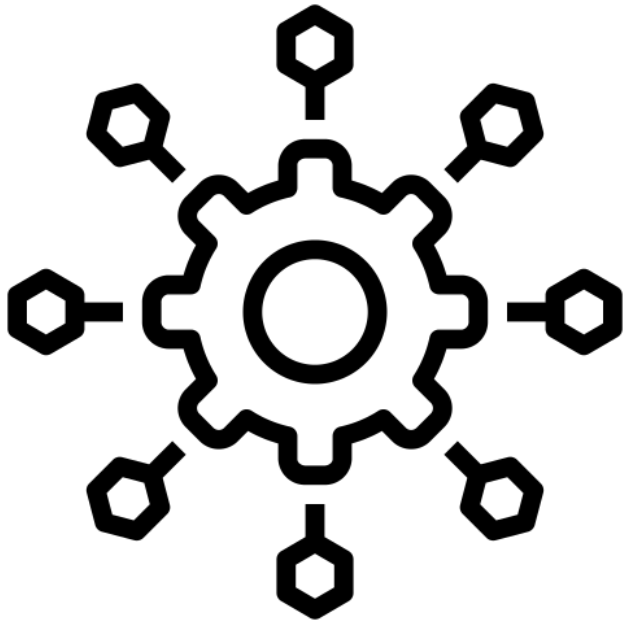
Механізми безпеки у мікросервісній архітектурі

Науковий керівник: Андрощук М. В.

Підготував: Чалюк А. О.

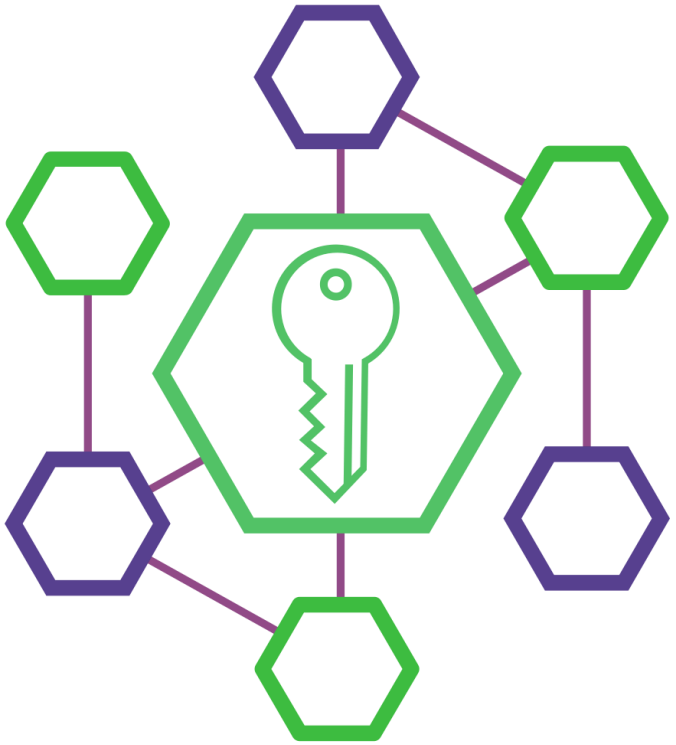
Актуальність теми

- Мікросервісна архітектура є популярною серед великих компаній (Netflix, Amazon, Uber, Spotify, SoundCloud)
- Нові види загроз зумовлені особливостями архітектури
- Постійна «гонка озброєнь» за участі розробників і хакерів



Мета

Огляд механізмів протидії проблемам безпеки мікросервісної архітектури та створення застосунку з використанням найсучасніших механізмів безпеки для їх демонстрації.

