Automatic Generation of Separation of Duty Fraud Scenarios

Stanislaus Stelle
Ulrich Flegel

SAP Research Karlsruhe
September 2009

Spring, 14.-15. September 2009, Stuttgart

SAP RESEARCH

THE BEST-RUN BUSINESSES RUN SAP™ **SAP**

Motivation

- The 67-year-old owner of a savings and loan association diverted millions of dollars in corporate funds to cover his own bad investments. The final cost of the savings and loan fraud to taxpayers was $2.5 billion.

- A female bank teller, 24, pilfered $22 from her cash drawer and originally claimed the money was due to "shortages." She later confessed.

http://www.acfe.com/documents/Report_to_the_Nation.pdf

Agenda

SAP RESEARCH

Agenda

SAP RESEARCH

Given Problem

Given Problem

- Given a backend algorithm of the European SUPER project
- Given a workflow description
- Given the task to model user information into the workflow description

Procedure

- Analysing the algorithm and its papers
- Implementing scenarios in the algorithm's file format by hand

Given Goal
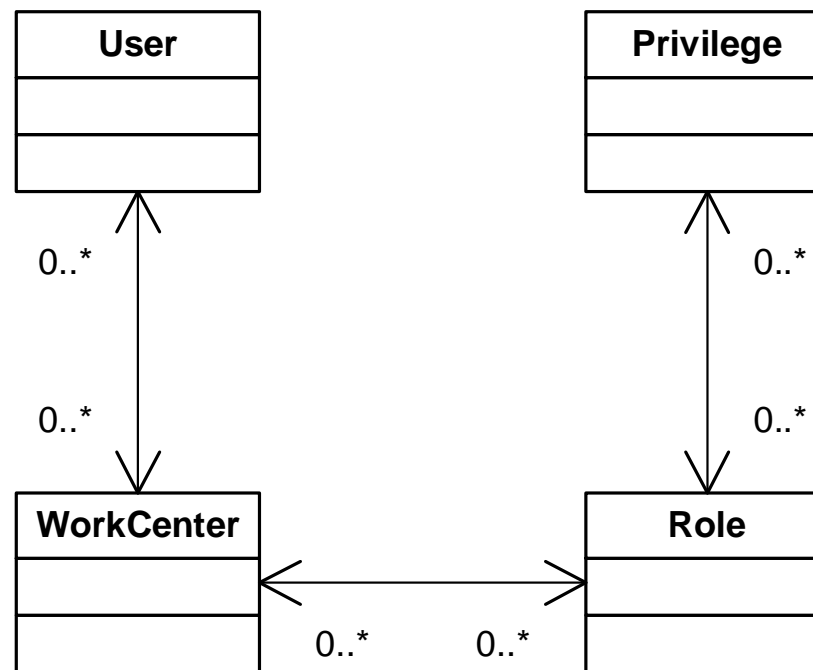
- Is it possible to automatically generate fraud patterns

Agenda

- In a SAP system users get work centers assigned
- Work centers encapsulate roles
- Roles encapsulate privileges

- In modern companies workflows are implemented as web services

- Web services are loosely bound applications which need to be concatenated to workflows

