Object Security Attributes: Enabling Application-specific Access Control in Middleware

Konstantin Beznosov

October 29, 2002

Distributed Objects and Applications, Irvine, CA

Overview

- Problem motivation
- Contributions
  - Classification of all solutions
  - Proposed generic solution
- Application to CORBA
  - Security Domain Membership Management (SDMM)

Conflict of Interests

Vendors:
- stable
- infrequently changing
- middleware security

Users:
- security decisions based on application-specific factors

Application-specific Factors

- Certain characteristic or property of an application's resource
  - Produced, modified and processed in the course of normal application execution
- Examples
  - Bank account's holders and their ranks
  - Phone numbers of telecom customer accounts
    - 5,000 changes/day with 10^6 subscribers

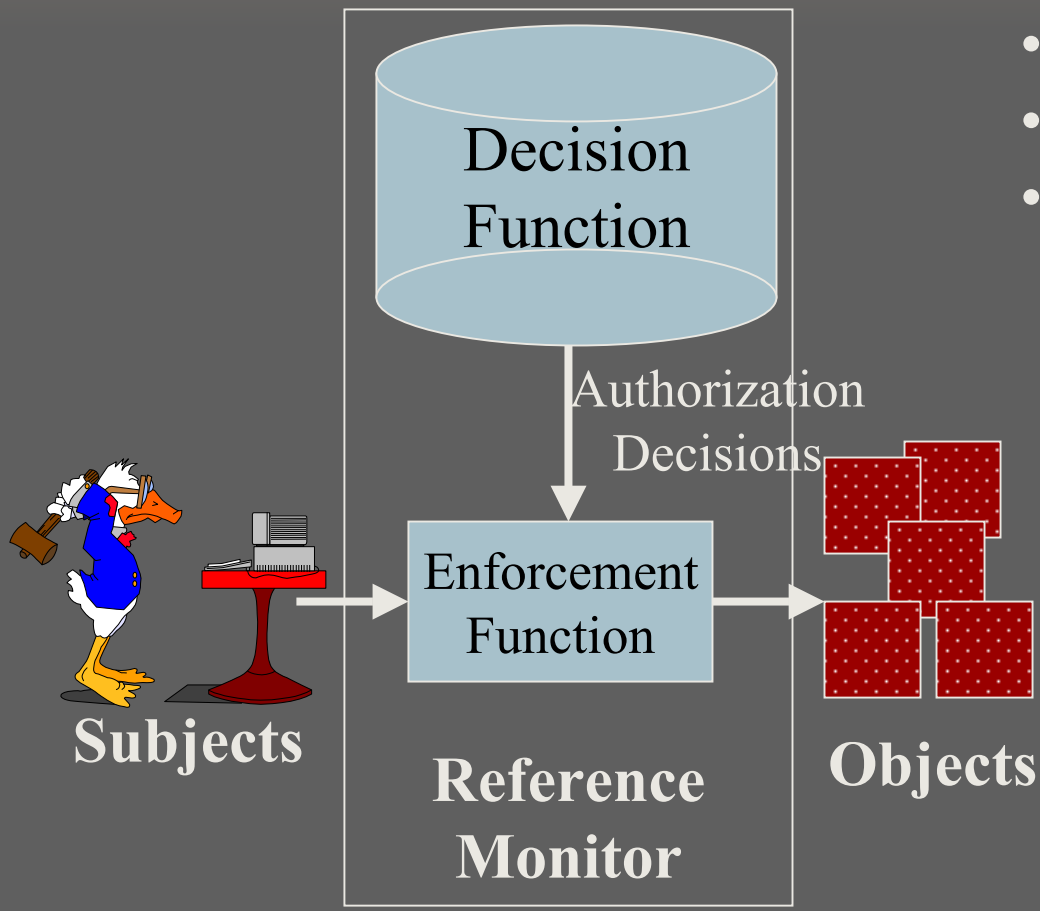
Main Problem Addressed

Keep middleware security generic and yet allow for application-specific security policies

