

Access Control

Implementing Access Control

Adam Doupé
Arizona State University

<https://pwn.college>

Implementation

- How to implement Access Control Matrix?

Access Control Lists (ACLs)

- Each column of the access matrix is stored with the object

<i>f</i>
<i>p</i> : rwo
<i>q</i> : a

<i>g</i>
<i>p</i> : r
<i>q</i> : ro

Capability Lists

- Each row of the access matrix is stored with the subject

p

f: rwo

g: r

q

f: a

g: ro

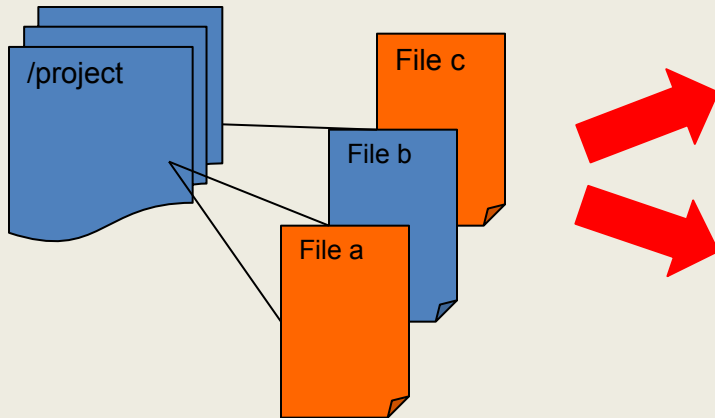
Relation

Subject	Access	Object
<i>p</i>	r	<i>f</i>
<i>p</i>	w	<i>f</i>
<i>p</i>	o	<i>f</i>
<i>p</i>	r	<i>g</i>
<i>q</i>	a	<i>f</i>
<i>q</i>	r	<i>g</i>
<i>q</i>	o	<i>g</i>

ACL vs. Capability

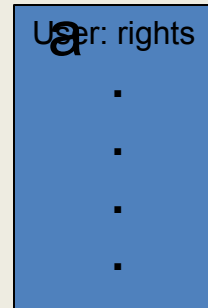
- ACL requires authentication of subjects
- CAP does not require authentication of subjects
 - Capabilities must be unforgeable and propagation must be controlled

ACL vs. Capability

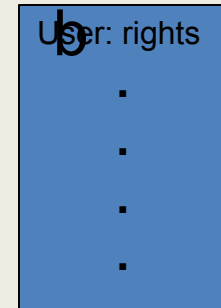


Per-Object basis

File



File



Per-Subject basis

use
r

Rights: File a, Rights: File b

ACL vs. Capability

- Least Privilege
 - CAP provides for finer grained least privilege control with respect to subjects, especially dynamic short-lived subjects created for specific tasks

ACL vs. Capability

- Access review
 - ACL better for access review of objects
 - CAP better for access review of subjects
- Revocation
 - ACL better for revocation on object basis
 - CAP better for revocation on subject basis

Capability Lists: Granting Access

- p wants to grant q read access to file f
 - How to do this?

p	$f: rwo$	$g: r$	
q	$f: a$	$g: ro$	
q	$f: ar$	$g: ro$	
q	$f: a$	$g: ro$	$f: r$