- Automatic concatenation needs annotations of web services

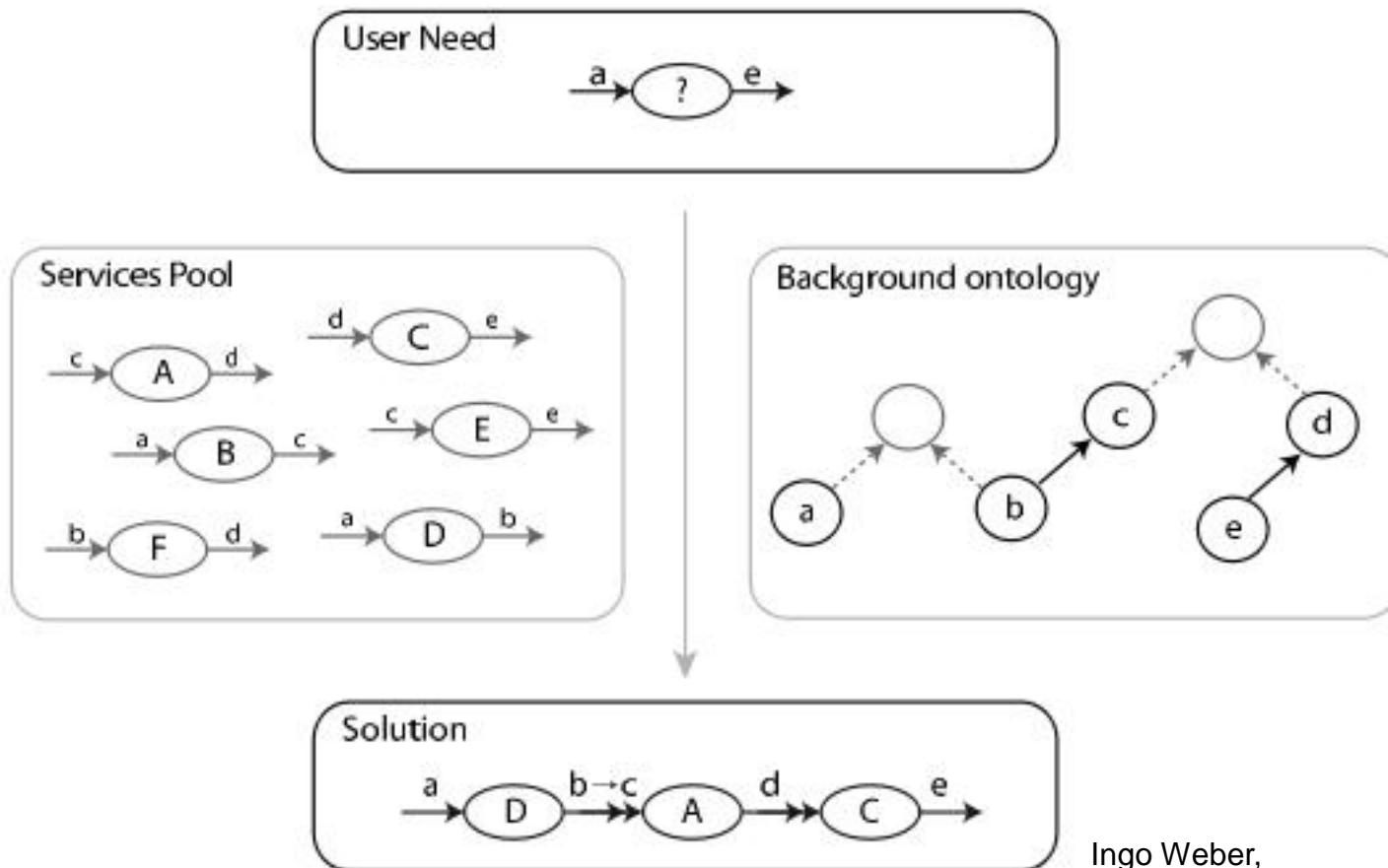- Annotations will be used to add user information to web services

