

University of Regensburg
Department of Information Systems
Wolfgang Dobmeier, Günther Pernul



Towards Privacy-Aware Handling of Authorizations

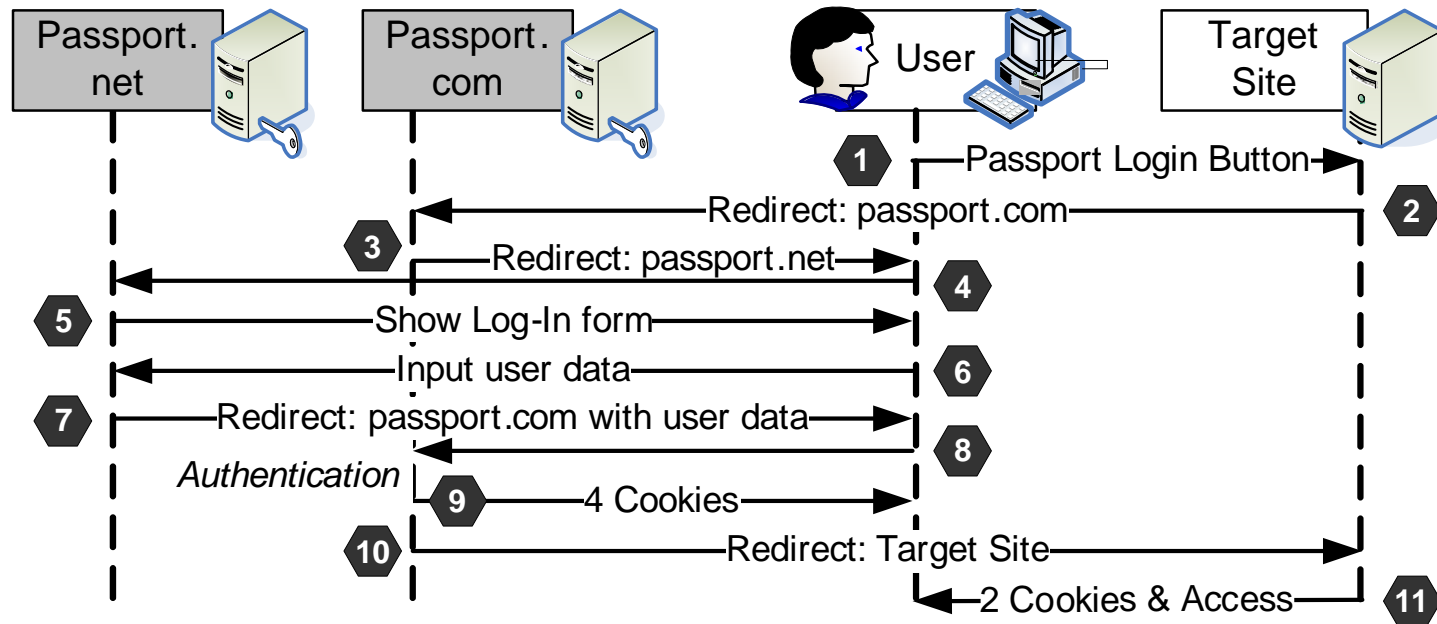
Policy 2007, Bologna, Italy

Security functionality and needed data

- Identification
 - Biometric data
- Authentication
 - Passwords, keys
- Authorization and access control
 - Policies, attributes
- Auditing
 - Log data

Centralised security data – the example of MS Passport

■ Single Sign-On Service for the Web



■ Today, it can be considered as failed

Issues with central storage and handling

■ Privacy

- User profiling
- Illegit distribution of information
- Compromise

■ Failure of central components

- Replication only partly helpful

■ Centralisation is antithetical to the distributed nature of the Internet [Kormann/Rubin, 2000]

Goals of our work

- The focus is on storage and processing of authorizations as these suffer from privacy problems, too
- We envision a system that tackles the aforementioned issues
- The user shall have some degree of control over how and where his authorizations are processed and stored („User Centricity“)

