



ASIACCS '11

Separation of Duties as a Service



Context & motivation

- Internal controls
 - Triggered by **scandals** (e.g. SocGen)
 - Mandated by **regulatory requirements** (e.g. SOX)
 - Recommended by **standards** (e.g. ISO 27k)
- Our focus: **Separation of Duty (SoD)**

Context & motivation

■ Internal controls

- Triggered by **scandals** (e.g. SocGen)
- Mandated by **regulatory requirements** (e.g. SOX)
- Recommended by **standards** (e.g. ISO 27k)

■ Our focus: **Separation of Duty (SoD)**

■ **Requirements** on specification and enforcement

- **Expressiveness**: capable of expressing broad range of constraints
- **Adaptable** to organizational and technological **changes**
- **Loose coupling** between business and internal controls
 - **Separation of concerns** business experts, HR, compliance officer
 - **Simplify integration**, e.g. of internal controls and legacy system

From abstract SoD algebra to implementation

Separation of Duty Algebra (SoDA)

[LW08]

Terms specify SoD constraints

e.g. $\phi = \text{Patient} \otimes ((\neg\{\text{Claire}\})^+ \sqcap (\text{Nurse} \otimes \text{Pharmacist}))$

Semantics: A set of users satisfies ϕ w.r.t. user-role assignment

[LW08] Li & Wang, Beyond separation of duty: An algebra for specifying high-level security policies, Journal of the ACM, 2008.

From abstract SoD algebra to implementation

Separation of Duty Algebra (SoDA)

[LW08]

Terms specify SoD constraints

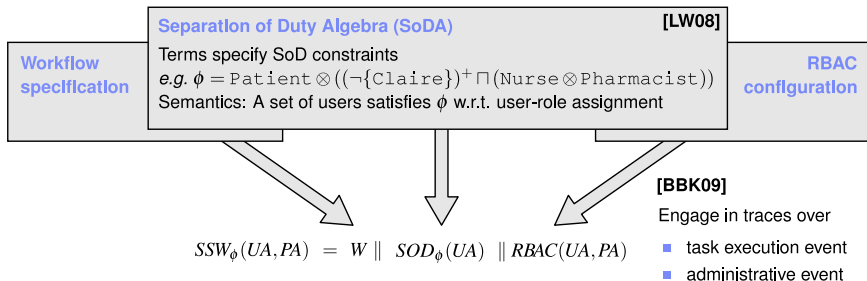
e.g. $\phi = \text{Patient} \otimes ((\neg\{\text{Claire}\})^+ \sqcap (\text{Nurse} \otimes \text{Pharmacist}))$

Semantics: A set of users satisfies ϕ w.r.t. user-role assignment

 $SOD_{\phi}(UA)$

[LW08] Li & Wang, Beyond separation of duty: An algebra for specifying high-level security policies, Journal of the ACM, 2008.

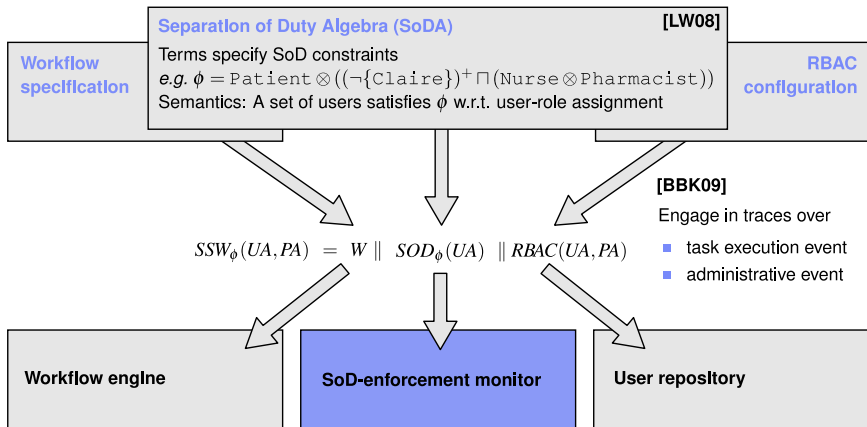
From abstract SoD algebra to implementation



[LW08] Li & Wang, Beyond separation of duty: An algebra for specifying high-level security policies, Journal of the ACM, 2008.