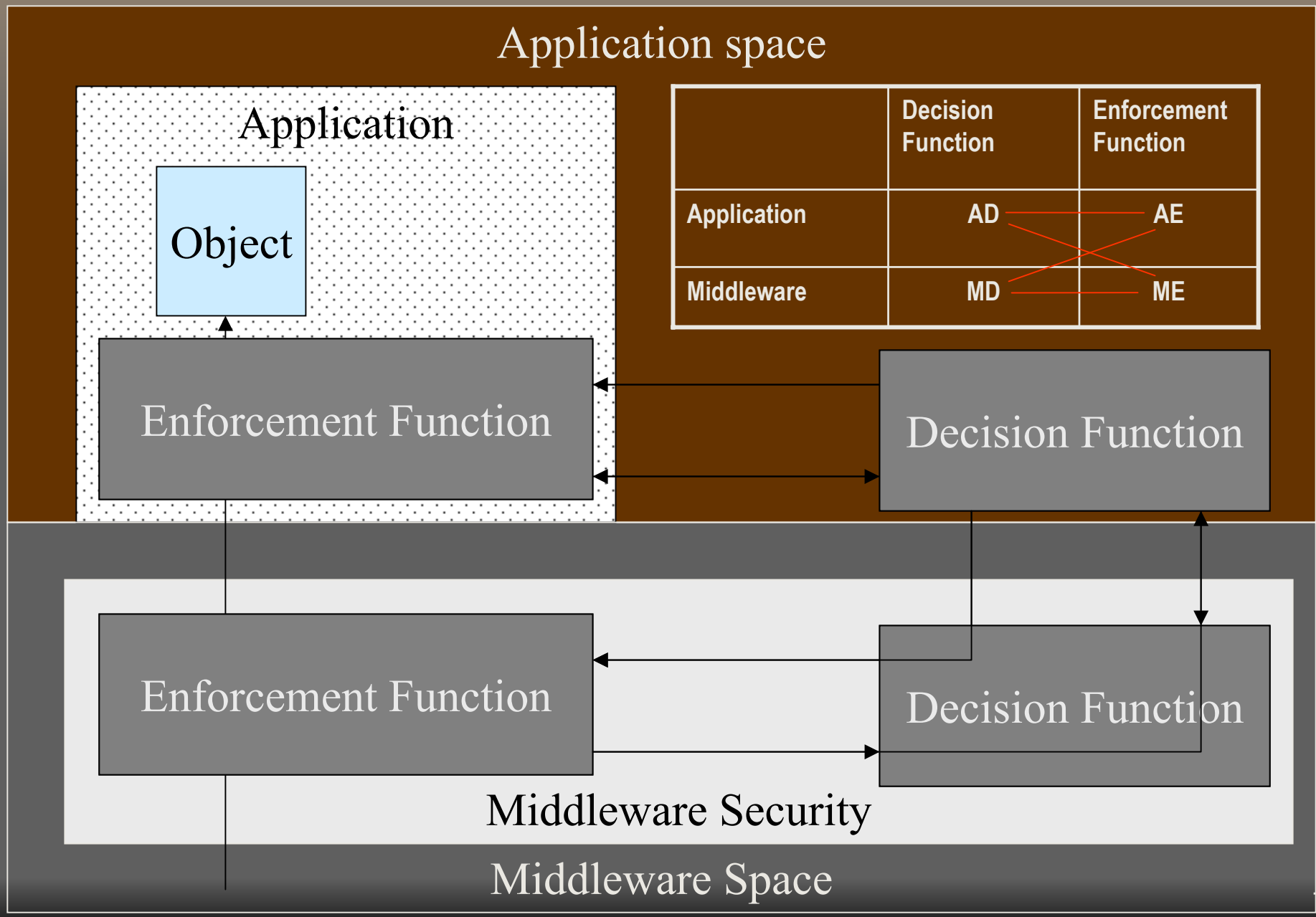
Solution: Additional level of indirection ☺

