Instance-based Authorizations

Spring Security ACL PoC

Matthias Buehl, Nena Raab
October 9, 2018

1. Create an advertisement (instance to protect)

ACL permissions

read (R)
write (W)
admin (A)
- publish
- grant permission

owner
(R,W,A)

Create entries in table: acl_entry

acl_object_id	ace_order	mask	sid (user or role ID)
4711	0	1 (R)	12345
4711	1	2 (W)	12345
4711	2	16 (A)	12345

Create entry in table: acl_object_identity

id	object_id_class	object_id_identity	parent_object	entries_inheriting
4711	1 (advertisment class)	1	[NULL]	true

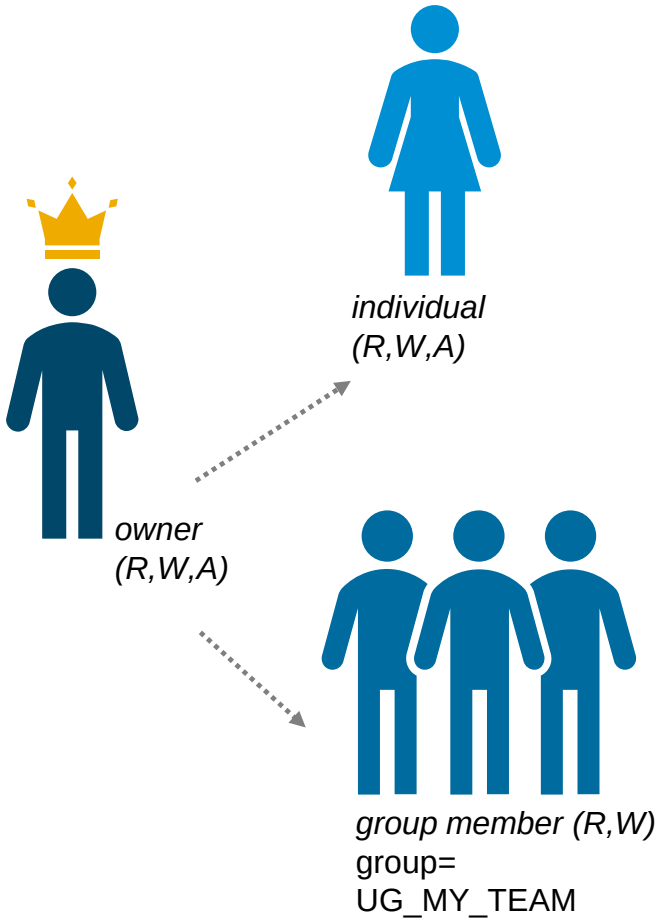
Create / use entry in table: acl_sid

id	principal	sid
12345	true	MUELLERW

create
view & update

advertisement lifecycle

2. Collaborate: grant access permission to individuals / groups



ACL permissions

read (R)
write (W)
admin (A)
- publish
- grant permission

Create entry(s) in table: acl_entry

acl_object_id (instance id, e.g. advertisement)	**ace_order**	**mask**	**sid**
4711	0	1 (R)	12345
4711	1	2 (W)	12345
4711	2	16 (A)	12345
4711	3	1 (R)	23456
4711	4	2 (W)	23456
4711	5	16 (A)	23456
4711	6	1 (R)	44444
4711	7	2 (W)	44444

Create / use entries in table: acl_sid

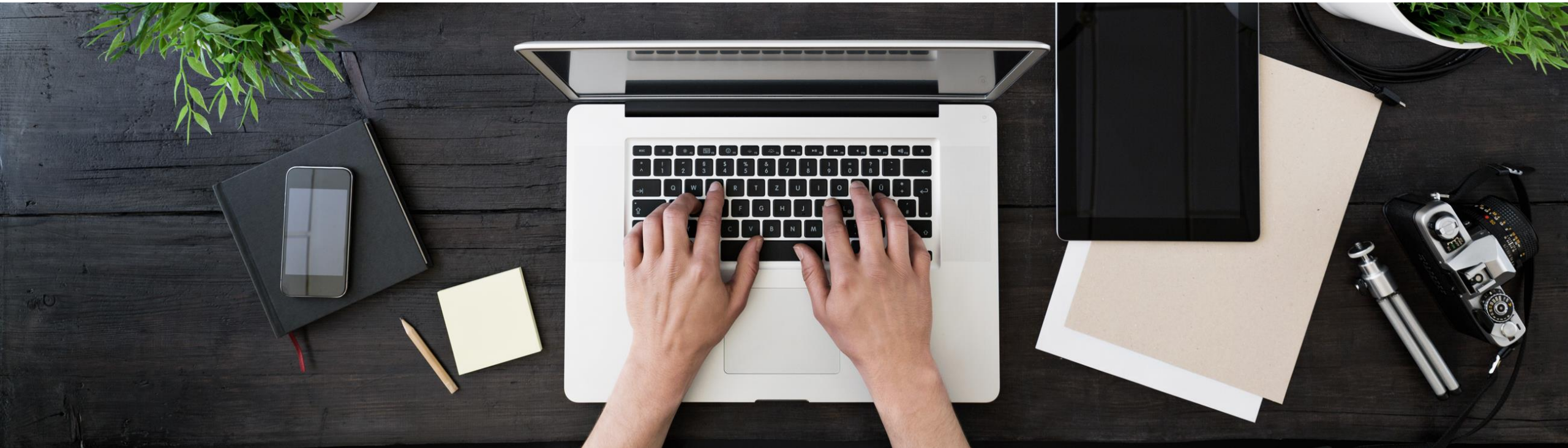
id	**principal**	**sid**
12345 (owner)	true	MUELLERW
23456 (individ.)	true	MEIERU
44444 (group)	false	UG_MY_TEAM

create
view & update

view & update (collaborate)

advertisement lifecycle

Demo: create advertisement and grant permission to others

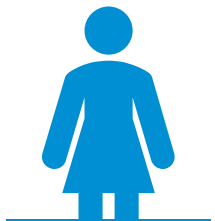


3. Publish advertisement to bulletinboard „DE_WDF03“

Publisher

- needs permission to „publish“

- needs access to target board (xs.user.attribute {board = DE_WDF03)}



Attr. board: DE_WDF03

individual (R,W,A)