Workflow

SAP RESEARCH
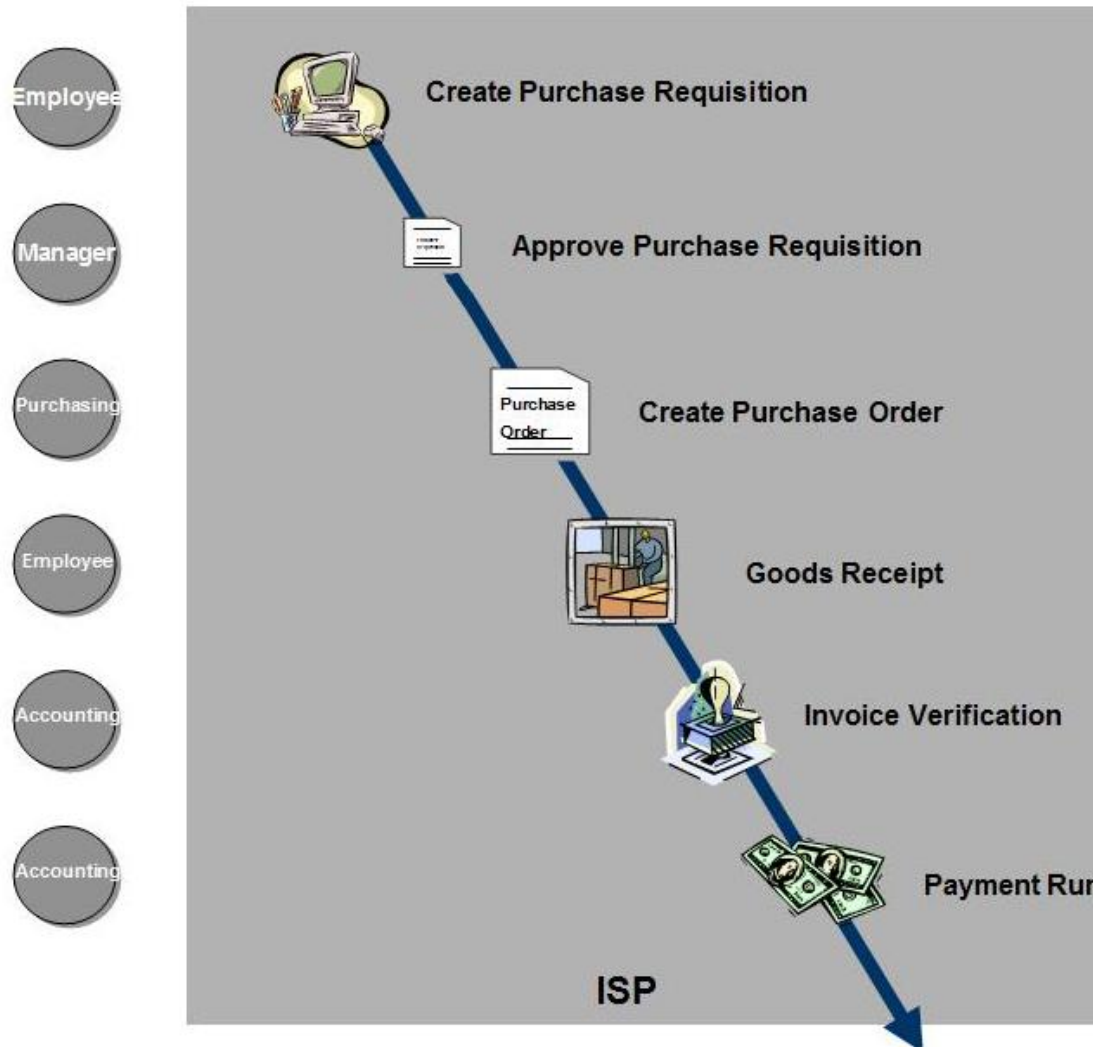
Workflow

Segregation of Duties

- Money change hands → more than one official in charge
- More people control a workflow
- Chances are higher that there is no fraud conducted

A General Reasoner

Ingo Weber,
  MAESTRO, 2008

Composer

Taxonomy	Ontology
■ A→B ≡ ¬A ∨ B	■ Objects
	■ Attributes
	■ Relations
	■ Function Terms
	■ Restrictions
	■ Rules
	■ Axioms
	■ Events

■ Ontologies can describe attributes and their relations

■ E.g. That employees are friends or married

Composer

SUPER's composer

- can only detect a single sequence of actions to satisfy initial and goal conditions

