INTRODUCTION

Serverless platforms free the web-developers from all backend management tasks and enable rapid prototyping of applications as a set of small functions (which may be readily available from third parties), where application logic is expressed in form of workflows. Serverless cloud also assists with features like autoscaling and pay-per-use. Moreover, conceptually serverless computing significantly raises the bar for attackers: small ephemeral functions execute separately from one another, and they have no local persistent storage.

Can these stateless ephemeral functions really lead to better security?

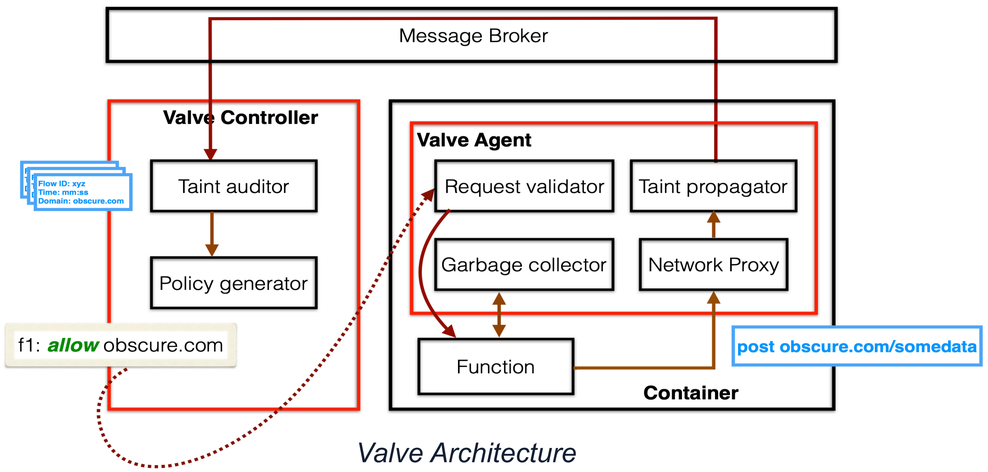
VALVE[1]

Problem

Untrusted third-party functions may introduce unintended flows within the serverless application.

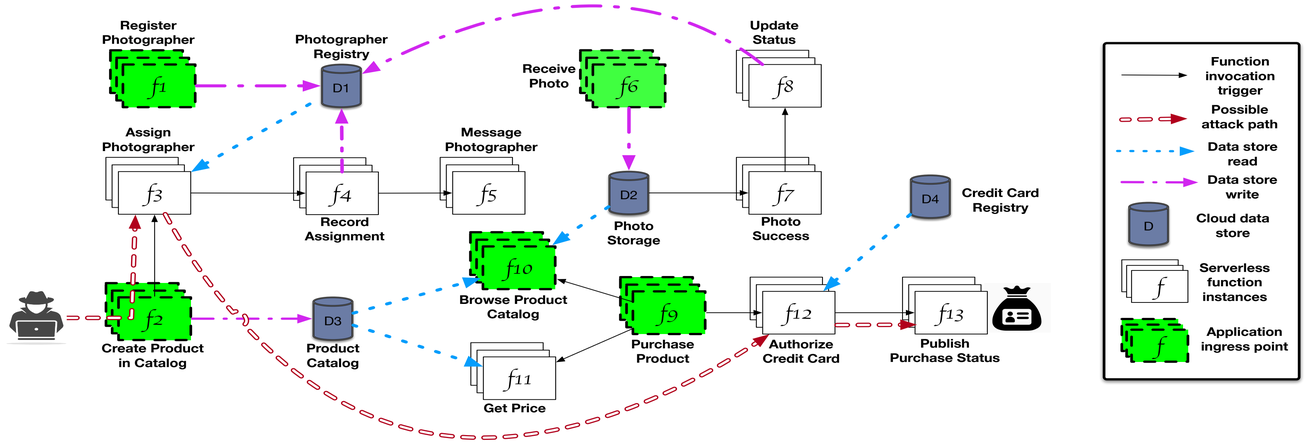
Solution

Discover hidden flows within the serverless applications and detect information flow violations among them.

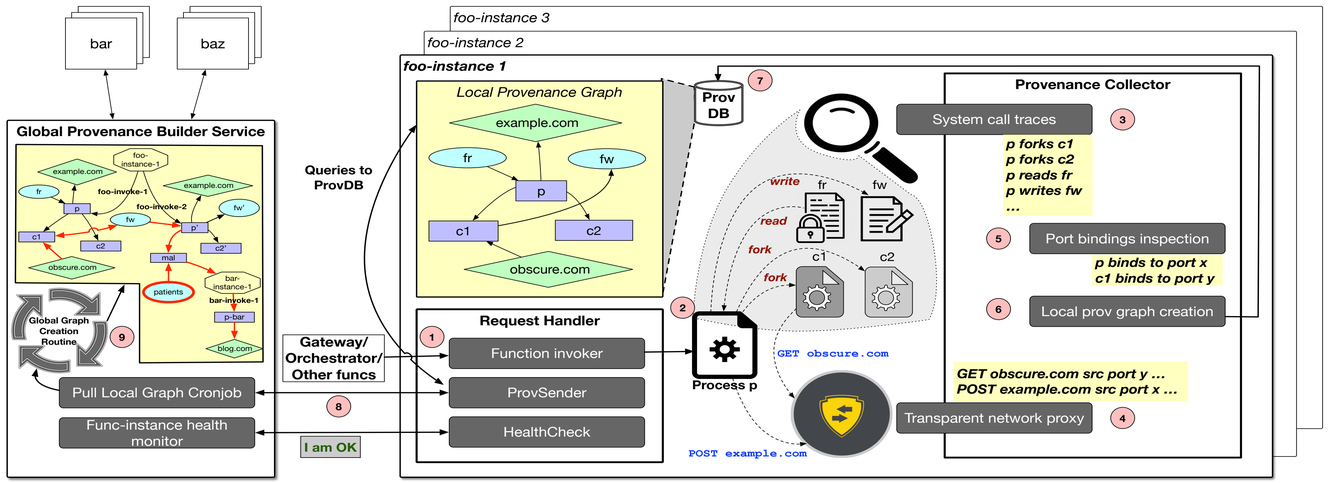


Valve Architecture

REFERENCE SERVERLESS APPLICATION AND ATTACK SCENARIOS



SERVERLESS AUDITING ARCHITECTURE



1. "Valve: Securing Function Workflows on Serverless Computing Platforms", Datta et. al., WWW 2020.
2. "Workflow Integration Alleviates Identity and Access Management in Serverless Computing", Sankaran et. al., ACSAC 2020.