[BBK09] Basin, Burri, & Karjot, Dynamic Enforcement of Abstract Separation of Duty Constraints, ESORICS 2009.

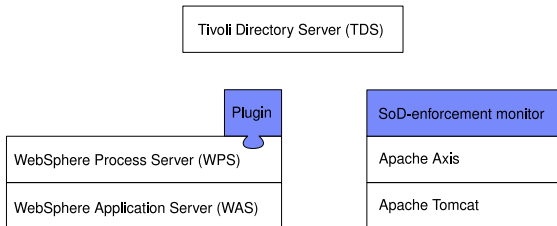
From abstract SoD algebra to implementation



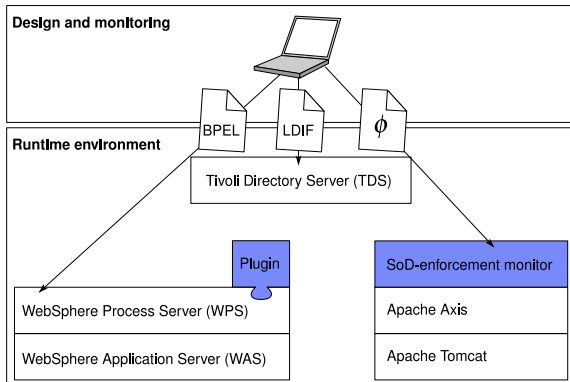
[LW08] Li & Wang, Beyond separation of duty: An algebra for specifying high-level security policies, Journal of the ACM, 2008.

[BBK09] Basin, Burri, & Karjot, Dynamic Enforcement of Abstract Separation of Duty Constraints, ESORICS 2009.

