A New World of Innovation

TRIALOG

# Privacy-by-Design Documentation Software Architecture Viewpoint

Antonio Kung

August 2013

# Introduction

- Based on Carnegie Mellon – Software Engineering Institute work
  - http://www.sei.cmu.edu/
- Main reference
  - Software Architecture in Practice, 3rd Edition
    - L.Bass, P.Clements, R.Kazman
    - Addison-Wesley, 2012.
- Other references
  - Documenting Software Architectures: Views and Beyond, 2nd Edition
    - P.Clements, F.Bachmann, L.Bass, D.Garlan, J.Ivers, R.Little, P.Merson, R.Nord, J.Stafford
    - Addison-Wesley, 2010
  - A General Model of Software Architecture Design Derived from Five Industrial Approaches
    - C.Hofmeister, P.Kruchten, R.Nord, H.Obbink, A.Ran, P.America
    - Journal of Systems and Software, Vol.80 Issue 1, January, 2007

TRIALOG

Introduction

# Software Architecture Practice

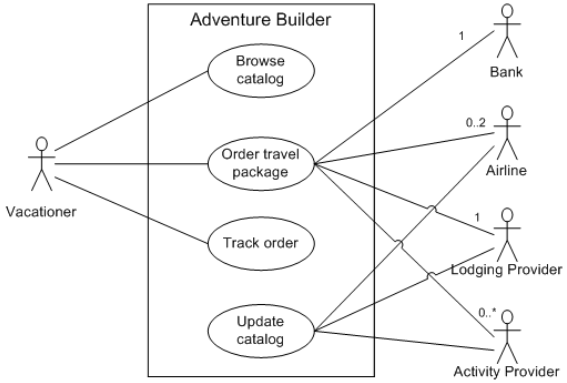
# Two types of Requirements

- Functional requirements
  - What a system does. Examples:
    - engine control
    - social network function
    - location oriented services
    - …
- Quality attributes requirements
  - How well the system does it. Examples:
    - execution qualities: security, usability, dependability, …
    - evolution qualities: testability, maintainability, scalability, …
    - business qualities: time-to-market, cost, …
    - …
  - Other term used: non functional requirement, constraints, quality of service requirements, non behavioral requirements
    - https://en.wikipedia.org/wiki/Non-functional_requirement)

# Documentation of Requirements

Example from wiki.sei.cmu.edu/sad/index.php/The_Adventure_Builder_SAD

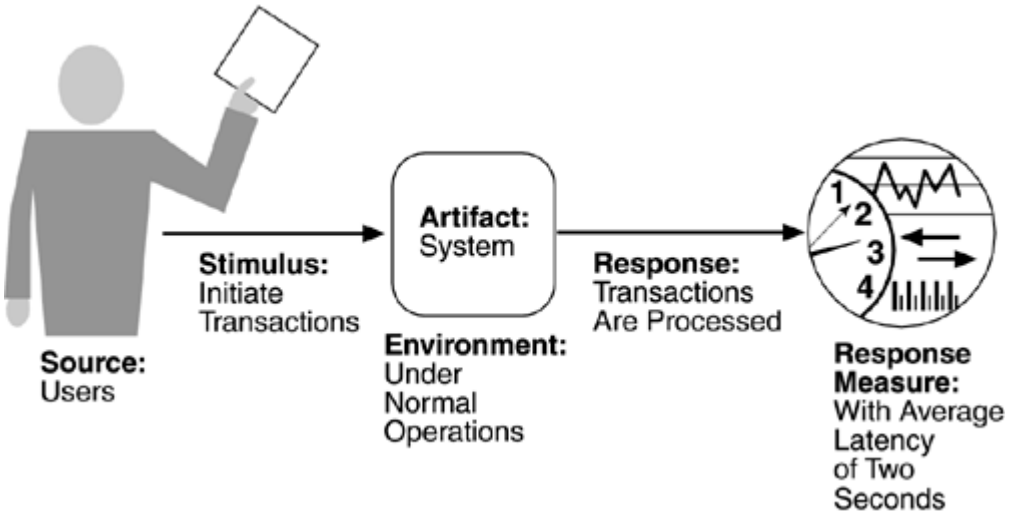
- Functional Requirements: Use Cases
  - Browse catalog
    - UC1. The user can visit the Adventure Builder Web site and browse the catalog of travel packages, which include flights to specific destinations, lodging options, and activities that can be purchased in advance. Activities include mountain biking, fishing, surfing classes, hot air balloon tours, and scuba diving. The user can select transportation, accommodation, and various activities to build his/her own adventure trip.
  - Order travel package
    - UC2. The user can place an order for a vacation package. To process this order, the system has to interact with several external entities. A bank will approve the customer payment, airline companies will provide the flights, lodging providers will book the hotel rooms, and businesses that provide vacation activities will schedule the activities selected by the customer.
  - …




