Security Analysis at Design Level

Tong Li

2012.05.31 @Garda

Syllabus

- Background
  - Security --- Endless Battle
  - Security Problem Representation
- Research Topics
- Ideas
  - Security Analysis on Design Level
  - Multi-view Security Architecture

Background

Security --- Endless Battle

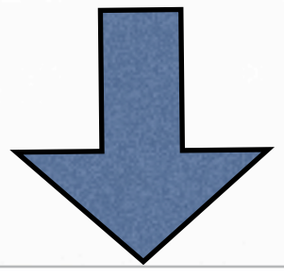
- Desktop Security

- Network Security

- Mobile Security

Problem Representation

$$D, S \vdash R$$



?

$$Ds, Ss \vdash Rs$$

Security Problem Representation

$\{Dv, Ds\}, \{Sv, Ss\} \vdash \{Rv, Rs\}$	
Rs: security requirements	Rv: all other requirements
Ds: domain assumptions related to security issues	Dv: all other domain assumptions
Ss: specifications satisfy security requirements	Sv: specifications satisfy all other requirements

Research Topics

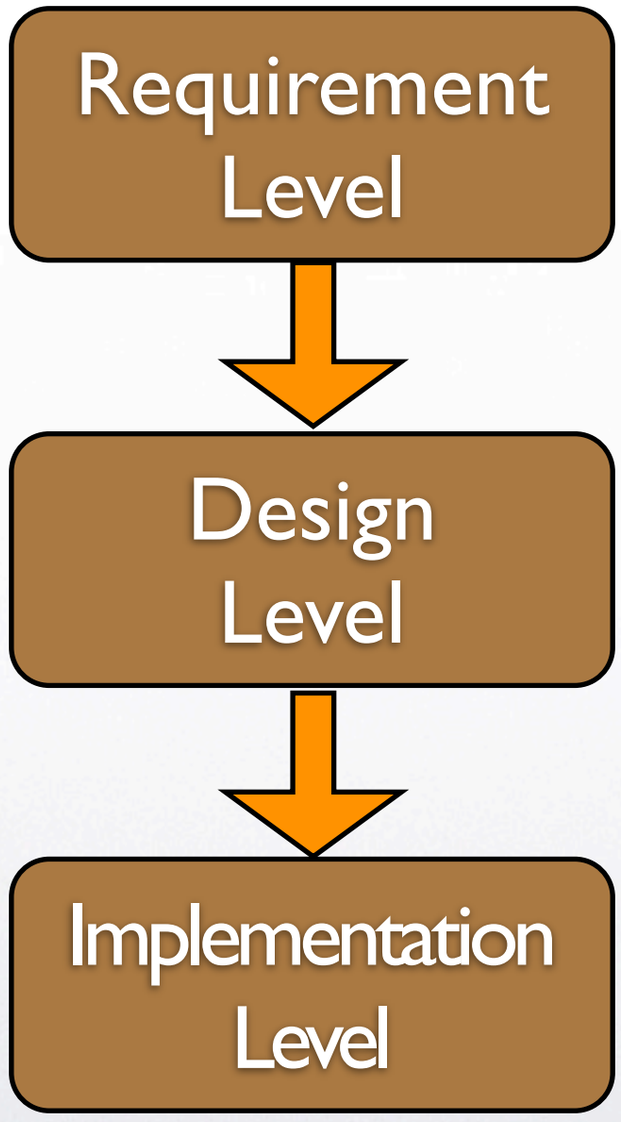
- Research goal: preserve systems' security when they evolve.
  - Verify security properties
  - Identify incremental solutions

Ideas

Security Analysis on Design Level

- Better understand the impact of security activities
- Enable the proof of system's security
- Identify additional requirements

