to: acme business solutions, L.L.C.

from: Matt Howard

subject: Securing microservices

date: June 21, 2018

cc: tech solutions, l.l.c.

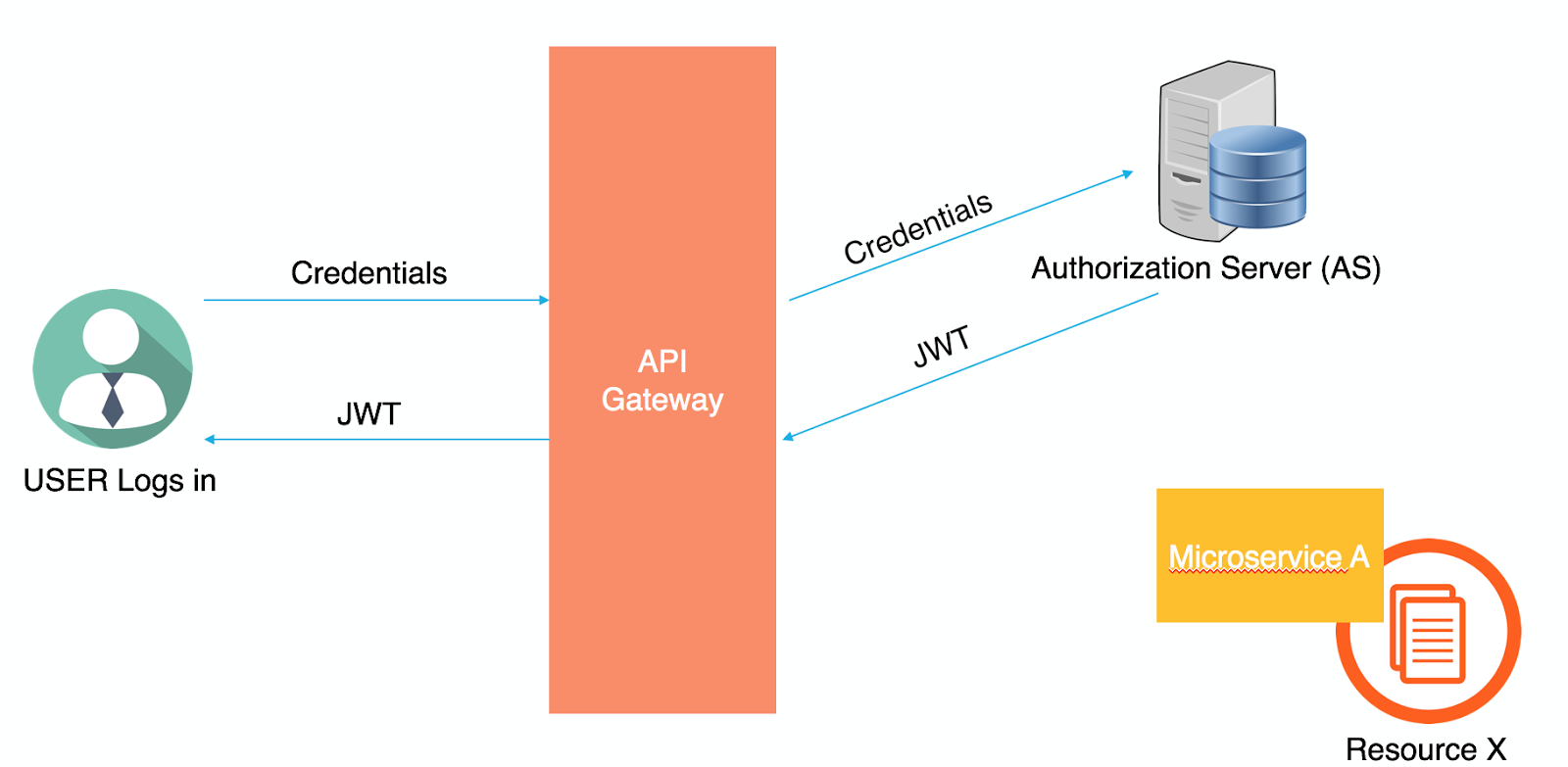
# securing microservices

This memorandum sets out the process and procedures Tech Solutions, L.L.C. will use to secure the microservices of ACME Business Solutions, L.L.C.

