Aalto University
School of Science
Bachelor's Programme in Science and Technology

Security in Microservice Architecture

- Impact of a Switch from Monolith to Microservices

Bachelor's Thesis

xx. xxxxxkuuta 2020

Tommi Jäske

Aalto-yliopisto
Perustieteiden korkeakoulu
Teknistieteellinen kandidaattiohjelma

KANDIDAATINTYÖN
TIIVISTELMÄ

Tekijä:	Tommi Jäske
Työn nimi:	Turvallisuus mikropalveluarkkitehtuurissa - Monoliitisesta arkkitehtuurista siirtyminen mikropalveluarkkitehtuuriin ja sen vaikutukset.
Päiväys:	xx. xxxxxkuuta 2020
Sivumäärä:	?
Pääaine:	Computer Science
Koodi:	SCI3027
Vastuuopettaja:	Professori Eero Hyvönen
Työn ohjaaja(t):	Professori Tuomas Aura (Tietotekniikan laitos)
Kirjoitetaan myöhemmin.	
Avainsanat:	avain, sanoja, niitäkin, tähän, vielä, useampi, vaikkei, niitä, niin, montaa, oikeasti, tarvitse
Kieli:	Suomi

Aalto University
School of Science
Bachelor's Programme in Science and Technology

ABSTRACT OF
BACHELOR'S THESIS

Author:	Tommi Jäske
Title of thesis:	Security in Microservice Architecture - Impact of a Switch from Monolith to Microservices
Date:	MonthName 31, 2020
Pages:	?
Major:	Computer Science
Code:	SCI3027
Supervisor:	Professor Eero Hyvönen
Instructor:	Professor Tuomas Aura (Department of Computer Science)
Will be written.	
Keywords:	key, words, the same as in FIN/SWE
Language:	English

Contents

1 Introduction

In recent years the mobile applications have revolutionized our daily lives. These services have infiltrated social life, shopping and almost every aspect of our existence. The services and their apps compete of our time and markets are reinventing themselves constantly. The rapid expansion and at times even faster decline of these web services need a matching architecture to meet these very specific needs.

There are many web services already in use which have been designed and implemented before the onslaugh of microservices. Some of these services need to evolve to be of use in the future. In many cases the monolith services have already started to use certain aspects from the microservice world, such as access tokens and REST API:s. The pressure from new competitors adopting new technologies right from the start and the fact that the industry and its developer base are extremely young dictates that the old and established services have to address the situation someway or the other. Monoliths have served us well but the time has come to evolve with the customer needs.

When new development is carried out by a startup the initial architecture might still be a monolith one. Newman (2019) states that due to limited resources a monolith might be a better fit to these companies trying to navigate to the actual product they are to offer. In the case of success the need to rapidly scale the offering emerges. Newman (2019) refers to these companies as ”scale-ups”. Newman (2019) also states that it is much easier to refactor an existing service than to create a new one and thus the need to split monoliths to microservices is and probably will be relevant to the near future.

Kalske et al. (2018) finds that as the codebase becomes large the MA leads to slower development. This is due to the possible complexity inherint in the entwined monolith. The number of placess to refactor is much larger than in a small microservice. Microservice should do one thing and as such it should be more understandable.

Stackoverflow annual survey (Stack Overflow) conducted on developers finds that half of the respondents identified as full-stack or backend developers. The professional developers had very little experience and about 40% of them had less than five years of professional experience.

The new developers entering the work force have very different mindset than the older more seasoned professionals. Thus, it is very clear that the ways of working and paradigms to be used are in constant change. The old and established have to embrace the change and refactor their architecture before it is too late. Microservices are not the proper choice for all needs (Newman, 2019) but in many cases there simply is no other valid choice. This change needs to happen in an orderly and safe way and the security aspects need to be addressed.

Microservice Architecture (MSA) differs in many ways from the more tradition Monolith Architecture (MA). This shift entails very specific security issues.

In this thesis the MSA and security literature is evaluated and the main differences between MA and MSA on security aspects are found.