- Quality Attributes Requirements Scenarios
  - Modifiability
    - QAS1. A new business partner (airline, lodging, or activity provider) that uses its own web services interface is added to the system in no more than 10 person-days of effort for the implementation. The business goal is easy integration with new business partners.
  - …

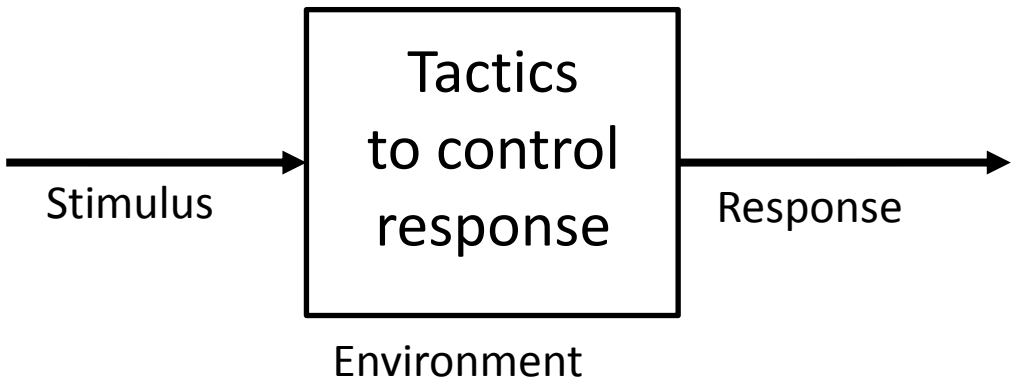
# Documentation of Requirements

## Quality Attribute Requirements Scenarios

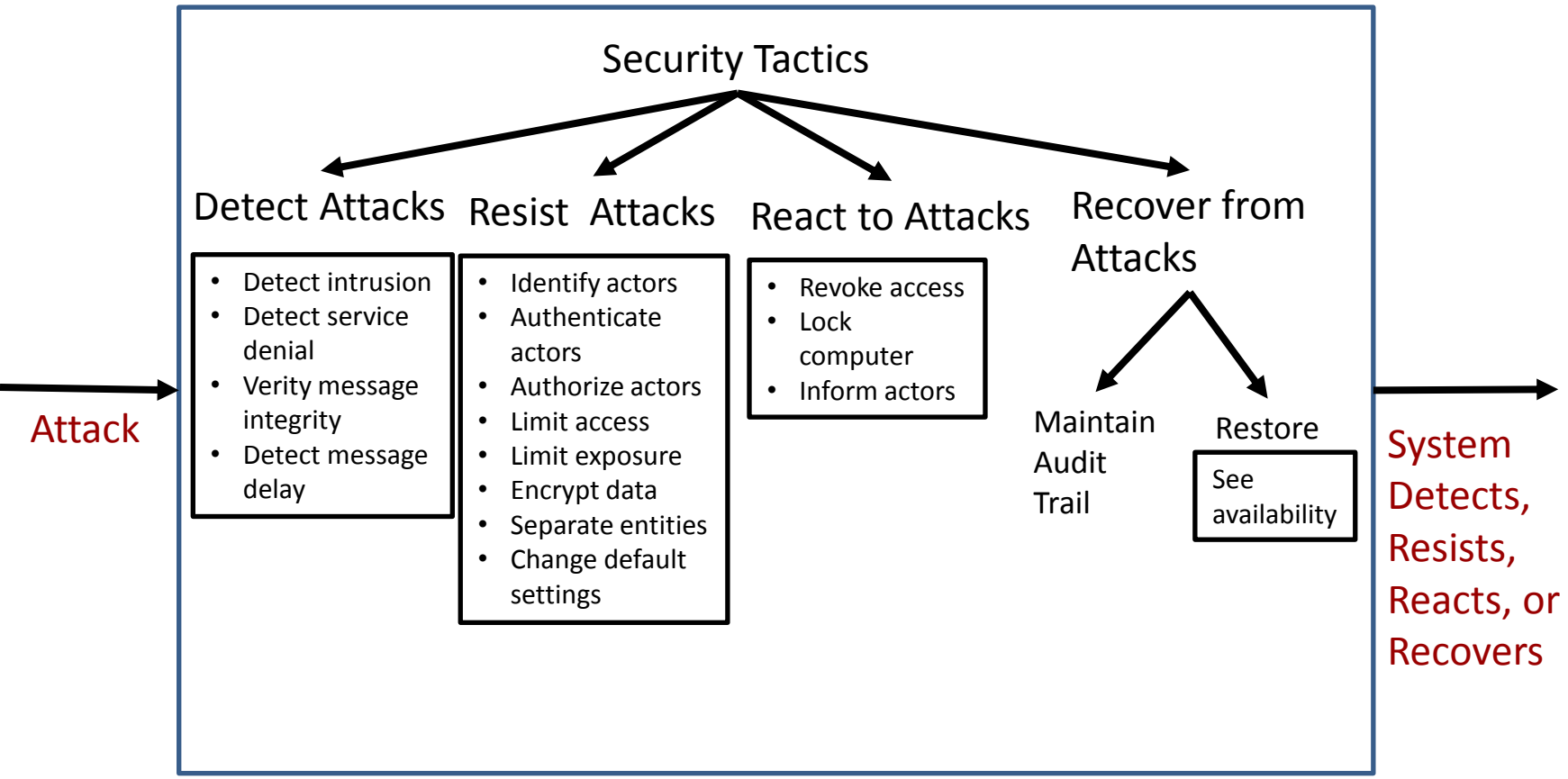



