Securing Web Access with DCE

Brian C. Schimpf
Gradient Technologies Inc.
Client/Server Applications - Can They Meet the Demand

- **Long Development Cycles**
  - Application development typically > 1 year
  - Development for multiple Client Platforms
  - Limited distributed computing developers

- **Administration Nightmare**
  - Installation and administration of many and complex desktop client applications
Internet/Web - Why Such Rapid Acceptance?

- Standards based networking
  - "Standard" Web Browsers and Servers
  - TCP/IP everywhere
- Cheap and easy access
- Quick Application and Information Deployment
  - Tools easy to learn
  - Browsers easy to use
  - Applications easy to deploy
Distributed Infrastructure

- Apply heterogeneous distributed computing infrastructure to Web accesses
- Location independence of servers via directory service
- Security infrastructure that provides:
  - strong user authentication (Kerberos)
  - data protection (integrity and privacy)
  - flexible and convenient authorization model
Three-Tier Architecture with DCE Web
Authorization Model

- Authorization performed by the server which controls the resource being protected
- Authorization model based on identity including group membership
- Authorization information contained in an ACL using a standard format
- DCE ACL model is extended to support sparse ACLs
Sparse ACLs

- Not necessary to create a separate ACL for each object in the hierarchy
- Objects without specific ACLs have an *inherited ACL* - ACL of superior object
- Inheritance is evaluated at access time as opposed to creation time
- Deleting an ACL makes it an inherited ACL
- Real ACLs can be created - inferior objects inherit new ACL immediately
Sparse ACLs (cont’d.)

Inherited ACL

Real ACL
DCE Web technology has been implemented as a product called *WebCrusader*

Based on work done by the Open Group Research Institute
Questions?

- For more information:
  - http://www.osf.org/www/dceweb/
- schimpf@gradient.com