The first chapter discusses the ... The last chapter in the thesis contains the conclusions and presents further research topics.

2 Monolith

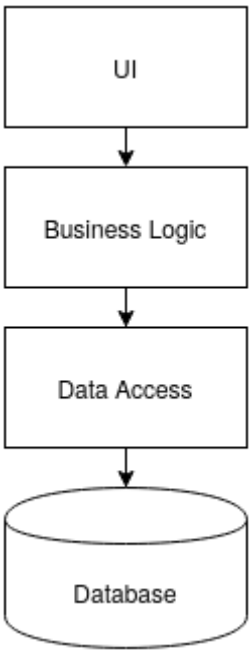

Figure 1: Traditional Monolithic Architecture (Kalske et al., 2018)

3 Changing the architecture

To change the architecture from MA to MSA should in general be a gradual process. The MA is or at least should be split to modules with separation of concerns (Yarygina, 2018). The actual splitting of the monolith can be carried out in various ways. One of whic is DDD (SOURCE FOR THIS).

The MSA differs from a MA in fundamental ways. According to Fowler and Lewis (2014) one of which is the communication between its components. In a monolith application the processes can send function calls or method invocations amongst them selves. In MSA the messaging is based on sending messages or HTTP requests.

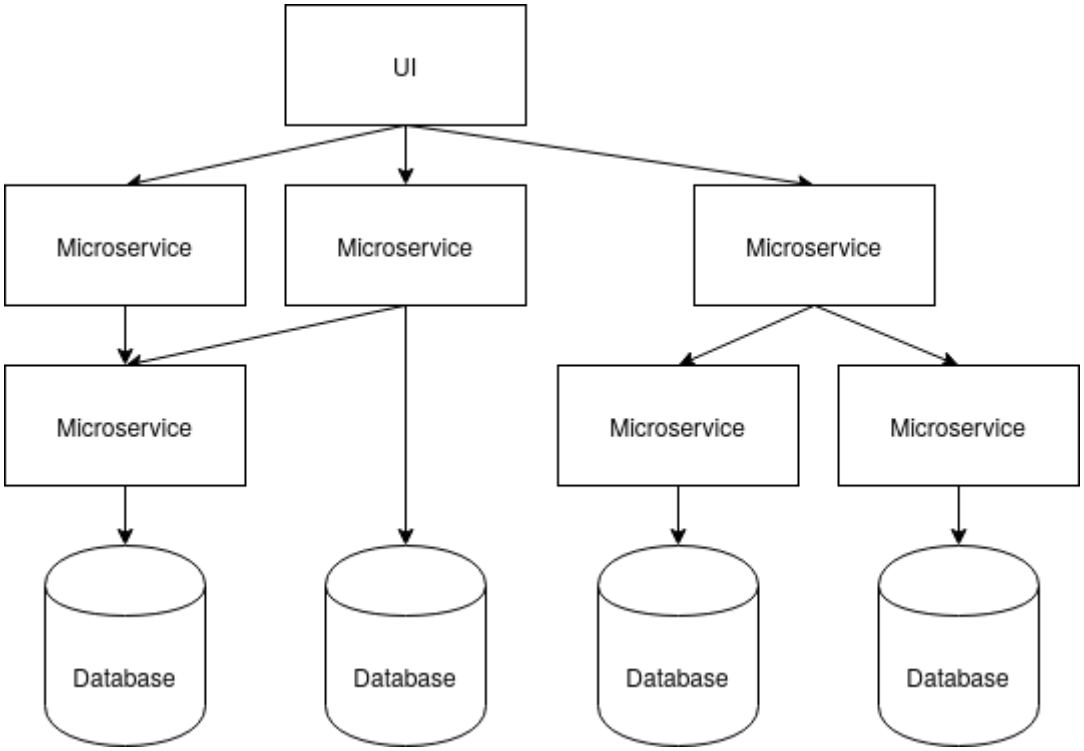

Figure 2: Microservice Architecture (Kalske et al., 2018)

Function calls entail a stackframe creation in the call stack, execution of the function code and finally popping the stackframe and returning the result. The actual overhead depends on the language and systems used to run the application (SOURCE). Compilers can optimize the code further and inline the function calls to eliminate the stackframe creation and following procedures to be carried out.

