To: Professor Krasso

From: James Brown

Date: 20 June 2020

Subject: Securing Microservices

Hello Professor. Thank you for approving our proposal to implement microservices. Before we start development, it is important for us to understand how we are going to implement a security model that ensures our systems are up to standard. Without security at the top of mind, our applications will not be secure.

How do we plan to keep our microservices secure? We will do so through the use of OAuth, 24/7 monitoring, reputable third parties for encryption and decryption, and ensuring security as at top of mind when our team is writing the code. This list is not all encompassing; however, these items will allow us to lay the groundwork for securing our microservices.

What is OAuth? OAuth stands for Open Authentication and is an industry standard security protocol that is used for authenticating clients who use whatever services you are creating. (OAuth) By being able to authenticate users, we will be able to control who access our systems and how frequently. As OAuth is also an industry standard, we know it works well and can be trusted. This is a huge advantage in comparison to building our own authentication protocols.

In addition to using the OAuth protocol, we will use a third-party system called “Prometheus” for 24/7 monitoring. Prometheus was built by the engineers at Soundcloud and is well known for being extremely reliable and giving robust reporting into monitoring. (Triosi). By monitoring our systems 24/7, we will have insight into potential attacks, service usage, and reporting that will help us optimize the services performance.

Up next, we will be using Amazon KWS for encrypting our OAuth secrets. What does this do? This ensures that the actual value of the secret is kept a secret (no pun intended). (Raible) We could write our own code for encrypt this, but that would leave us open to vulnerabilities. There are a lot of moving parts to security, and the industry has been developing security standards for many years, so it doesn’t make sense to re-invent the wheel.

Last, but not least – we should always keep security at the top of our minds when writing any code. This habit will in turn lead to us making a microservice that is more secure. Security can make or break a company, so I believe it should always be a conversation that is had when writing any software.

In summary, I believe implementing the above suggestions will help ensure that we have a system that is secure. Thank you for your time and consideration.

References

OAuth 2.0. (n.d.). Retrieved June 20, 2020, from https://oauth.net/2/

Raible, M. (2020, March 23). Security Patterns for Microservice Architectures. Retrieved June 20, 2020, from https://developer.okta.com/blog/2020/03/23/microservice-security-patterns

Troisi, M. (2019, November 15). 8 best practices for microservices app sec. Retrieved June 20, 2020, from https://techbeacon.com/app-dev-testing/8-best-practices-microservices-app-sec