- Separation of concerns

Decision-Enforcement Paradigm

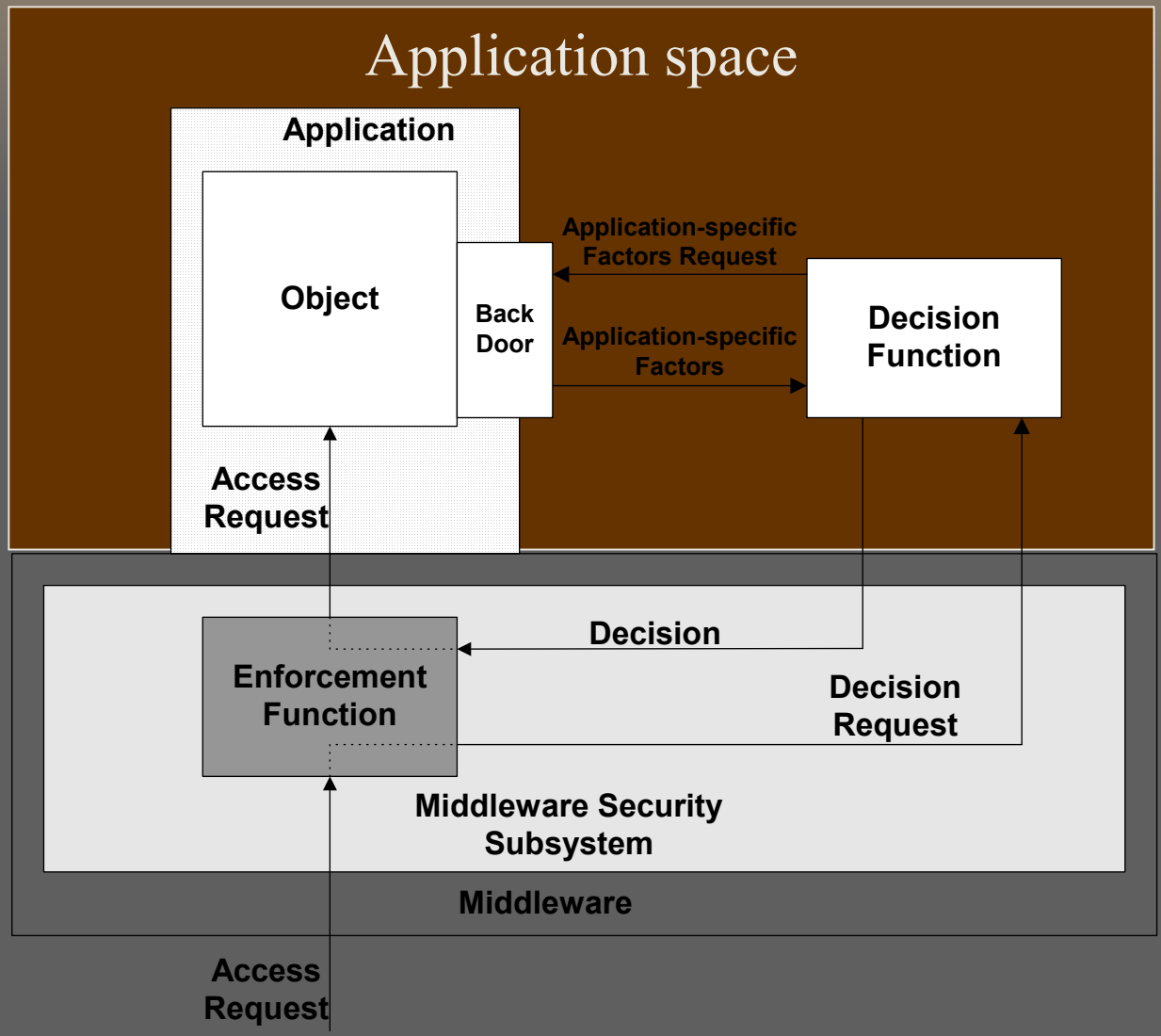


- Access control
- QoP (secrecy, integrity)