- cannot find anything that is not written in its configuration

- Cannot automatically detect all fraudulent concatenations

Agenda

SAP RESEARCH

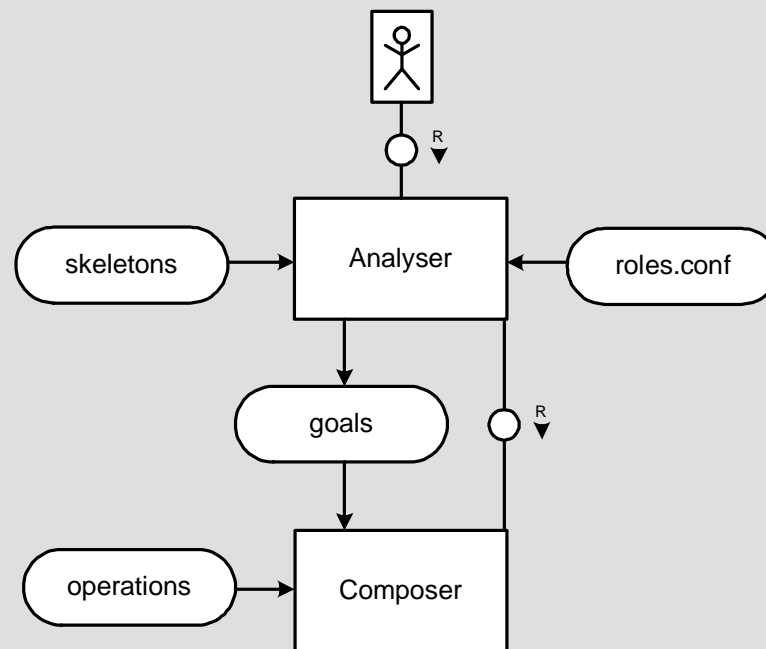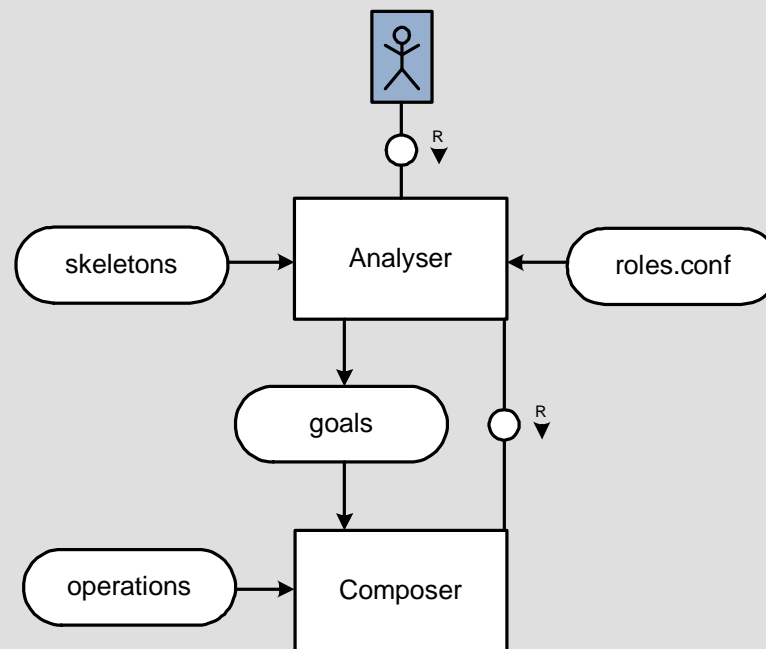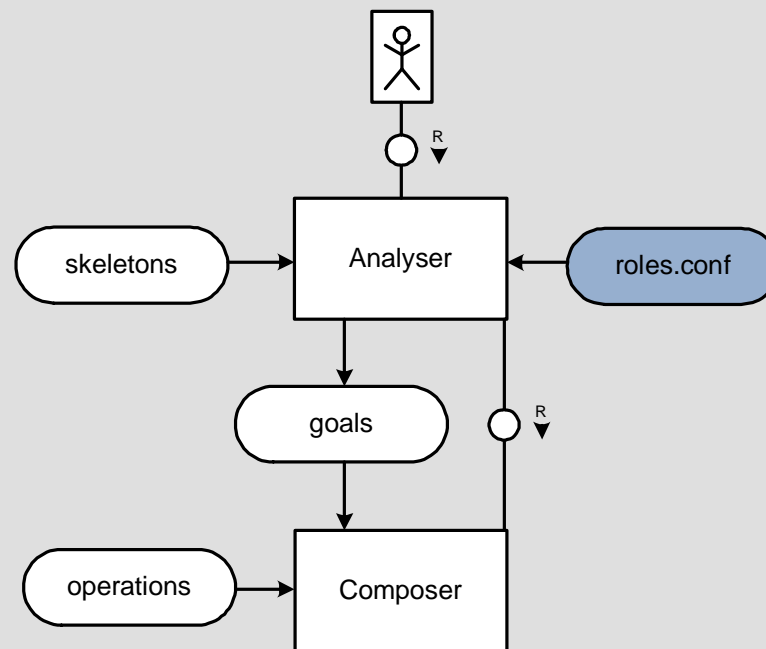# Architecture

