Synthesis of forensic-ready software architectures for microservices-based systems

Presenter: Davi Monteiro (davi.monteiro@lero.ie)
Supervisors: Bashar Nuseibeh, Yijun Yu, Andrea Zisman

Introduction

- What is the microservices architectural style?
- What are the benefits and drawbacks?
- Why microservices need to be forensic-ready?

Motivating example

- Shopify case study - confused deputy problem

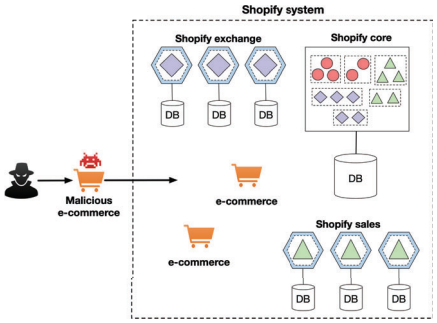


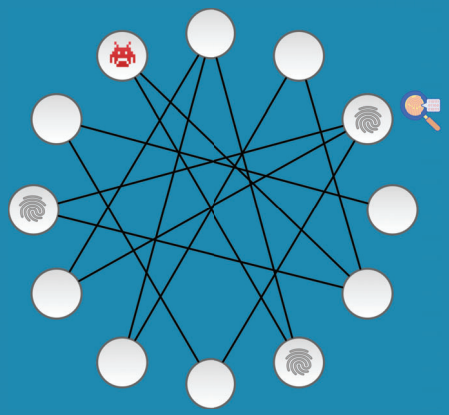
Fig. 1. Shopify e-commerce platform: a hybrid approach of monolith and microservices architectures.

Digital forensic challenges

- Ephemeral environments
- Dynamic attack surface
- Investigation space problem
- Islands of knowledge problem
- Post-*mortem* analysis

References
[1] Yan Cui, "Capture and forward correlation IDs through different Lambda event sources," 2014. [Online]. Available: https://hackernoon.com/capture-and-forward-correlation-ids-through-different-lambda-event-sources-220c227c65f5
[2] W. Li, Y. Lemieux, J. Gao, Z. Zhao, and Y. Han, "Service mesh: Challenges, state of the art, and future research opportunities," in 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), April 2019, pp. 122–1225.
[3] Blackwell, C. (2010). Improved situational awarenss and response with enhanced OODA loops. In 6th CSIIR Workshop. ACM Press.

How to **facilitate** digital forensic investigations in **microservices**-based systems?



Automated **reasoning** to explain the **contributing factors** that led to an **incident.**

For more information, please scan the QR code.

Lero THE IRISH SOFTWARE RESEARCH CENTRE
Science Foundation Ireland sfi For what's next
University of Limerick
Ireland's European Structural and Investment Funds Programmes 2014-2020
European Union
European Regional Development Fund
Southern Regional Assembly

How complex microservices-based systems can be?

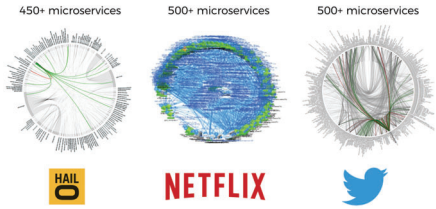


Fig. 2. Examples of microservice architectures using death star diagrams [1].

How to monitor microservices-based systems?

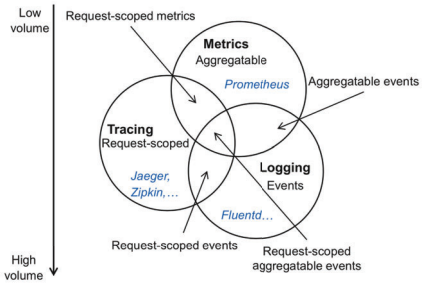


Fig. 3. Venn diagram for monitoring microservice-based applications [2].

Problems with the monitoring

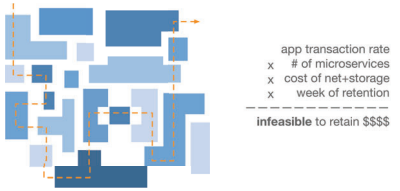


Fig. 4. Distributed tracing in microservice-based applications.

How to investigate incidents in microservices-based systems?

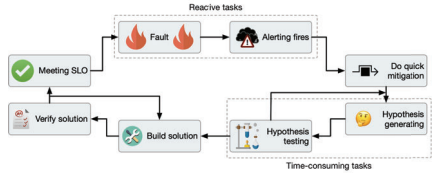


Fig. 5. An investigation feedback loop based on the OODA loop [3].