Create / Use entry in table: acl_sid

id	principal	sid
12345 (owner)	true	MUELLERW
23456 (individ.)	true	MEIERU
44444 (group)	false	UG_MY_TEAM
55555 (board)	false	DE_WDF03

Create entry in table: acl_entry

acl_object_id	ace_order	mask	sid
4711	0	1 (R)	12345
…	…	…	…
4711	7	2 (W)	44444
4711	8	1 (R)	55555 (DE_WDF03)

create view & update

view & update (collaborate)

publish to bulletinboard(s)

view

advertisement lifecycle

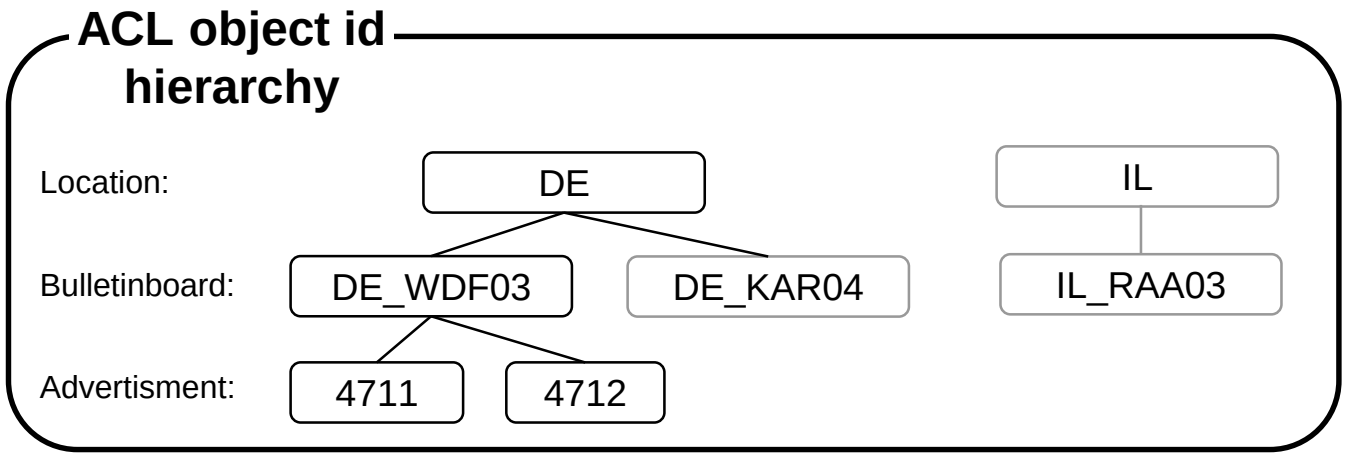
4. View published advertisements (with hierarchies)

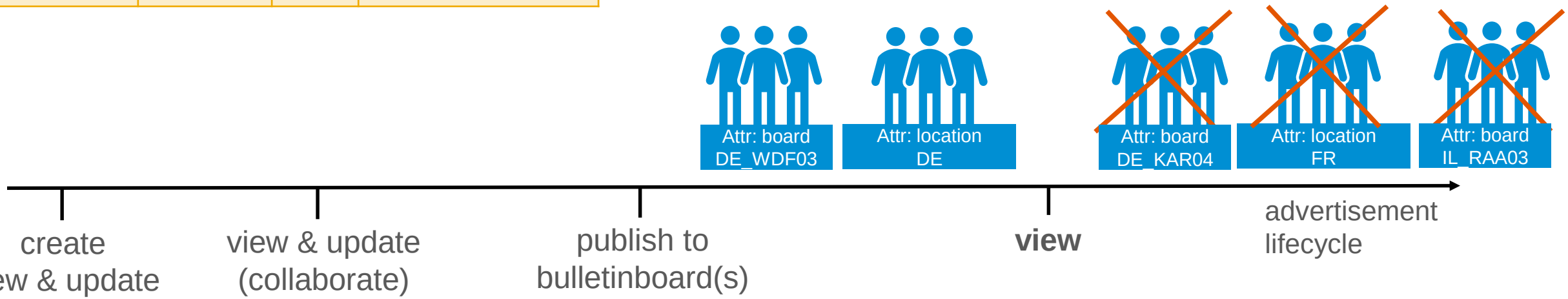
read entry(s) in table: acl_object_identity

id	object_id _class	object_id _identity	parent _object	entries _inheriting
4711	1 (advertisement class)	1	5816	true
4712	1 (advertisement class)	2	5816	true
5816	2 (bulletinboard attribute)	DE_WDF03	5812	true
5812	3 (location attribute)	DE	[NULL]	false

read entry(s) in table: acl_entry

acl_object_id	ace_order	mask	sid
4711	8	1 (R)	55555 (DE_WDF03)





Demo: publish advertisement and leverage acl hierarchies