Securing the Last Mile in Continuous Deployment Pipeline

Building security-enhanced and consistent Continuous Deployment Pipeline

www.data61.csiro.au

A new architecture to build a security-enhanced and consistent Continuous Deployment Pipeline:

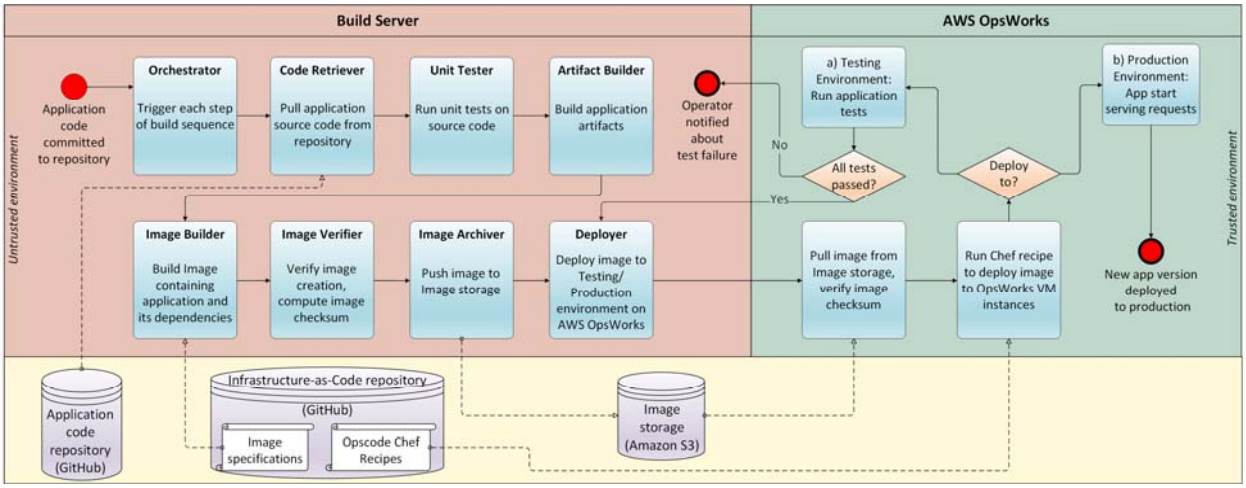
- Re-architecting with verifiable micro-services
- Reducing the attack surface and limiting the damage in case of a compromise

Problem Statement

- **Security in Continuous Deployment Pipelines is crucial**
  - Deployment security is product of pipeline security
  - Compromise of pipeline = compromise of deployment
  - Valuable target for attacks – but given little attention so far
- **Difficulties in securing a deployment pipeline**
  - Build server generally a monolithic system
  - Subcomponents run with same privileges
  - High complexity, large attack surface
- **Assurances are difficult to provide**
  - New approach needed: re-design pipeline

Approach

- **Re-architect pipeline as micro-services**
  - Subcomponents smaller, better verifiable
  - Restricted capabilities for each subcomponent
  - Composition tactics and security patterns to integrate subcomponents
- **Security benefits:**
  - Reduction in attack surface
  - Restricted impact if subcomponent breached
- **Engineering process:**
  - Secure one subcomponent at a time
  - Some subcomponents outside direct control, e.g., located with Cloud provider – isolate these



Impact

- Reference implementation of pipeline
- Library of formally verified building blocks
- Engagement with IT companies
- Research Publications
  - DSN 2015 paper in review
  - RELENG 2015 paper in review

Next Steps

- Reference architecture for Pipeline
- Consultancy for SMEs
- Case study with IT companies

FOR FURTHER INFORMATION
Paul Rimba
e Paul.Rimba@data61.csiro.au