Using InCommon Client Certs for eduroam

Jeff Hagley and Ryan Martin
October 3rd, 2011
Internet2 Fall Member Meeting
Why we Chose to use InCommon Certs

• Provide implementation details and lessons learned for the R&E community
• Cost
• Infrastructure
• Future Plans
RADIUS Setup

- FreeRADIUS
  - CRL Checking
    - BASH script to update this
  - Common CA Cert Chain across InCommon
    - All InCommon Members have same signing Intermediate Cert
  - Only allowing Internet2 authentication
    - Proxy controls this
  - Cert Fragmentation Size
Cert Deployment Hierarchy

Organization: Internet2

- Department - Laptop
  - Lifespan of 4 years
  - No Escrow

- Department - Mobile
  - Lifespan of 4 years
  - No Escrow

- Future Plans...
  - Signing
  - Encryption
  - Etc...
Client Setup

• Used “+” sign in email address to issue multiple certs
  • Comodo added this after a bug report from us
  • Using “+” sign to get one user in more than one department
    • A hack we are hoping goes away in the future
    • Keeps email client from automatically using the cert for signing and encryption
OSs deployed on

- iOS 4.3.5 doesn’t work, previous versions do
- Mac OS 10.6 and 10.7 works
- Windows 7 works (limited experience, we are Mac people)
Documentation and Policies

• Master Key Escrow Policy
• Certificate Revocation Policy
• FreeRADIUS setup information
• Installation on Clients
• Email Ryan for copies of any of them to use as a template
Issues

• iOS 4.3.5 issue
  • We would love to have others test this and report it to Apple
  • Bug ID 10080052
• OSCP and FreeRADIUS vulnerability
  • CVE-2011-2701
• Users can only be assigned to one department (Comodo is aware of this issue)
Future Plans

• OSCP implementation, after vulnerability is fixed
Contact Info

• Jeff Hagley – hagleyj@internet2.edu
• Ryan Martin – rmartin@internet2.edu