- Audit



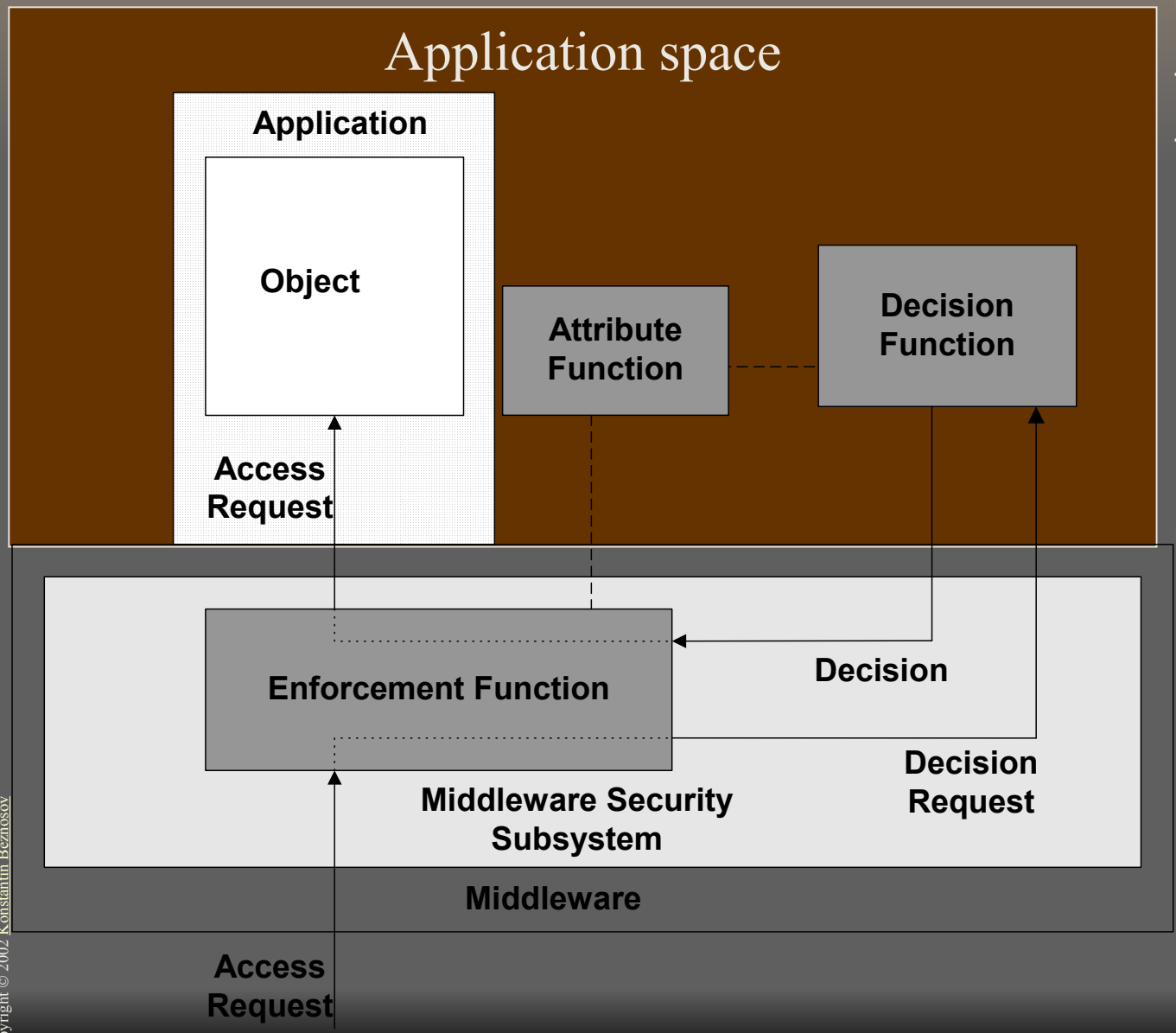
	Decision Function	Enforcement Function
Application	AD	AE
Middleware	MD	ME