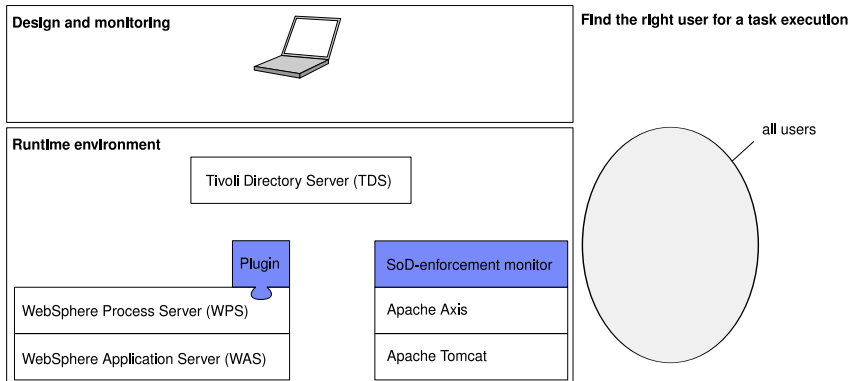
Architecture & enforcement



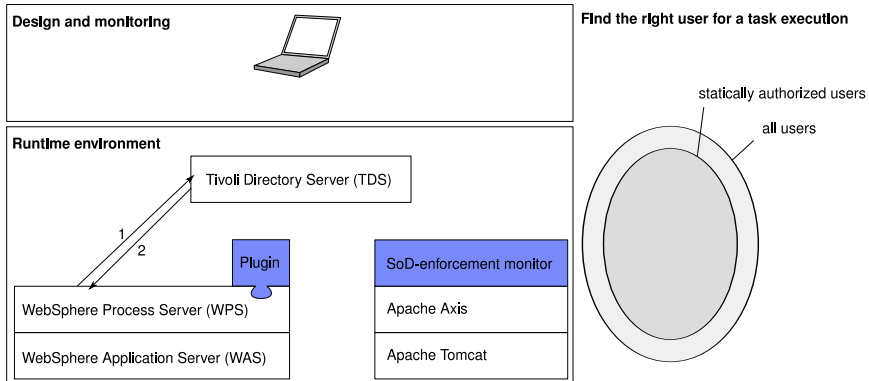
Architecture & enforcement



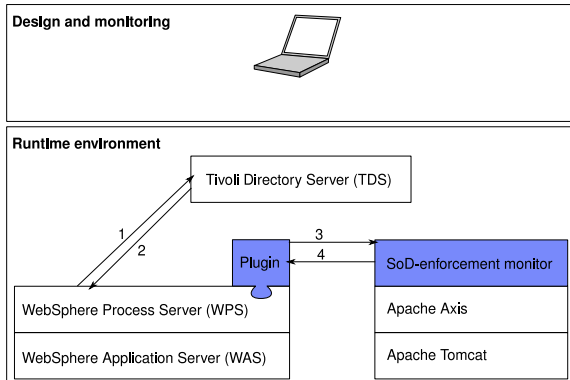
Architecture & enforcement



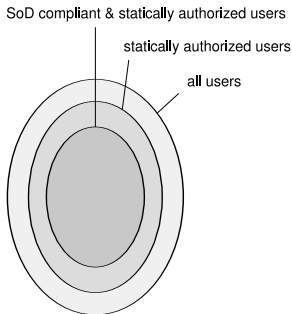
Architecture & enforcement



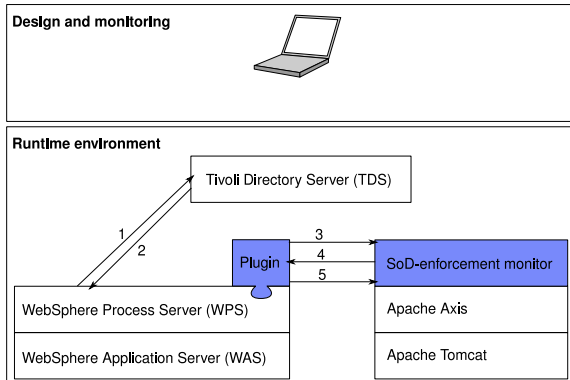
Architecture & enforcement



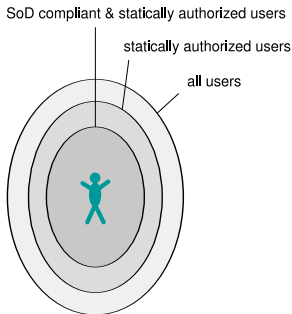
Find the right user for a task execution



Architecture & enforcement



Find the right user for a task execution

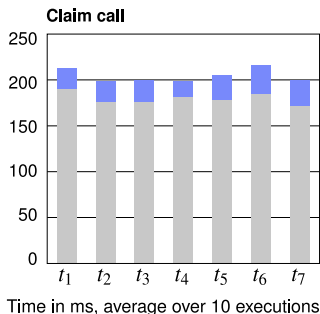
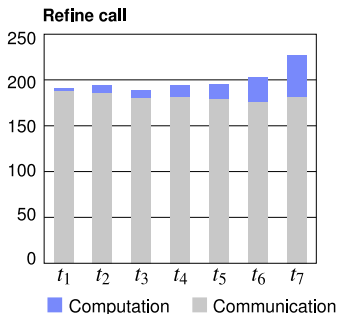


Complexity and performance in practice

- Deciding **satisfiability** of a SoDA term is **NP-hard [LW08]**.
 - Theoretical models: in the **number of users**
 - Our implementation: in the **number of (executed) tasks**

Complexity and performance in practice

- Deciding **satisfiability** of a SoDA term is **NP-hard** [LW08].
 - Theoretical models: in the **number of users**
 - Our implementation: in the **number of (executed) tasks**
- **Case study**: drug dispensation workflow in hospital
- **Time measurements**: SoD enforcement ca. 10% communication increase



Conclusions

- Contribution: **SoD as a Service** – new approach to enforce
 - **expressive** SoD constraints
 - **adaptive** to organizational changes
 - **loose coupling** with existing (prob. legacy) systems
 - **acceptable performance** (penalty)

- Interesting questions:
 - Where to maintain **context / history** (in distributed architecture)
 - **Abstract vs. business-specific** constraints: where is the right balance?