How to make a system secure



How to make a system secure

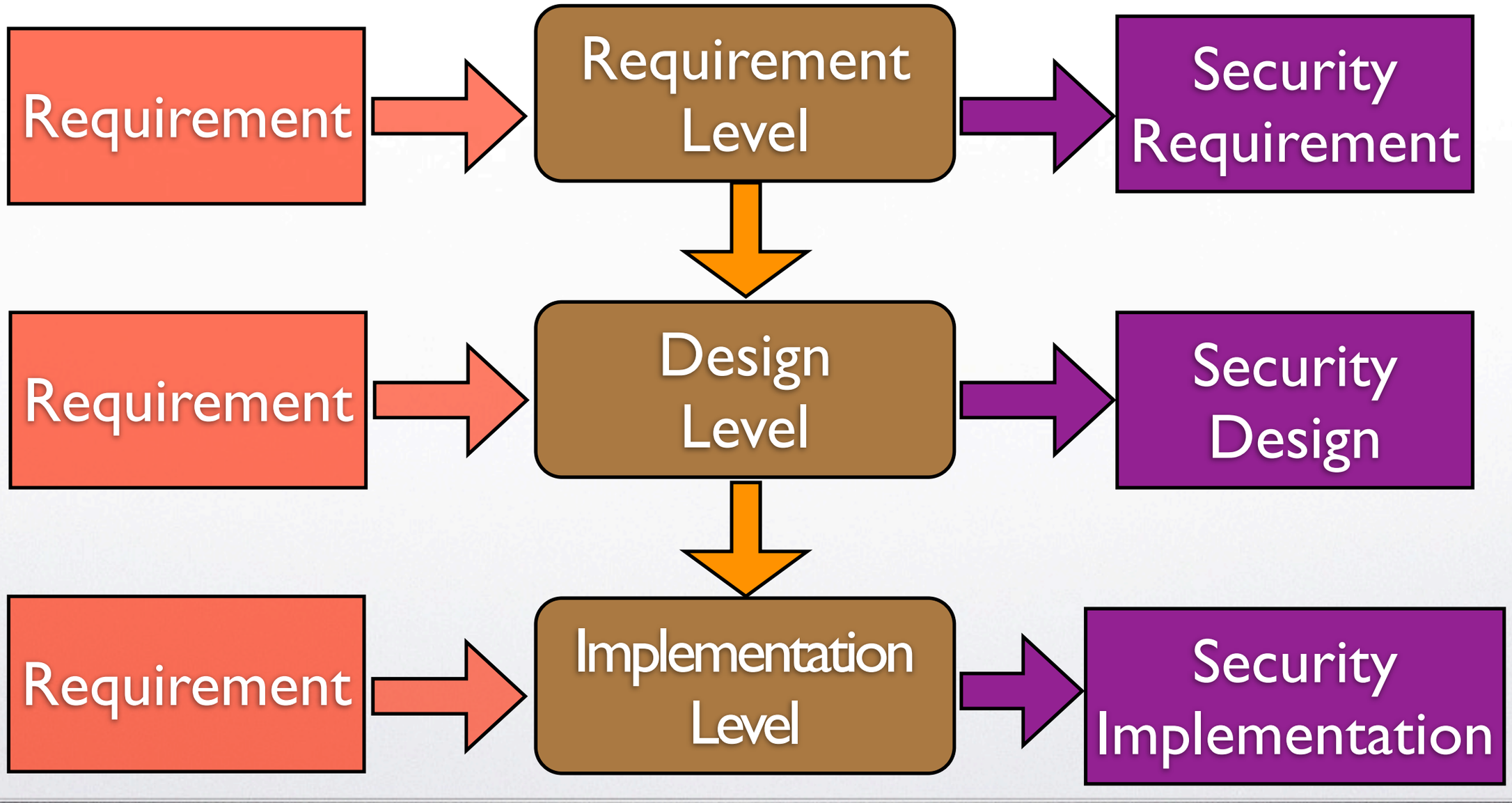
- Top-down security solution steps
  - Identify all security requirements
    - e.g. prevent data from unauthorized modification
  - Provide security designs
    - e.g. access control
  - Implement security strategies
    - e.g. certain COTS software