- Scenario describes
  - Source (e.g. employee)
  - Stimulus (e.g. access)
  - Stimulated Artifact (e.g. database)
  - Environment (e.g. web site)
  - Response (e.g. policy check and enforcement)
  - Response Measure (e.g. protection level)

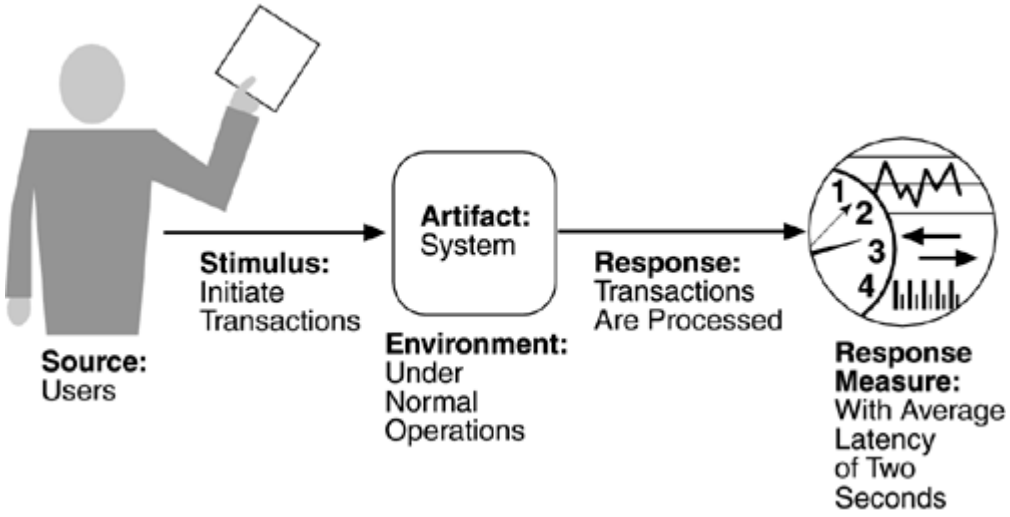
- Architecture tactics
  - Design decision that influences the achievement of a quality attribute response
  - Focus on a single quality attribute response




