To: Professor Krasso

From: Jonathan Disla

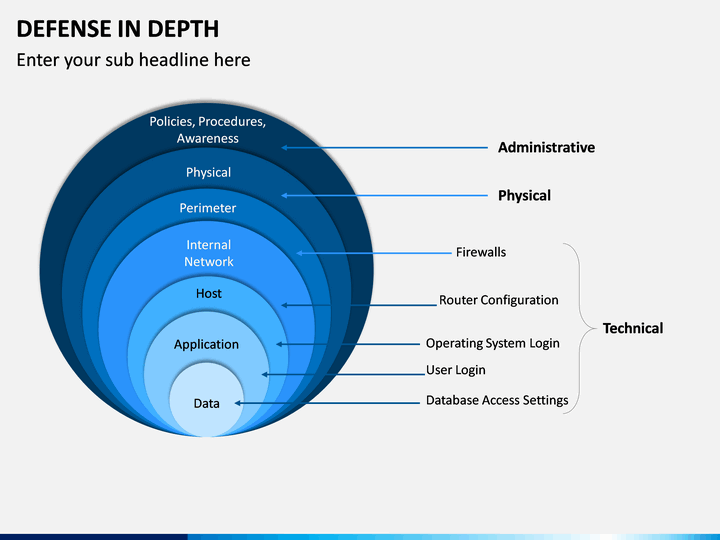
Date: 7 May 2021

Subject: Securing Micro services

There are various ways to secure micro services. Firstly, micro services are independent services that communicate together. An application is structured in the form of small services around the business domain or communicating around the business logic of the application. In this memo, I will cover the security risks of using micro services, the depth defense mechanism and tokens with API gateway.

While there are many benefits to this architecture such as flexibility, shorter development times and scalability, there are also risks that we can handle by securing micro services. For example, micro services communicate with each other including with 3rd party applications. This creates a security threat from the 3rd party application being able to gain access to the micro services data causing a breach. Thus, security of individual services is one of the prominent problems in a micro service architecture.

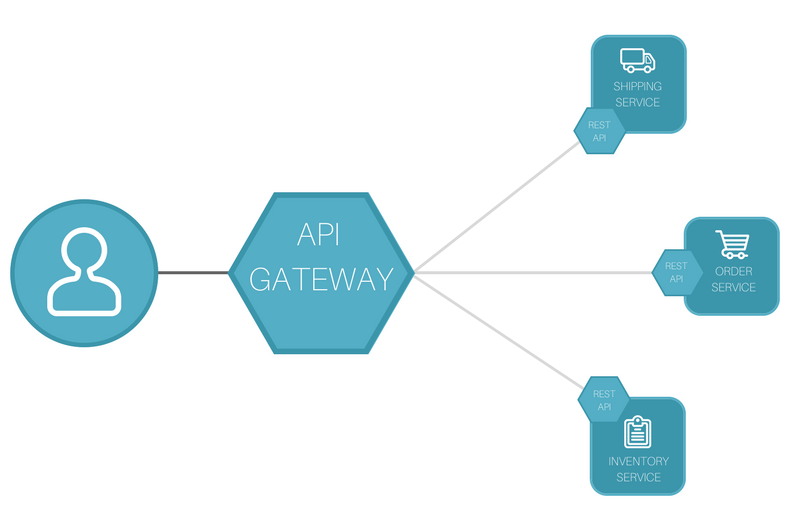
The defense in depth mechanism acts in the way of layering security around the services. We can think of this as putting together a sandwich where there are layers of I ingredients inside. The point of the depth mechanism is that a threat has to go through different layers of security to potentially breach the security of the micro service. The benefit to this mechanism of security is that if an attacker can get past the first layer, by the time they get to the second layer the service should have alerted of the breach. According to edureka, “potential attackers cannot crack the security on a single go, and have to go forward and try to crack the defense mechanism of all the layers” (edureka).



*Fig. 1. Defense in Depth*

*sketchbubble.com*

We are all familiar with going to a website and within seconds of loading the page, we are asked to accept the storing cached and cookie data. Tokens are stored in the form of cookies to easily identify a user. The way to secure this token is to use Jason Web Format (JWT). JWT is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object (jwt.io).

*Fig. 2. API Gateway. Express gateway*

An API Gateway adds an extra element to secure services through token authentication. This gateway is what essentially hides the micro services from a third party client limiting the possibility that the client can cause a security threat services. The client communicates only with the API gateway and the API gateway gathers the services requested.

References

Edureka. “*Microservices Security | Best Practices To Secure Micro Services”.* YouTube, 8 October 2019.

https://www.youtube.com/watch?v=wpA0N7kHaDo&ab\_channel=edureka%21

JWT. “*Introduction to JSON Web Tokens”.* Jwt.io, Accessed 7 May 2021.

https://jwt.io/introduction