Communication using the network is extremely slow. In a paper Zari et al. (2001) studied the response times of web sites offered to the public. The websites response times where measured in seconds.

The requests sent to other microservices throught the network are extremely slow when compared to operation within one computer as the function calls would be. Therefore, the communication patterns should be changed to take into account the change in communication path.

If the architecture is changed in such a way that the previous communication model amongs the components is preserved, there would be an excessive amount of communication and the resulting system is not as performant as it could be (Fowler and Lewis, 2014).

4 Security

Richter et al. (2018) implemented a test system mimicking the Deutsche Bahn seat reservation system using MSA. The technologies used in the study were: Amazon Web services as the deployment platform, Elastic Compute Clouds running on Kubernetes nodes, and Docker for containers in which the actual services were run. They found out that the cloud-based infrastructure when used in MSA resulted in a more complex solution than in MA. The complexity in modern software systems is inherent. Implementing security is very difficult and resource intensive. The rewards from a good security are invisible. When microservices are implemented or even planned the security should be taken into account as early as possible. Implementing security later on the project or as an after thought is can be more expensive and very difficult.

The added layers all have to be configured correctly and an error in one could potentially compromise the whole system.

5 Authentication

In these cases where the user has to be authenticated the web service needs a way to do this securily. Usually authentication is done using a tuple containing user credentials i.e. a username and a password for the user. The user is authenticated and a key or token is transmitted to the user via the network. This communication should in both MA and MSA be encrypted in a way that none of the actors in the transfer path can intercept the message and be able to use the credentials.

The credential counterparts i.e. shared secret by the server and the user have to be available for the web service for verification. When using MSA the service should own it's own data. When ever such information is available it is a target for thieves and hackers. The services in MSA are to be individually deployable and the service scalable. Authentication service implementation has to take this into account. The service has to adhere to practices that minimize the risks of data breaches.

session, JSON Web Token (JWT) https://tools.ietf.org/html/rfc7519, token (JWT, OAuth 2.0), (API gateway, IdP) vs distribution

Identity and Access Management (IAM), Identity federation, Azure Active Directory, Active Directory Federation Services (ADFS), Google, Facebook, Twitter, LinkedIn etc., Single-Sign-On (SSO), Security Assertion Markup Language (SAML), SAML identity provider, OpenId provider, OAuth, OpenId Connect (OIDC), Identity Management: Identification, Authentication, Authorization. ...

5.1 Java Script Object Notation Web Token (JWT)

JWT is a format to represent claims. It is base64 encoded point separated strings which concatenated can easily be carried in the HTTP request or response. The contents is key value pairs and the token may or may not be signed and encrypted (Jones et al., 2015b). The token may contain expiration time. If the token is used to validate requests without a server side implementation that can revoke a token it will be valid until this time.

The JWT token is issued by an authority trusted by the service or services. The issuer has to sign the token for there to exist any real authoritative weight on it.

The signing of JWT can be carried out in various ways. These are presented in the Jones et al. (2015a). The signature is computated using the algorithm and keys or certificates specified in the header values. When the token is signed using PKI private key it can be verified by all parties in possession of the public key.

The choices for signing algorithm for signing the JWT algorithm contain ”none” as one of the choices. This was found to be troublesome by McLean (2015). He found that many libraries did not operate in desired way. The receiving party could be fooled to validate a mutated token without any signature with the ”none” as it's algorithm. In addition to this vulnerability McLean (2015) found that the verification suffered from another fatal flaw. When a token was created by using a symmetric algorithm the servers could be fooled to believe that a token signed by just the public key and not the secret HMAC -key was a valid one.

5.2 Attacks

Authentication can be attacked by a multitude of methods.