Resulting Setup

Resulting Setup

Architecture
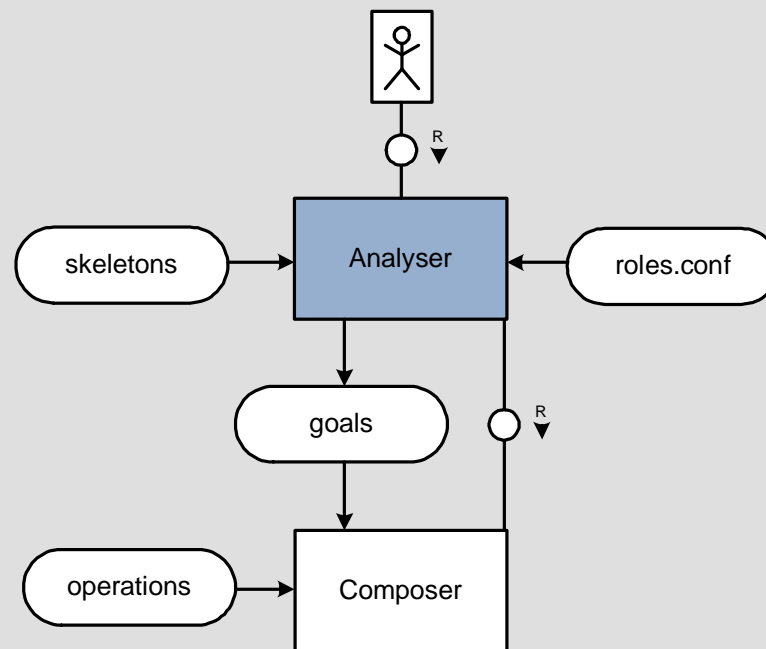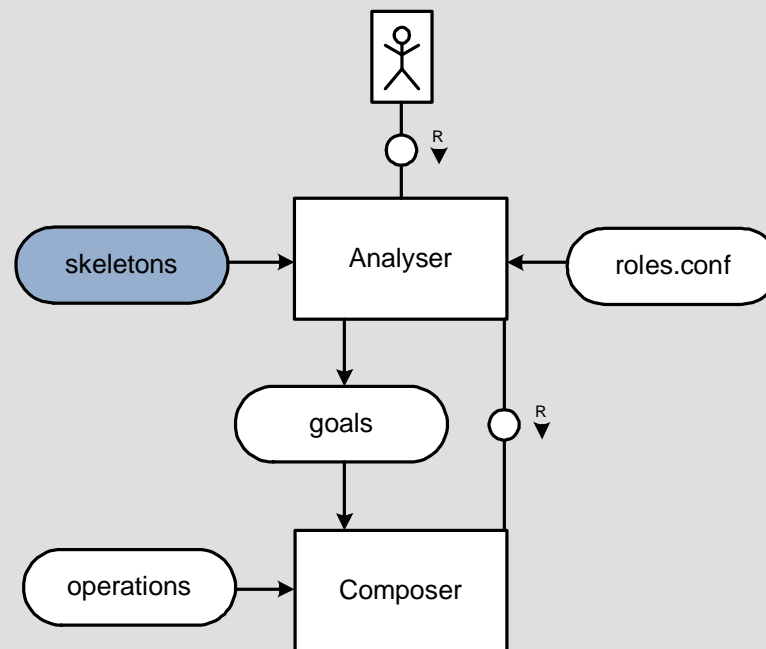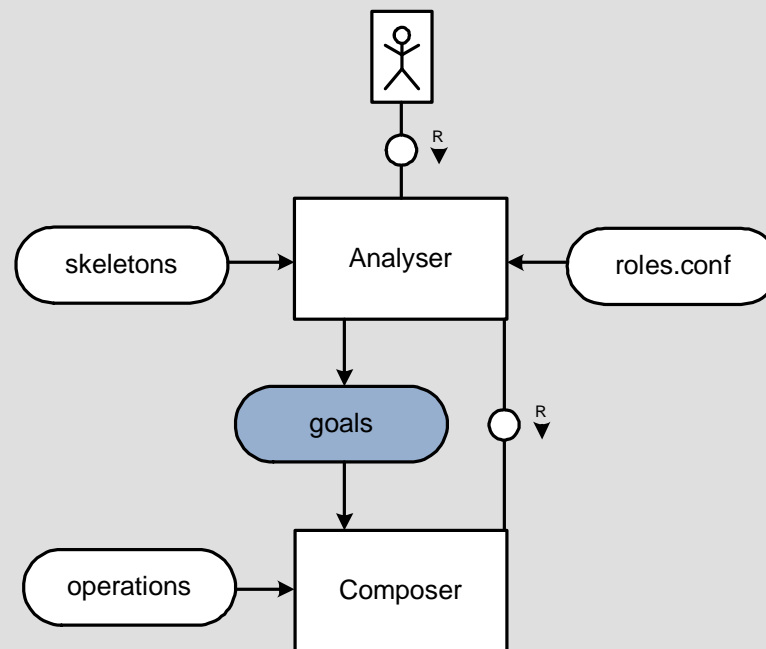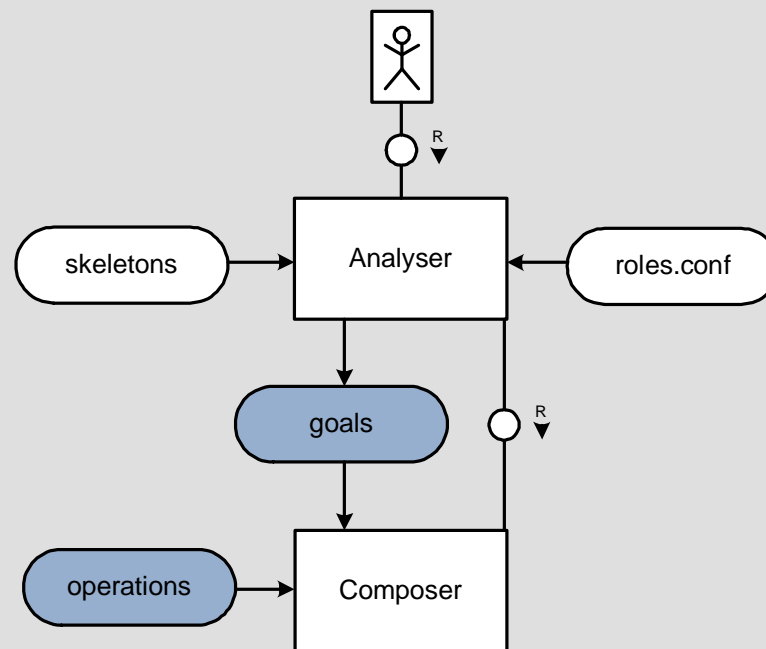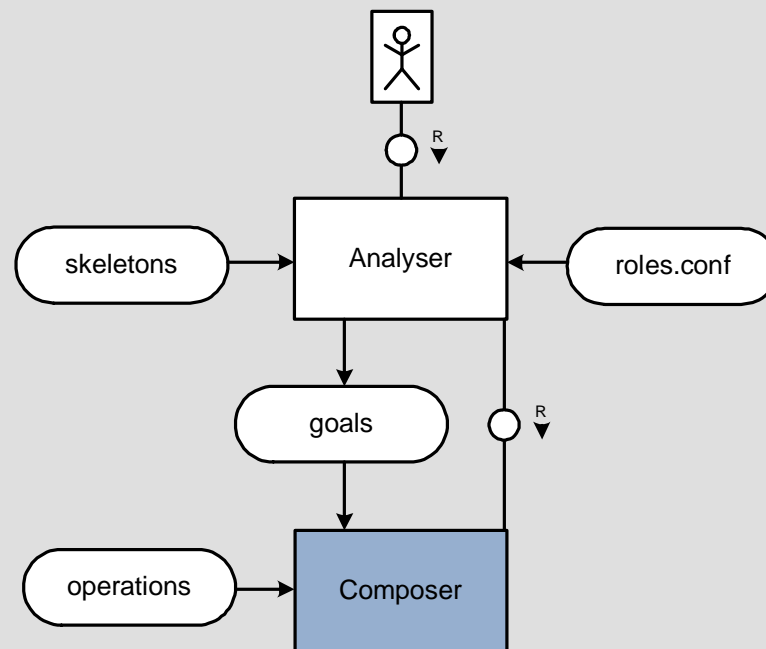
Resulting Setup

