remember Me”

- CAS provides “Remember Me” module for repeated access without reentering credentials
- Involves greatly extending duration for Ticket Granting Tickets validity
- Advantages:
  - Works with ClearPass.
  - Easy to implement.
  - No locally stored credentials.
- Disadvantages:
  - Would make “Remember Me” available for traditional CAS auth as well, may not be desirable
  - Opting out specific relying applications is not well supported.