- Cracking
- Impersonation attacks
- Hacking the system
- Malware
- Social engineering
- Cracking the encryption on the communication channel exchanging credentials and keys or tokens.

From 2013 onwards malware and data breaches performed by hackers have increased and the scale of the damage is massive. The user data containing also the user passwords

or hash thereof is valuable commodity which can be traded in the black markets. The damage of the dataloss can be susbtantial. The estimated value from the Yahoo data breach is over $440 billion. The attacks seem to have been targeted to entities with valuable data and also to such targets that are lacking secure infrastructure. The least likely target to be hacked where non profit organisations and the most likely were medical related organizations (Hammouchi et al., 2019).

The hacked account credentials have to some extent been available for download from the web. Hunt (2020) created a service where everyone can verify whether any of their accounts are amogst the ones added to the service. The service named as "';– have i been pwned ?" allows users to enter their username or password to the site and see a result.

5.3 Authentication in Monolith

Discussion on various ways to execute authentication in MA.

5.3.1 Authentication in Microservice Architecture

6 Authorization

Authorization of the user rights can be implemented in various ways. One of which is an authorization service which can contain the access control matrix. Services being accessed verify from the authorization service that a particular user or the role that the user has can access the requested service or functionality.

In a MA the access rights to a functionality can be implemented using annotations within the source code. This can be effective since the verification can be done in memory or atleast without network communication. If a session is used it can contain the information needed to verify access rights.

In contrast to the MA in the MSA the access control matrix or matrices can't be as easily accessed. In order to verify that a specific right exists the service would have communicate with the authorization service every time a user tries to access a functionality with access restrictions. This could potentially lead to an extremely lively communication from all the services a formation of a bottleneck to the service.

https://techbeacon.com/security/microservices-apps-do-identity-access-management-without-overhead

6.1 Authorization in Monolith Architecture

In MA it is possible to implement features in such ways that a session can carry user information. This information can consist of granted roles and rights for the user. This session can be queried when e.g. access control is needed to execute an action or operation.

6.2 Authorization in Microservice Architecture

7 Session

7.1 Session in Monolith

7.2 Session in Microservice Architecture

8 Cloud

8.1 Monolith

8.2 Microservices Architecture

9 Monitoring

9.1 Monolith

9.2 Microservices Architecture

10 Logging

10.1 Monolith

10.2 Microservices Architecture

11 Fault Tolerance

11.1 Monolith

11.2 Microservices Architecture

12 Communication

As already discussed in an MA the service components can communicate using events, procedure calls or other methods available within a single server machine. Usually all this communication stays within a single computer and thus does not necessarily compromise

confidentiality.

Microservices can not trust any of the (Otterstad and Yarygina, 2017)

In MSA single services communicate via a network. TODO

Next messaging systems list is from (Yarygina, 2018): lightweight - REST API, Sync RPC, GraphQl - Async REST, gRPC - Apache Kafka, ZeroMQ - Java Message Service: 1 ActiveMQ, 2 JBOSS messaging, 3 Glassfish - AMQP: 1 RabbitMQ, 2 Qpid, 3 HornetQ - MuleESB, Apache ServiceMix, JBossESB - heavyweight WebSocket

12.1 Representational State Transfer (REST)

Fielding (2000) presented REST in 2000 and it has become very successfull. The architectural style is was derived using various constraints one of which is the demand of stateless communication. The communication i.e. the request must contain all information for the server to fullfil the request. All session state is stored in the client of which the server has no prior knowledge before a request.

In her doctoral thesis Yarygina (2018) critiques the REST paradigm from the security perspective. She states that the design of the architecture does not meet the security requirements for web applications. The statelessness of REST does not allow for any server side sessions and thus making e.g. token repudiation impossible due to not being able to verify tokens other than the correct issuer by signature and the validity. As such tokens are more compatible with REST but there still has to be the private keys in the server for signature verification.