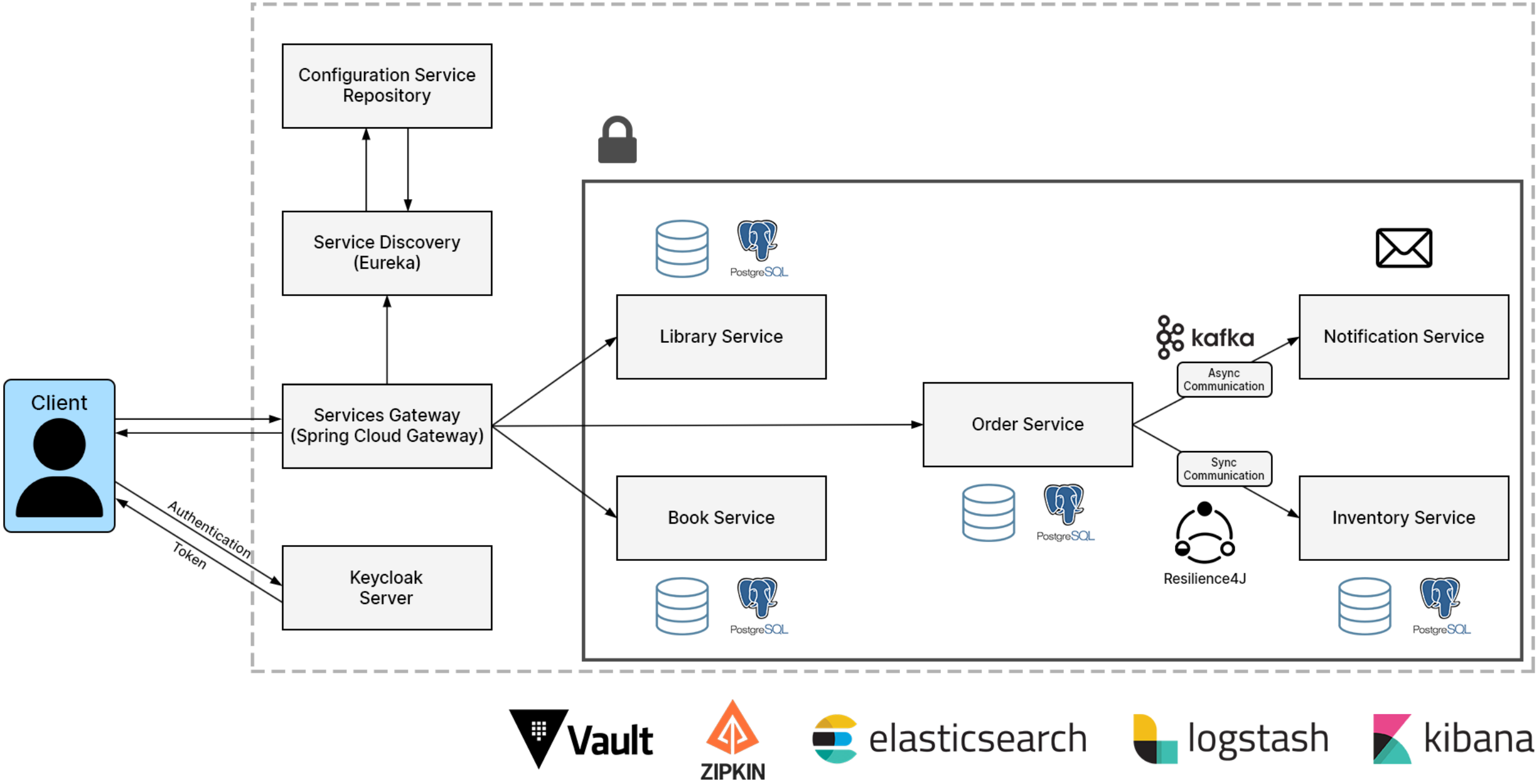


Види загроз

- Проблеми з контролем доступу
- Мережною комунікацією
- Витоком чутливої інформації
- Розгортанням сервісів

Механізми захисту

- Аутентифікація та авторизація
- Використання mTLS та JWT
- Шифрування конфіденційної інформації
- Моніторинг системи
- Використання DCT, мінімальний набір дозволів контейнерів, відокремлене зберігання чутливої інформації


Configuration Service Repository
Service Discovery (Eureka)
Client
Services Gateway (Spring Cloud Gateway)
Authentication
Token
Keycloak Server
Library Service
Book Service
Order Service
PostgreSQL
kafka
Async Communication
Sync Communication
Notification Service
Inventory Service
Resilience4J
Vault
ZIPKIN
elasticsearch
logstash
kibana

Інструменти для перевірки

OWASP
Zed Attack Proxy

sonarqube

Висновки

- Розглянуто різні проблеми безпеки та підходи їх пом’якшення
- Створено мікросервісний застосунок
- Використано сучасні технології до безпеки

Дякую за увагу