To: Professor Krasso

From: Faye Van Roekel

Date: December 5, 2019

Subject: Security Recommendations for Microservices

This memo is to confirm that the company has decided to implement and deploy microservices and discuss security of the microservices. Outlined below are some recommendations for security options for the microservices. If the three discussed below are not ones that we find feasible for us there are more options to look into as well.

1. The company could adopt OAuth 2.0 as our standard for user authentication. OAuth2 is currently the industry standard. Some of the benefits of OAuth 2.0 are that it gives choices of how a user can get an access token:
   1. through authentication with an “authorization server”,
   2. through a redirect from a third-party site to a URL containing an access token, or
   3. through using the username and password from a third party site (such as Google) to obtain a token.

The benefit would be flexibility in setting up our user authorizations. There are a few vulnerabilities in the form of an attack such as insecure storage of secrets, lack of confidentiality of data and server trust. If a solution would be built to improve the security level of OAuth it would be beneficial since there are several libraries and platforms for OAuth that we can use to speed up our development phase.

1. Another option the company could adopt would be a defense in depth protocol for our more sensitive services. Defense in depth means that if we apply several layers of security to the services, an attacker would have to overcome not just one but all of our defenses to access those services. Fine-grained firewalls could be built between each service which would include sets of rules and host-to-host encryption. Since the company would be using microservices it would then allow more fine-grained security, such as service-specific rules to containers, APIs and firewalls.
2. A third option for the company would be analyzing our data stores component-by-component and decide if any of them would need encrypting. An advantage is data for each service is independent of other data, and we there wouldn’t be overhead of encrypting unimportant data just so we can encrypt the important data.

If the above options are not ones that the company would decide to use there are other options that can be explored as well in securing our services. The recommendations above would be best implemented as the microservices are set up and deployed. By taking action on security now, there would have assurance of safety in deploying the services and making them available.

A close up of a map

Description automatically generatedExample of Microservice Architecture

(Richardson, 2019)

**References**

Richardson, C. (2019). What are microservices? Retrieved December 5, 2019, from <https://microservices.io/>

Johanna Curiel. (n.d.). The State Of Social Authentication: Is OAuth Up To The Job? (article). Retrieved from <https://techbeacon.com/security/state-social-authentication-oauth-job>

Carrie Wodehouse. (n.d.). Tips For Securing A Modernized Service-Based Architecture (article). Retrieved from <https://www.upwork.com/hiring/development/microservices-security/>