ADME – Application Decides, Middleware Enforces



- could be inefficient on expensive to activate objects
- Vulnerable to deny of service attacks
- DF too complex for application developers to implement

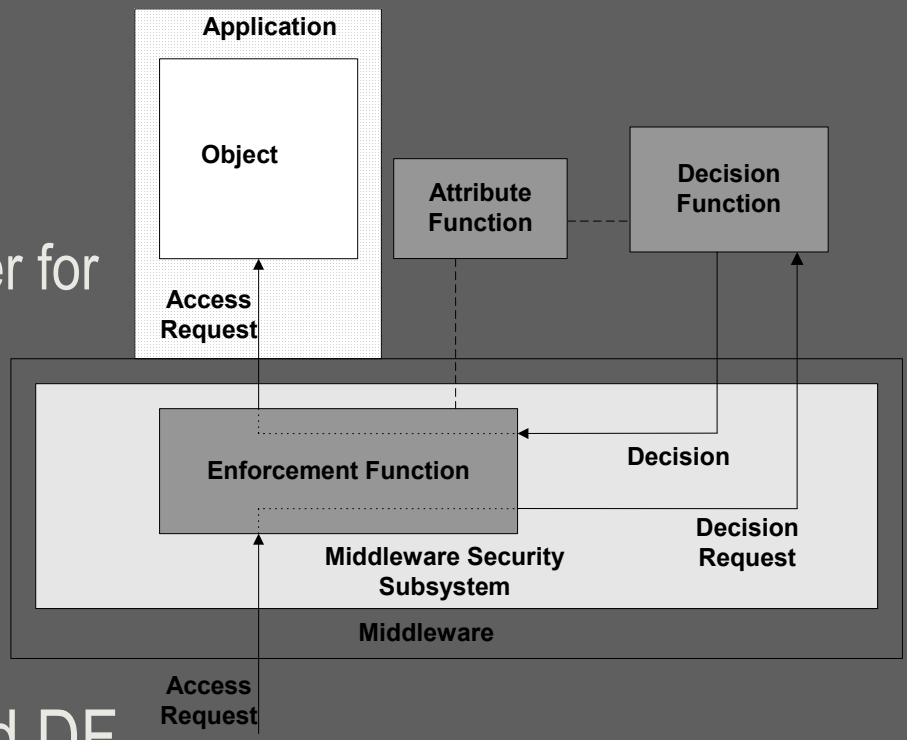
Proposed solution -- ADME/AF



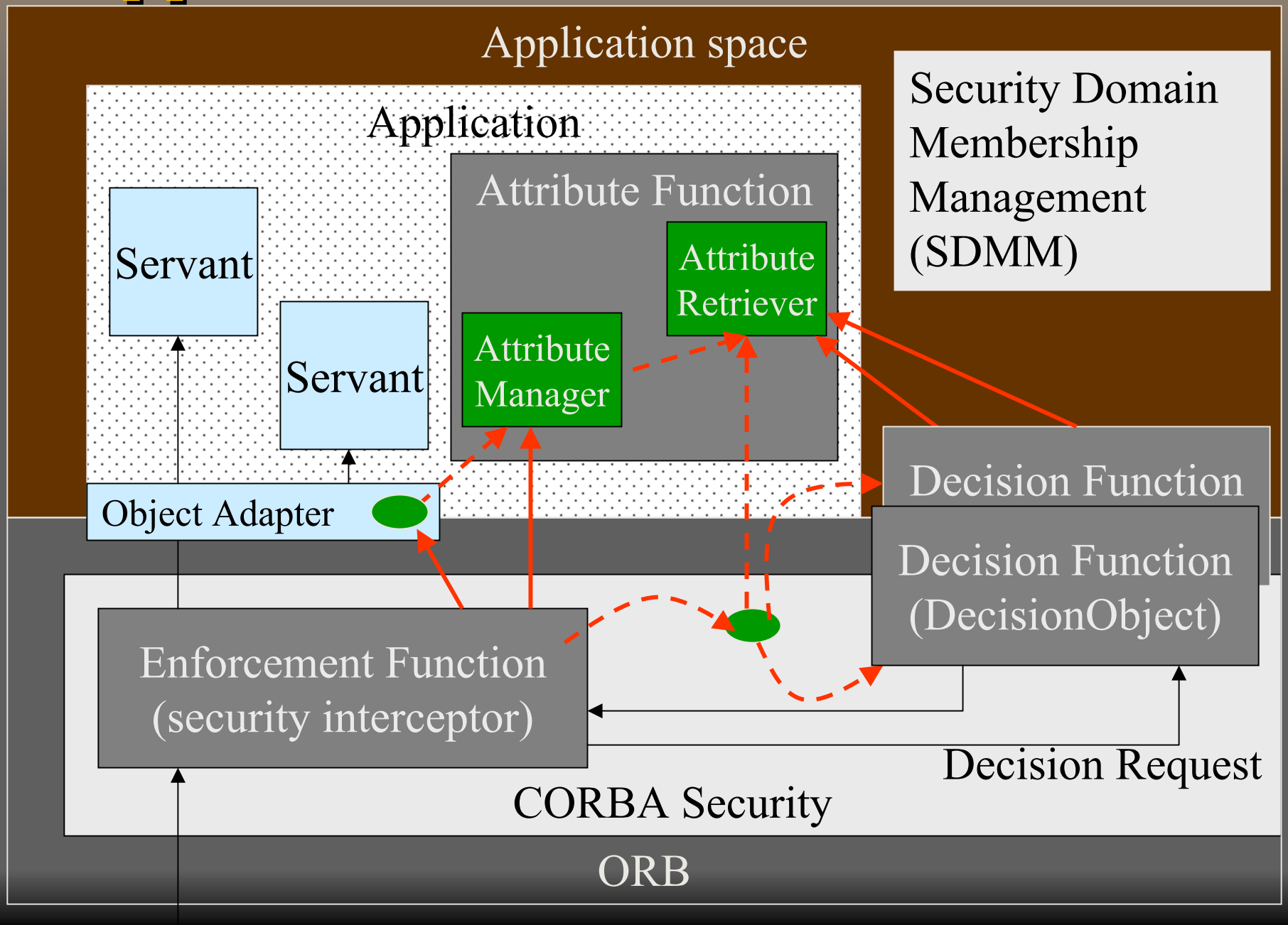
- **Object Attributes**
- \+ Advantages of ADME
- \+ Separation of concerns
  - EF – middleware vendor
  - DF – authorization vendor
  - AF – application owner
- AF's input:
  - Information for identifying the target's state

Who calls AF?

- Could be EF
  - EF has target's state identification information
  - DF could be a generic COTS Better for multiple DF's
- Could be DF
  - Lazy retrieval
  - Only needed attributes
- Could be shared between EF and DF



Application to CORBA



Discussion

- – Only information known before the object is called
- – Not for all middleware platforms
- – Not for all policies

- + Better tradeoff in responsibilities
- + Does not require application to implement either DF or EF

- non-middleware platforms?
- non-security policies

Summary

- Problem: Keep middleware security generic and yet allow for application-specific security policies
- Contributions:
  - Classification
  - ADME/AF
- Application to CORBA – SDMM (orbos/2001-07-20)
- Related work
  http://www.beznosov.net/konstantin