- Example of tactics
  - from Software Architecture in Practice, 3rd Edition



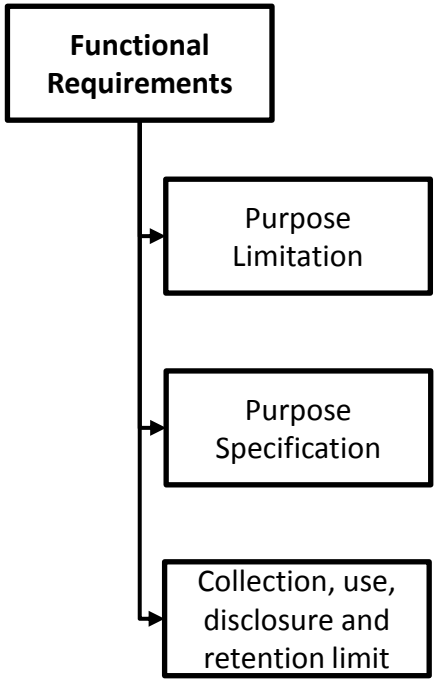
- Description of justification of architecture tactics. For each selected tactic
  - Quality attributes scenarios without tactic
  - Quality attributes scenarios with tactic
  - Benefit (Comparing improved response measure)



# Application to Privacy

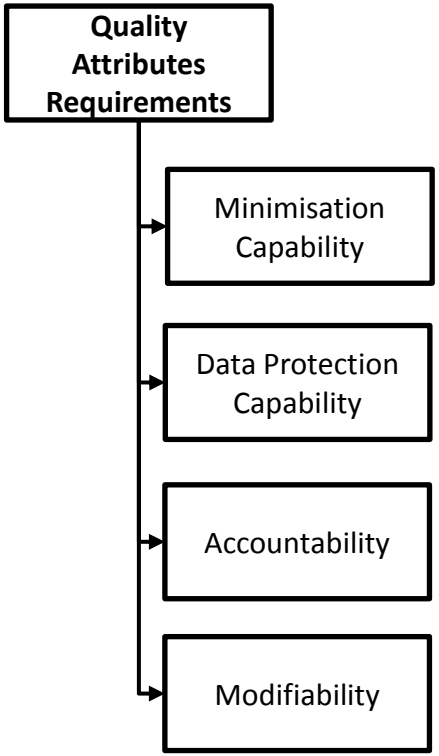
# Privacy Requirements for a System

- Functional requirements
  - Purpose Limitation
  - Purpose Specification
  - Collection, use, disclosure and retention limit