Security Requirement

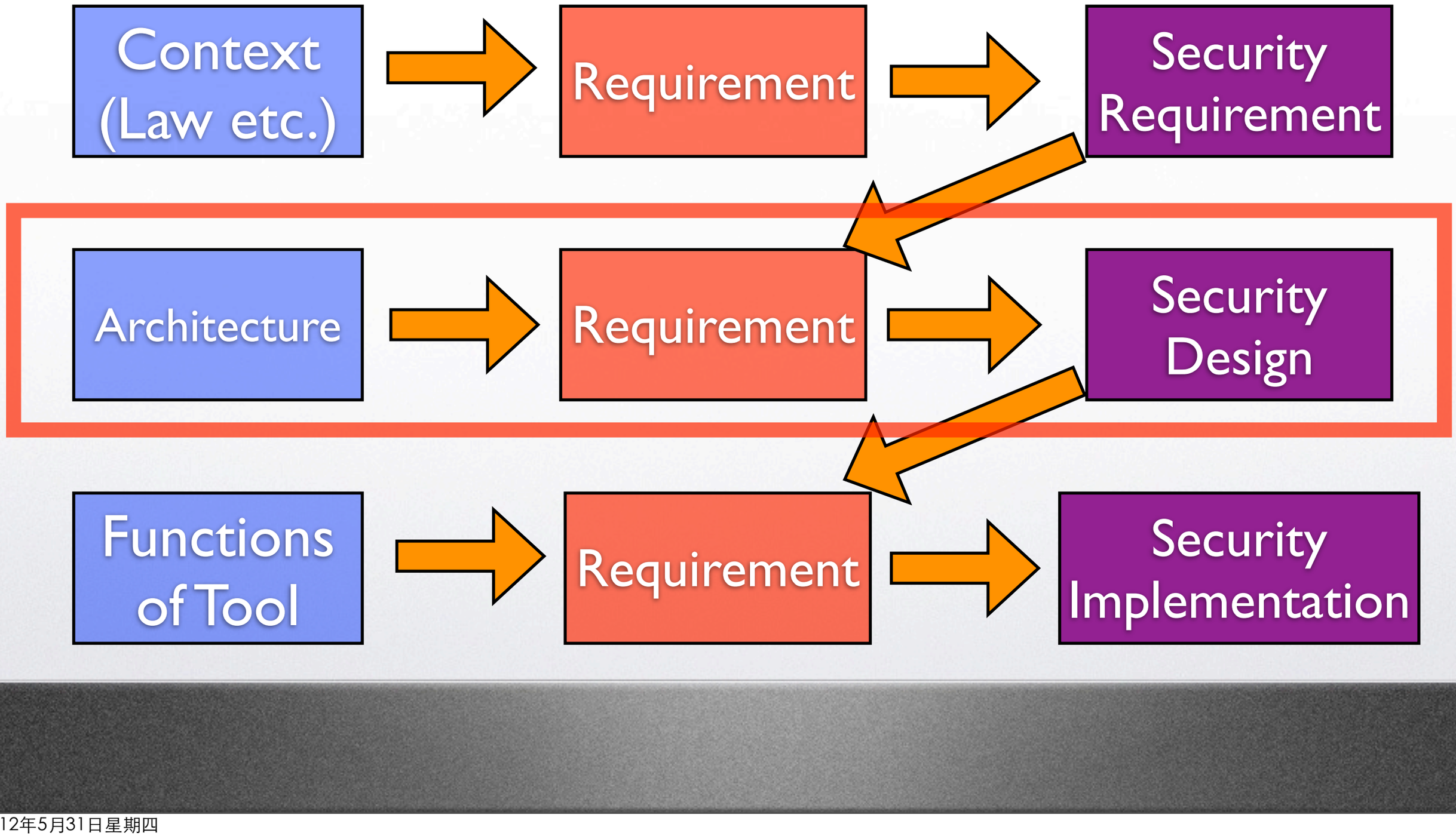
Security Design

Security Implementation

How to make a system secure



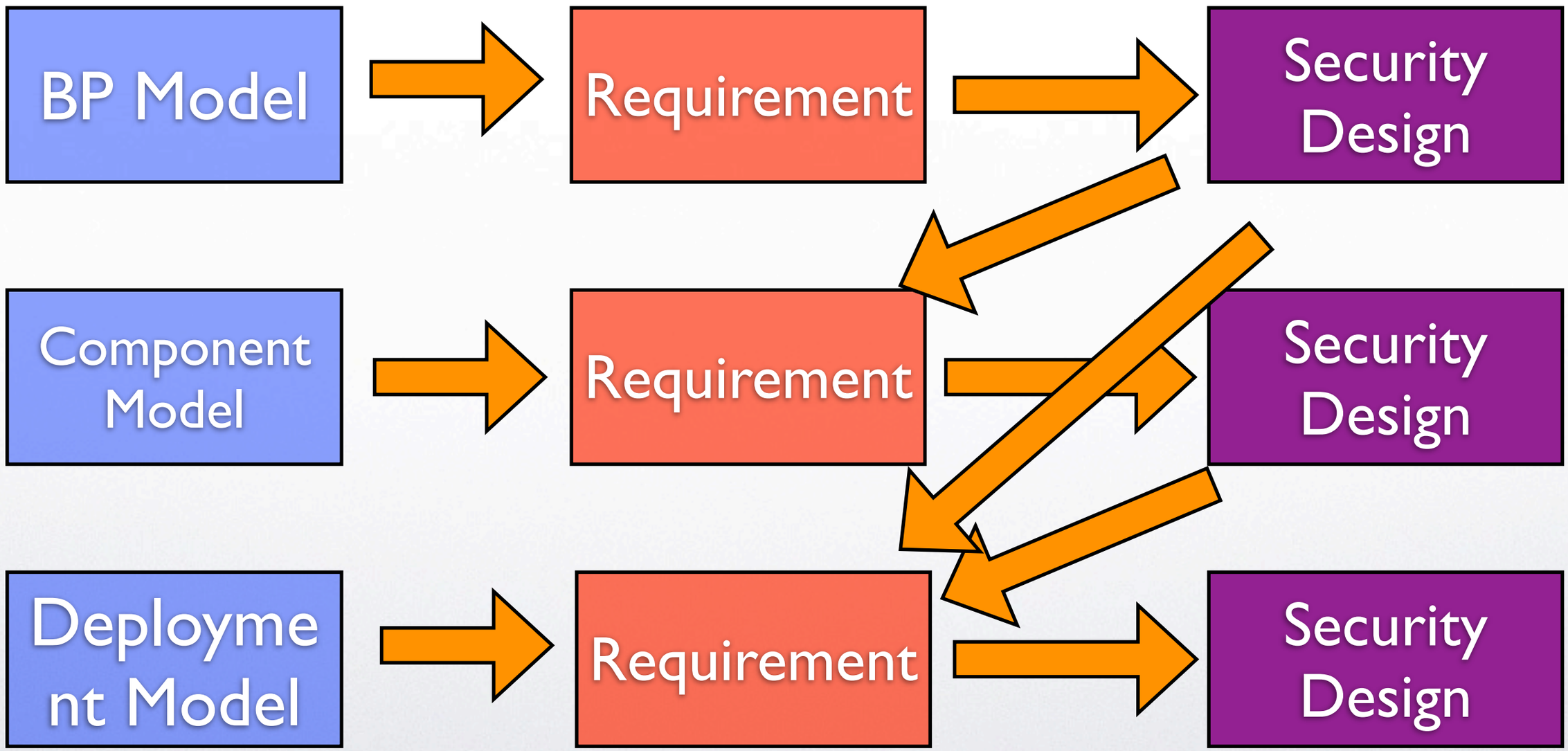
How to make a system secure



Multi-view Security Architecture

- Requirement
- Architecture
  - Business Process
  - Software Component
  - Physical Deployment
- Implementation

How to make a system secure



Future work

- Complete Case Study
- Verification Model

Thank you!