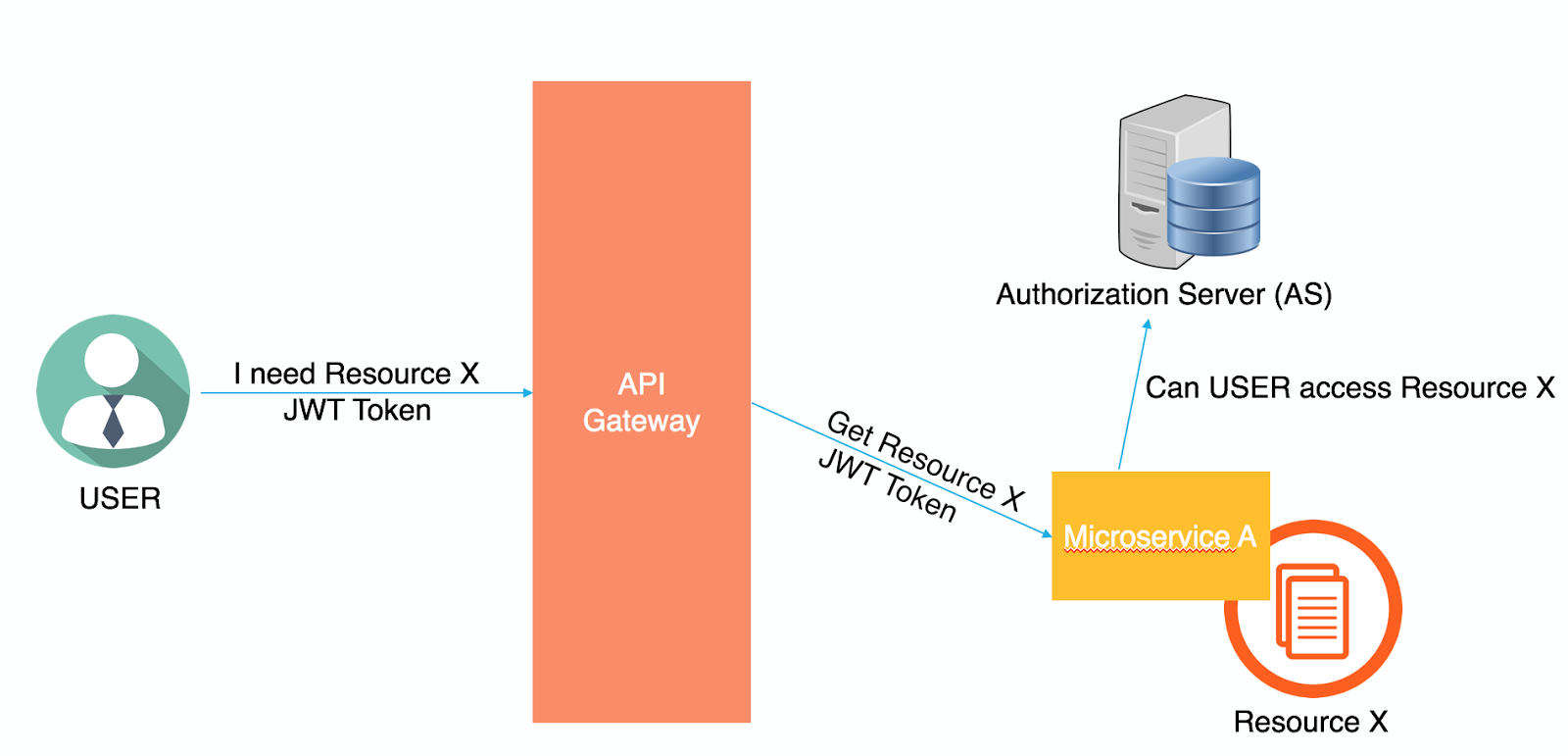
The technology you put into your business should add value by supporting your businesses objectives and facilitating its efficiencies. Securing these assets is just as important, if not more than, as their processing and request handling ability. Tech Solutions, L.L.C will secure your microservices by using “Defense in depth” to supply multiple layers of security controls throughout your microservice. This will prevent any would-be attacker who may be able to exploit one security layer from accessing the microservice by making them figure out how to defeat all of your defenses. (Troisi, 2018)

We will start by identifying the most sensitive services you have. We will build an API Gateway using OAuth2 to handle user identification and access control of your web and desktop applications. OAuth/OAuth2 are the industry standard for user authorization. OAuth2 gives access to user data while at the same time protecting their account credentials. It does this by delegating user authentication to the service that hosts the user account. Then authorizes third-party applications to access the user account. (Siraj, 2017)

How API Gateway works (Siraj, 2017)



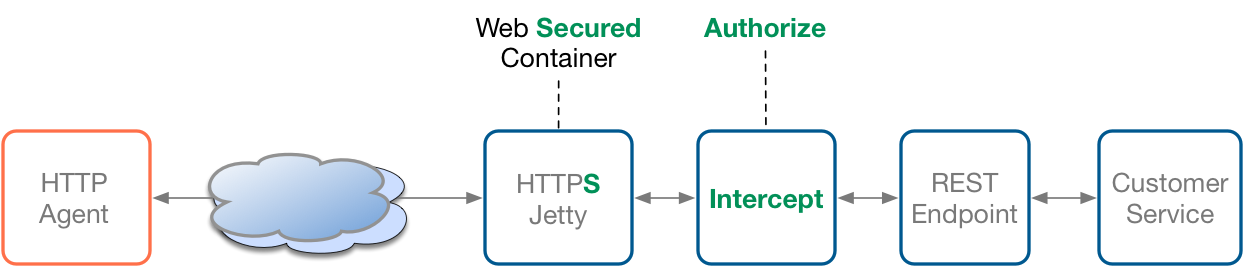
How OAuth2 works (Siraj, 2017)



We will then use NaCl/libsodium for encryption and enable automatic security updates. Automatic security updates are the best way to ensure your microservice architecture is secure and scalable at the same time. We’ll do this in the early development phase so it easier to keep all of the software under control. (Troisi, 2018)

Using containers will enrich the architecture and enable SSL/TSL security layer to encrypt the data exchange between the HTTP Agent and the Server. The HTTP Web Container will be responsible for authenticating the user and restricting access to the web resources, while the interceptor will become for authorizing access to the service. (Moulliard, 2016)

How Web Containers Work (Moulliard, 2016)



We will build a very staunch, security system for your microservice architecture, to minimize the risk of attacks and data breaches.

## Resources

## Troisi, M. (n.d.), 8 Best Practices for Microservices App Security, Retrieved 21 June 2018, from: <https://techbeacon.com/8-best-practices-microservices-security>

Sirajs, M. (2017 September 20th), Software Development Times, Securing Microservices: The API Gateway, authentication, and authorization, Retrieved 21 June 2018, from: <https://sdtimes.com/apis/securing-microservices-the-api-gateway-authentication-and-authorization/>

Mouillard, C. (2016 June 28th), Security Enforcement of Microservices, Retrieved: 21 June 2018, from: <https://dzone.com/articles/security-enforcement-of-the-microservices>