Resulting Setup

Resulting Setup

Resulting Setup

Architecture

Resulting Setup

Architecture

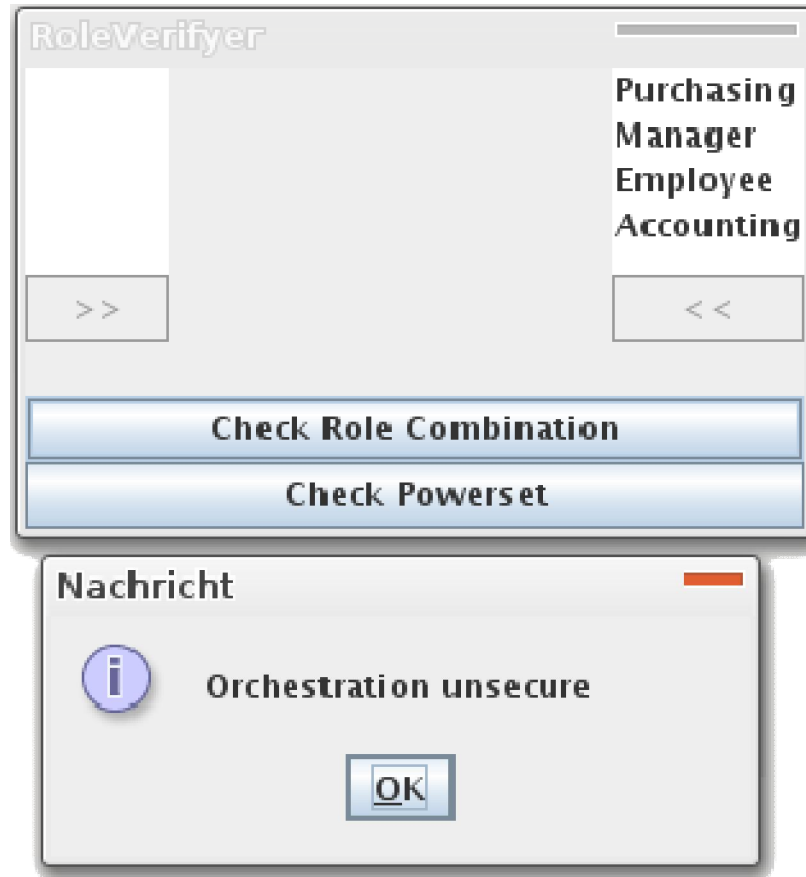## Resulting Setup

Architecture