12.2 Event-Driven Communication

12.3 Coping With Failure in Communication

Montesi and Weber (2016) present widely used design pattern for MSA. The Circuit Breaker can be used to mitigate the very likely case that a microservice operates slower than the other services calling it and runs out ot resources to fulfill the requests in time. The circuit breaker is either implemented in the microservices or as a proxy between the client and the microservice. When the microservice does not service requests as intended the circuit breaker is to trip and send a failure message to the clients immediately when requests are received thus allowing the microservice time to service the prior responses.

The circuit breakers can prevent an application becoming completely unresponsive and crashing when a denial of service attack is carried out on the service.

13 Defence in depth

Jander et al. (2018) propose a solution for secure communication in MSA even in multicloud solutions. perimeter defence -> neglect security of individual microservices.

14 Comments

authentication, credential

authorization, access control, policy decision point (PDP), policy enforcement point (PEP), A Framework for Policy-based Admission Control https://tools.ietf.org/html/rfc2753

15 Other MSA specific security matters

15.1 Platforms

Docker Swarm Kubernetes (K8s) Azure

sandbox virtualization

15.2 Monitoring and logging

15.3 Software Development

15.4 Deployment and Operation

Developing software using the MA the structure the whole application or service is usually deployed as a whole and the program code can be compiled, tested and used as a single unit or multiple modules. In contrast to this a service implemented by using a MSA can be deployed in single microservice units and thus a single service can be worked upon individually and deployed once ready.

The immediacy in the deployment of the microservices entail a very specific security risk. In a paper Ahmadvand et al. (2018) present threats from malicious insiders working on the services as developers or other positions with access to sensitive information. In microservice development the finished implementations are to be immediately released to production. There are few steps in the CD pipeline prior to this but once tests pass in the test environments the pipeline is supposed to publish the changes to the actual production environment. The paper presents four specific threats. The first one is that

the knowledge of sensitive information is spread among the developers more widely than in MA. The developers need access to be able to produce working solutions. The second threat is that the insiders monitoring and operating the running system intentionally harm the system by making malicious changes. The third threat is the developers knowing the configurations and their ability to make almost instat changes to them or the microservices them selves. The last presented threat in the paper is the non-repudiation. The system is not able to dis-allow malicious requests when the developers have had access to the keys and other configurations. They can effectively implement services or requests that emit malicious requests or responds.

Malicious attempts in a MA are more easily screened by performing security audits and by peer reviewing the code. In a MSA the knowledge of a single service and it's inner workings are shared by a more limited number of people. Finding the compromised actions from the interoperability of the distinct microservices is a daunting task.

15.5 Service discovery

Service discovery as presented in Montesi and Weber (2016) is a design pattern in which a registry is kept on currently running microservices. The microservices register them selves to the service discovery registry. This registry is used by either a router to route client service calls to running microservices or by the client directly.

https://www.nginx.com/blog/service-discovery-in-a-microservices-architecture/
https://www.consul.io

15.6 Externalized configuration

To allow for easy configuration change management there should exist a configuration orchestration service. This service should have an API from which services in their startup can load their appropriate configuration. The configuration of the whole system can be easily maintained through the API.

The contents of the configuration is highly sensitive information. It consists of addressess, credentials and other information that alter the behaviour of the system. Therefore, the content must be stored safely and not allowed to be read or altered by unauthorized users.

16 Conclusion

This paper discussed the security aspects of changing the architecture from MA to MSA.

In MSA there are more things to go wrong than in MA. The deployment necetitates

installing: virtualization, monitoring, and a plethora of other tools. In some cases these tools might not even exist and they have to implemented by inhouse developers and thus more costs are incurred upfront and also in the upkeep of the system. In addition to being more costly own development has higher risks involved.

MSA has higher complexity due to more tools needed and having more potentially exposed attack surface. Security can be though of as being as good as it's weakest link. In general a MSA deployment has multiple layers which all have to be consistent and correct. One example being the configurations of a system from the operating system on the server running the virtualization environment. All of the layers from the server hardware to the handling of errors in the actual code have to be of ample quality to mitigate a failure in security.