Partitioning of policies

- Policies consist of authorizations and apply to defined subjects and objects and different operations

- General criteria of partitioning:
 - Subject-, object-, or operation-oriented
 - Semantic criteria

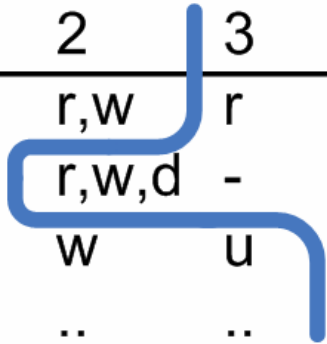
- Have to be applied to the different AC models

Matrix-based models

- Authorizations exist directly between subjects and objects as entries in cells of a matrix M
- Partitioning of M into submatrices via

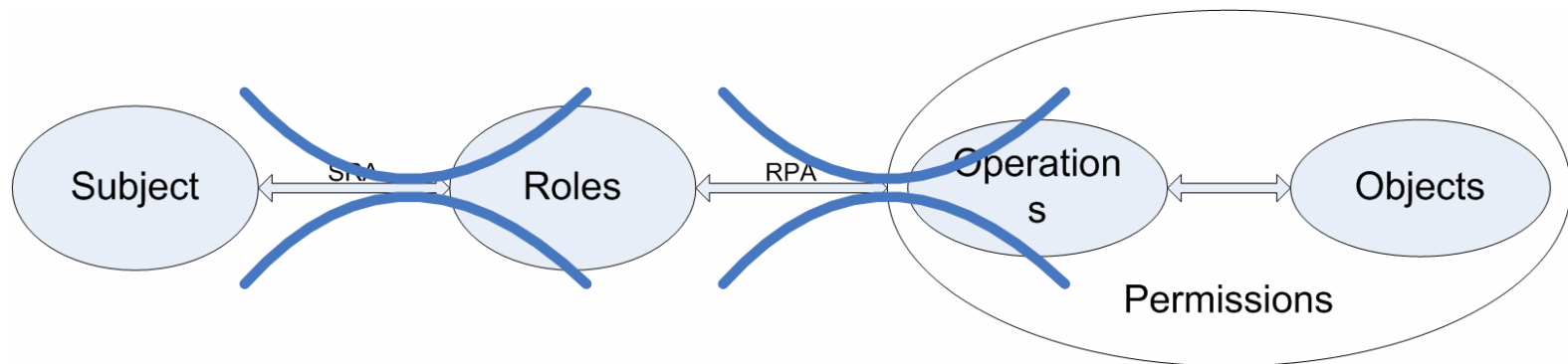
$$M_i : s \times o \rightarrow Op$$

	1	2	3	...
A	r	r,w	r	..
B	w	r,w,d	-	..
C	w	w	u	..
...



Role-based models

- The concept of a role as an intermediary between subjects and authorizations
- Role-permission and subject-role assignments can be split up



Attribute-based and mandatory AC models

- ABAC: dynamic authorizations
 - Subjects and objects are specified via a set of attributes and conditions
 - Techniques for hiding policies and attributes have been developed (e.g., Frikken et al. 2006; Li/Li 2006)

- MAC: authorizations are determined via a fixed set of rules plus metadata (clearance/classification)

- However, the processing of authorizations can be governed

Controlling the processing of authorizations

- Paradigm: User Centricity
- The user should be able to define
 - which PDP should evaluate the authorization
 - where the according policy is stored

Privacy implications

	Centralised Storage	Distributed Storage
Centralised PDP	All authorizations and their usage are known to a single entity.	Each authorization process, but only part of a user's authorizations is known to a specific PDP.
Distributed PDPs	All authorizations are known to a single entity but not the time of their usage.	Knowledge on user's potential and performed authorizations is distributed among distinct entities.

Outlook

- Further development of the approach
 - Impact on policy administration
 - Usability aspects
 - Trust relationships between participating entities

Thank you very much!

{wolfgang.dobmeier, guenther.pernul}@wiwi.uni-regensburg.de