Resulting Setup

Architecture
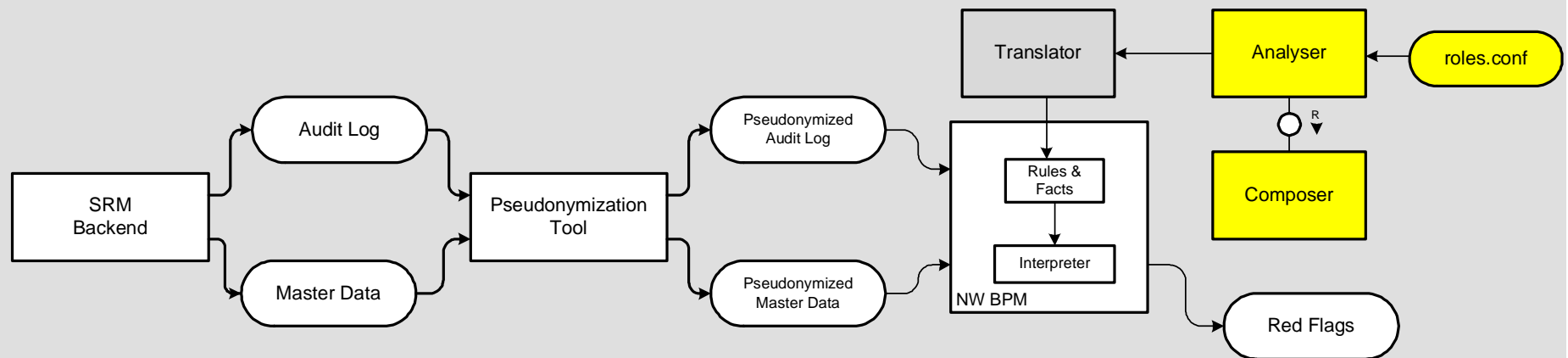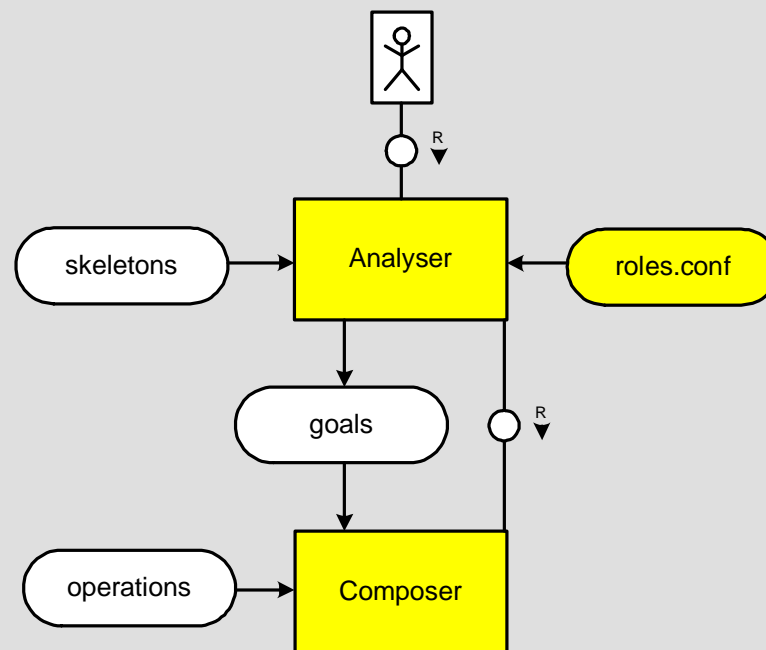
Resulting Setup
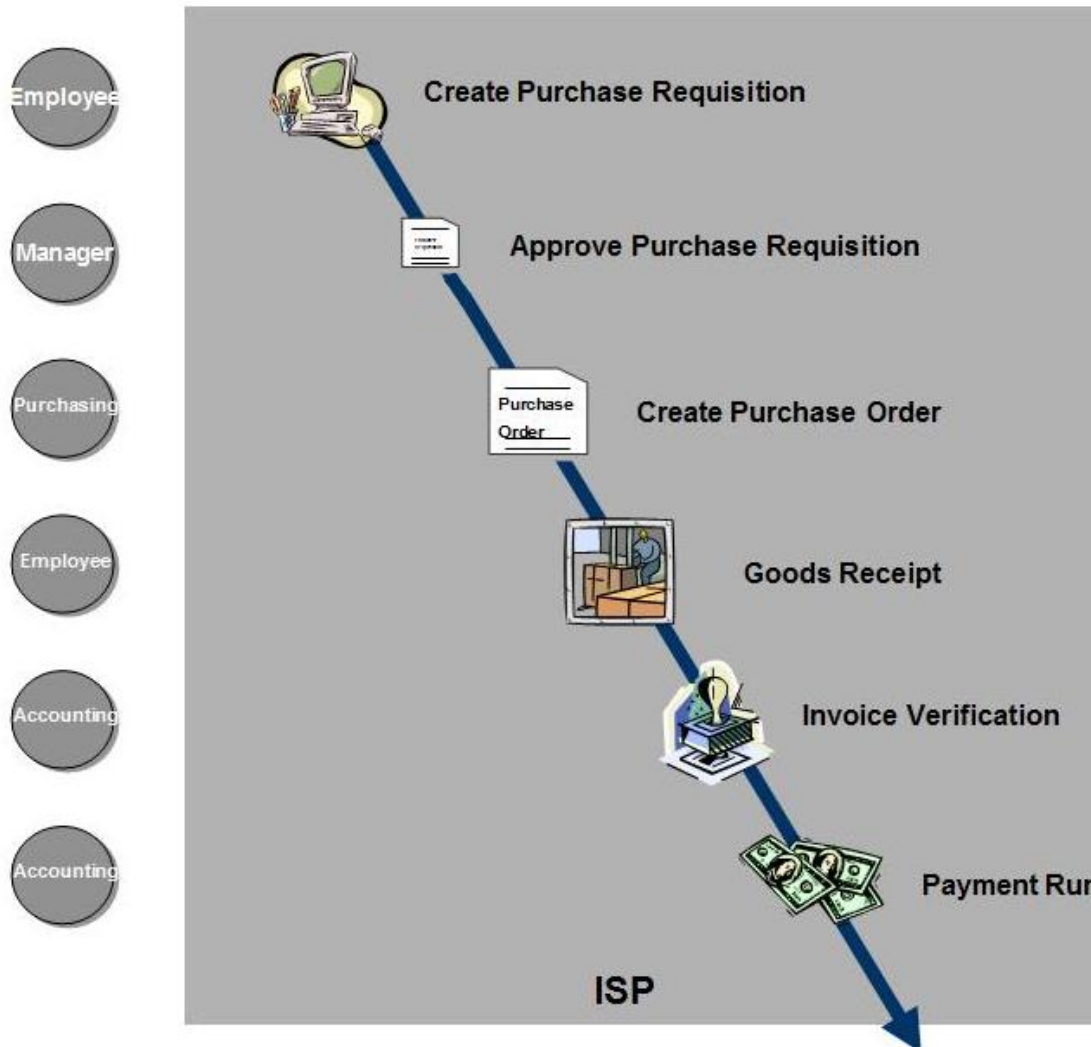
Example

