PROTECTION IN THE BIRLIX OPERATING SYSTEM

Oliver C. Kowalski

Hermann Härtig

SECURITY QUESTION

Is a given subject allowed to perform an operation on a given object?

OUTLINE

1. protection paradigm at „user interface“ level
2. the implementation in BirliX
   (and a BirliX walkthrough while we’re at it)

PROTECTION MECHANISMS

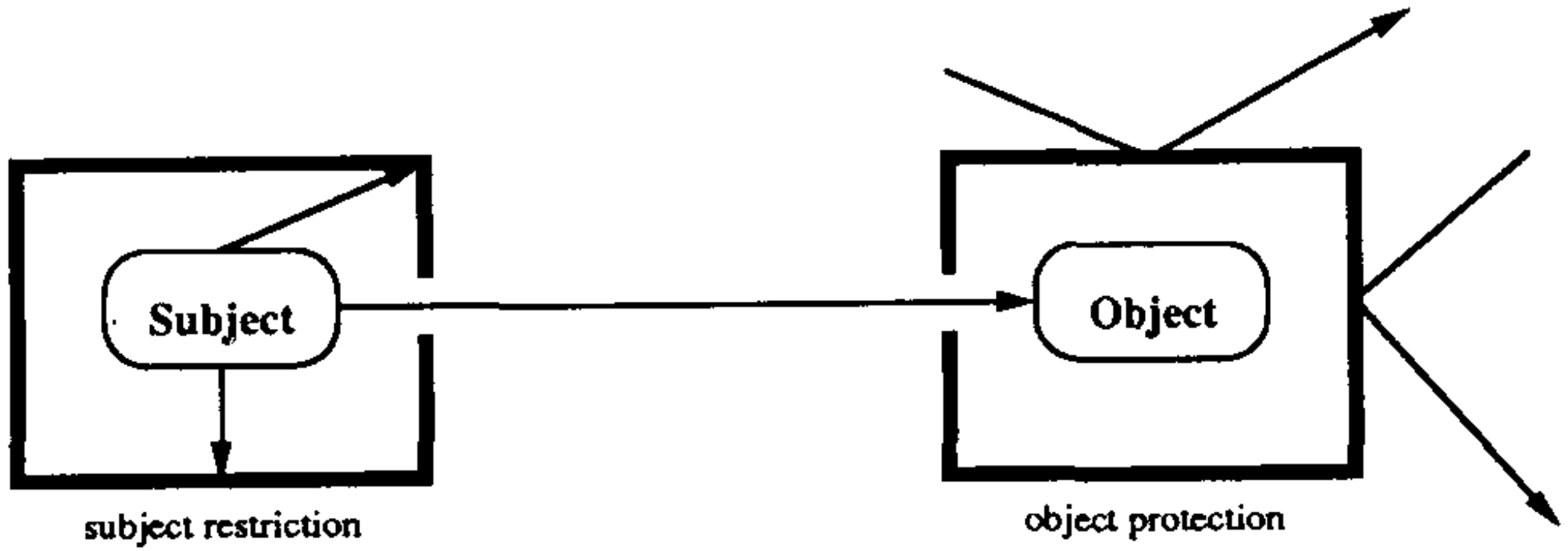
widely used limited ACLs (aka POSIX)

- entities acting as subjects are attributed to a principal (human)
- objects maintain a list of subjects and their rights

pure ACLs

- individual program instances as subjects
- not practicable with short-living subjects

COMBINATION



BIRLIX

BirliX terminology	The Real World™
abstract data type (ADT)	service, IDL
type description	server program
ADT instance (iADT)	running server
team	process, task
team manager	init, launchd
agent	client thread
native	cleanup thread, garbage collector
bindings	sessions
passive team	persistent snapshot
user representative (URep)	login

DISCUSSION

- relevance and novelty of BirliX concepts
- What have we learned since then? Have protection mechanisms improved?
- Is the combination of object protection and subject restriction the right compromise for usable security?
- „… in the second case it's a cryptographic seal. With this a user is able to grant trust to a workstation.“ Really?