

CS530

Authorization

Bill Cheng

<http://merlot.usc.edu/cs530-s10>



Authorization: Two Meanings

- ➡ **Determining permission**
 - Is principal P permitted to perform action A on object U ?
- ➡ **Adding permission**
 - P is now permitted to perform action A on object U
- ➡ **In this course, we use the first sense**

Access Control

- ➡ Who is permitted to perform which actions on what objects?
- ➡ Access Control Matrix (ACM)
 - columns indexed by principal
 - rows indexed by objects
 - elements are arrays of permissions indexed by action
- ➡ In practice, ACMs are abstract (not realizable) objects
 - ACM is huge and sparse
 - ACM is often distributed
 - instantiations
 - ACLs
 - capabilities