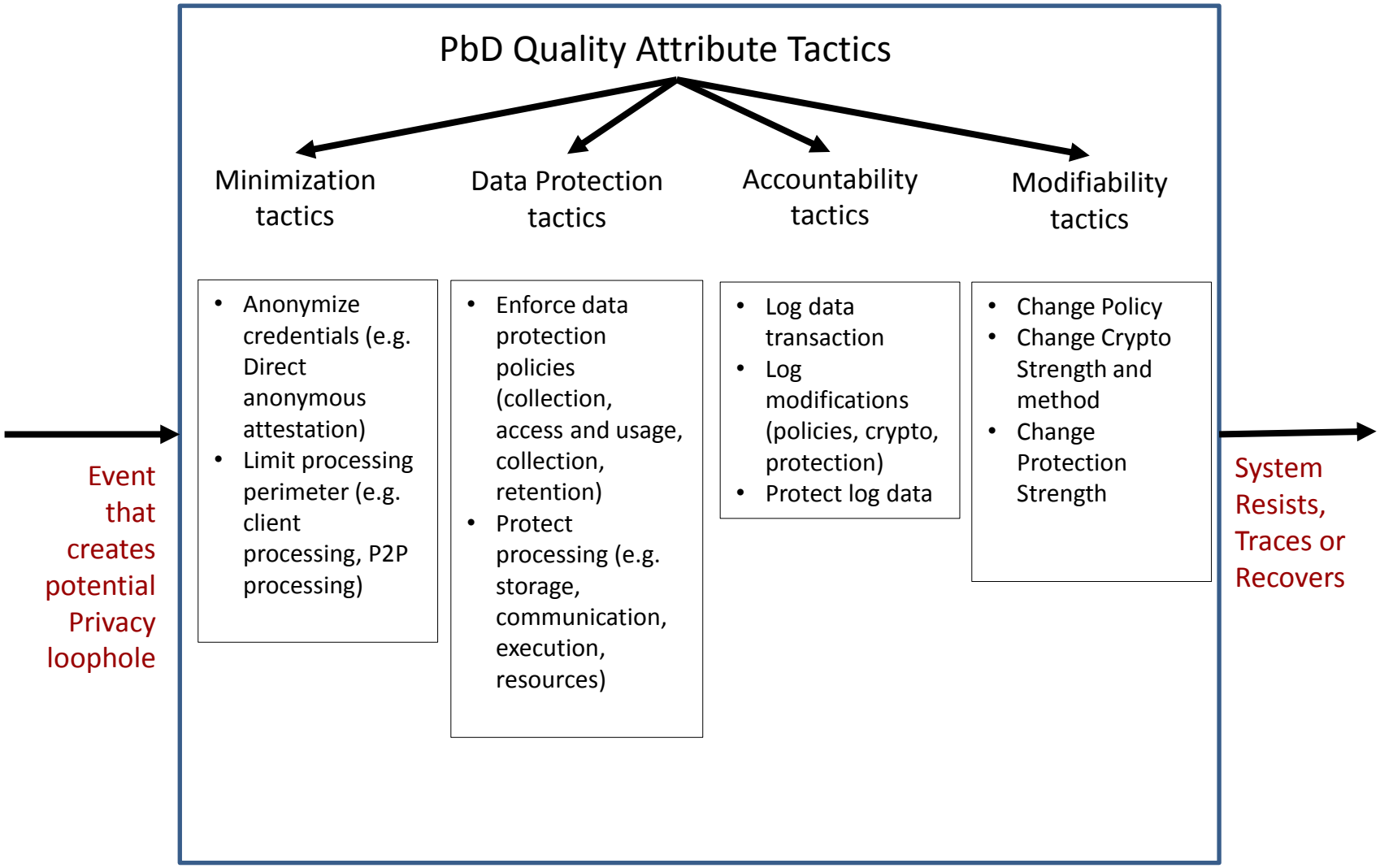



# Privacy Requirements for a System

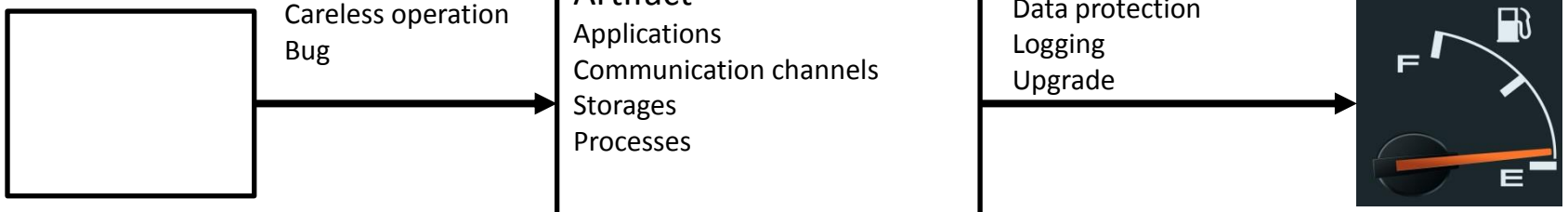
- Quality attributes Requirements
  - Minimisation capability
  - Data protection capability
  - Accountability
  - Modifiability




# PbD Quality Attributes



# PbD Quality Attribute Scenario



Source

People,
Software agents,

Stimulus
Attack
Careless operation
Bug

Artifact
Applications
Communication channels
Storages
Processes

Environment
Application
Organisation handling application
Subcontractors of organisation

Response
Anonymisation
Policy based operation
Data protection
Logging
Upgrade




Response measure
Level of minimisation
Level of data protection
Level of accountability
Level of modifiability

Antonio Kung

August 2013

www.trialog.com