Communication from inprocess to networking -> completely different ball game. Security in depth imperative. Zero trust.

Security has to be taken into account right from the beginning of the project to change the architecture. The choices made in the development of the web service when following a MA do not carry to the MSA as such.

Future research...

The research carried out...

References

Mohsen Ahmadvand, Alexander Pretschner, Keith Ball and Daniel Eyring. Integrity protection against insiders in microservice-based infrastructures: From threats to a security framework. *Software Technologies: Applications and Foundations*, 2018.

Roy Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. Ph.D. thesis, University of California, Irvine, 2000.

M. Fowler and J. Lewis. Microservices - a definition of this new architectural term, 2014. Available `https://martinfowler.com/articles/microservices.html`. Viewed 15.2.2020.

H. Hammouchi, O. Cherqi, G. Mezzour, M. Ghogho and ME. Koutbi. Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, 151(99):1004–1009, December 2019.

T. Hunt. ';– have i been pwned ?, 2020. Available `https://haveibeenpwned.com`. Viewed 8.2.2020.

K. Jander, L. Braubach and A. Pokahr. Defense-in-depth and role authentication for microservice systems. *Procedia Computer Science*, 130(1):456–463, December 2018.

M. Jones, J. Bradley and N. Sakimura. Json web signature (jws). RFC 7515, RFC Editor, May 2015a. URL `http://www.rfc-editor.org/rfc/rfc7515.txt`. `http://www.rfc-editor.org/rfc/rfc7515.txt`.

M. Jones, J. Bradley and N. Sakimura. Json web token (jwt). RFC 7519, RFC Editor, May 2015b. URL `http://www.rfc-editor.org/rfc/rfc7519.txt`. `http://www.rfc-editor.org/rfc/rfc7519.txt`.

Miika Kalske, Niko Mäkitalo and Tommi Mikkonen. Challenges when moving from monolith to microservice architecture. *Current Trends in Web Engineering*, Irene Garrigós and Manuel Wimmer, editors, pages 32–47, Cham, 2018. Springer International Publishing. ISBN 978-3-319-74433-9.

Tim McLean. Critical vulnerabilities in JSON Web Token libraries, 2015. Available `https://auth0.com/blog/critical-vulnerabilities-in-json-web-token-libraries/`. Viewed 15.3.2020.

Fabrizio Montesi and Janine Weber. Circuit breakers, discovery, and API gateways in microservices. *CoRR*, abs/1609.05830, 2016. URL `http://arxiv.org/abs/1609.05830`.

S. Newman. *Monolith to Microservices. Evolutionary patterns to transform your monolith.* O'Reilly Media, Inc., 2019. ISBN 9781492047841. 1st edition.

Christian Otterstad and Tetiana Yarygina. Low-Level Exploitation Mitigation by Diverse Microservices. *6th European Conference on Service-Oriented and Cloud Computing (ESOCC)*, Flavio De Paoli, Stefan Schulte and Einar Broch Johnsen, editors, volume LNCS-10465 of *Service-Oriented and Cloud Computing*, pages 49–56, Oslo, Norway, September 2017. Springer International Publishing. doi: 10.1007/978-3-319-67262-5_4. URL `https://hal.inria.fr/hal-01677618`. Part 2: Microservices and Containers.

Daniel Richter, Tim Neumann and Andreas Polze. Security considerations for microservice architectures. pages 608–615, 01 2018. doi: 10.5220/0006791006080615.

Stack Overflow. Stack Overflow Developer Survey Results 2019. Available `https://insights.stackoverflow.com/survey/2019`. Viewed 1.2.2020.

T. Yarygina. Overcoming security challenges in microservice architectures. *Proceedings - 12th IEEE International Symposium on Service-Oriented System Engineering, SOSE 2018 and 9th International Workshop on Joint Cloud Computing, JCC 2018*, 2018.

M. Zari, H. Saiedian and M. Naeems. Understanding and reducing web delays. *in Computer*, 34(12):30–37, December 2001.