Example
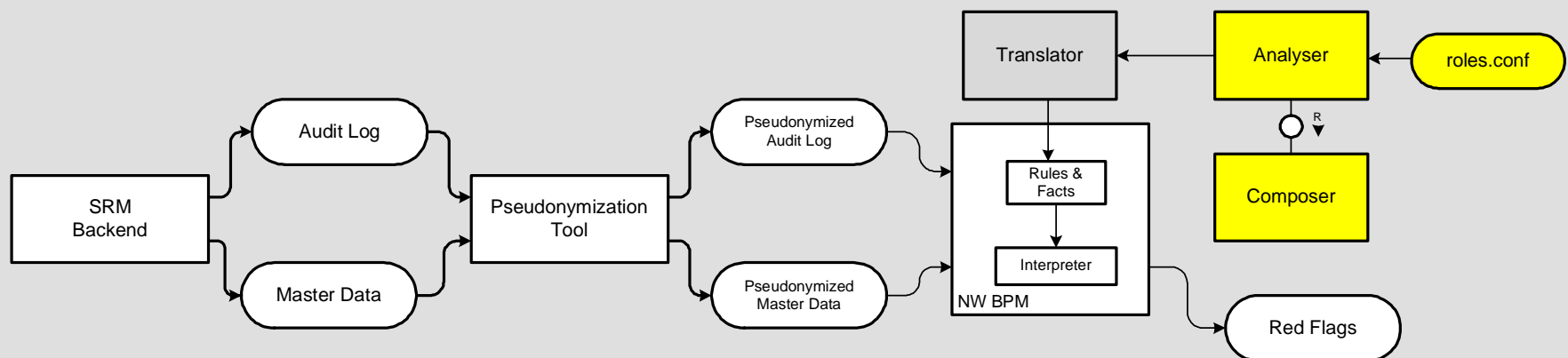
Example

Fraud Detection System

- Currently in development by Cristina Fortu
- Generated fraud patterns can enrich its repository
- Patterns can be generated by analysing supersets of privileges

Sources

- http://www.accountingnation.com/portal/A-FraudOverview.aspx
    - Accessed Thursday, 27th of August 2009
- http://www.acfe.com/documents/Report_to_the_Nation.pdf
    - Accessed Thursday, 27th of August 2009

Thank you!