TOWARDS MICROSERVICES SECURITY CONTROL LAYER

Alessandro Molari, Eugenio Cavina and Eugenio Pierfederici
Cyberloop
alessandro.molari@cyberloop.it, eugenio.cavina@cyberloop.it,
eugenio.pierfederici@cyberloop.it

Abstract

Adapting applications to a microservices approach brings a series of advantages along with new challenges in project, deployment, monitoring and governance. For this reason, it is important to decouple security aspects from the actual microservices logic, as they are orthogonal to the logical specifications of the microservices. This means that an independent security control layer allows to simplify control and governance over those aspects by defining rules, policies and controls in a logically centralized way, even if those rules are then physically applied in a distributed way. Our final objective is to provide an enterprise architectural approach to handle those security aspects as first-class citizens, thus oriented to a security-by-design methodology.

1 Introduction

The idea behind microservices is to split applications in a smaller set of interconnected services with clearly defined interfaces instead of building a single monolithic application. This approach requires new architectures, design patterns and paradigms to manage and govern the complex set of relationships that the distributed system needs. That brings new security challenges and opportunities. In-depth security applied to the traits of microservices requires to take decisions using global information rather than local to the single microservice in order to be effective. This can be accomplished by creating a security decisional process that includes control, management and governance taking decisions based on available global information instead of microservice local information. This allows to propagate the information in the whole network of services, without the need of each service to observe the same behavior before taking action against a specific threat. Moreover, global knowledge of the whole system provides a better understanding of stage and level of compromise, that can be extremely effective in reducing the response time and increase the number of threats identified.

The nature of a microservice (do one thing and do it well) is an opportunity to apply strict policies for each of them, maximize cybersecurity efficiency and resiliency to attack, difficult to accomplish with a monolithic approach where requirements and interfaces are not easily circumscribed.

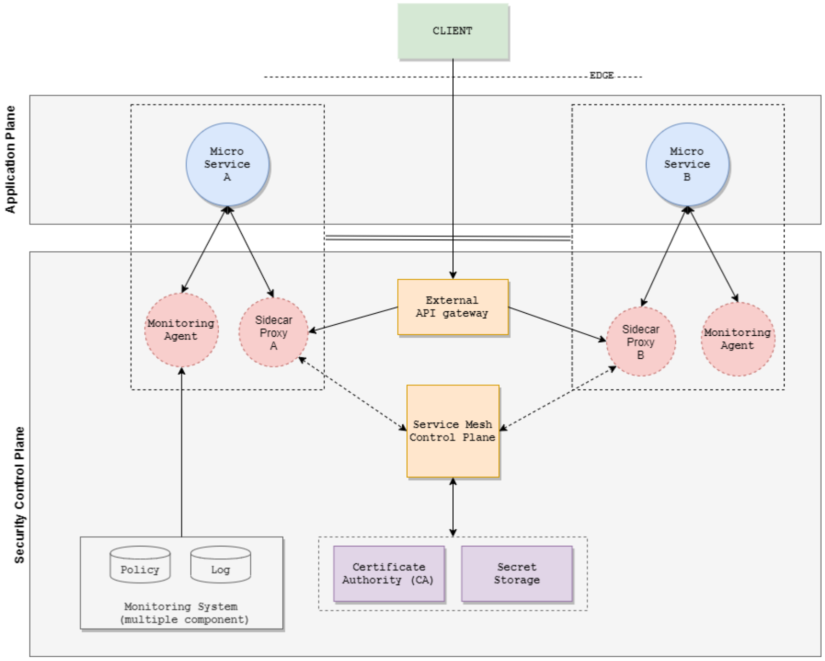
Moreover, the highly descriptive nature of microservices can be followed with a security-as-code approach. This allows to know every cybersecurity rule and control ahead in time, to replicate in any environment and to the generic infrastructure-as-code approach.

Microservice security is a multifaceted problem and it relies heavily on underlying technologies and the surrounding environment (Yarygina & Bagge, 2018). Starting from this concept we analyzed the problems in the enterprise environment in which we operate and defined an architectural approach consistent with modern security requirements with an example of technological open source stack to guarantee a reasonable level of security in a microservices environment.

This approach is based in having a layered security control plan that evaluate transversal aspects with respect to deployment requirements, interconnection security and runtime/behavior security. It also must respect features such as scalability, lightness and ease of automation to be adoptable by enterprise organizations.

We present a fully integrated framework to simplify management, control and governance of security aspects specific for a microservices ecosystem.

Even though it covers generic attacks, the focus is in dealing with targeted attacks and tailored cyber-attack kill-chains: in this case it is mandatory to protect every component of every application distributed on each node and every single interconnection of every microservice. In particular, it allows to rapidly contain and mitigate risk in a rapid and effective way to minimize impacts of cyber-attacks.



References

Yarygina, T., & Bagge, A. H. (2018). Overcoming Security Challenges in Microservice Architectures. *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 11-20. doi:10.1109/SOSE.2018.00011