Cybersecurity Measures within Microservice Applications

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Wen Ip

Spring, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

STS Research Paper

Introduction and Background

At my summer internship, I remember first hearing about the term “microservice architecture”. The company I was working with was looking into reorganizing the structure of their architecture, especially since the company was switching over to cloud platforms as many cloud technologies have been growingly popular. Over the course of ten weeks, I worked on an application for a large banking company on a five-person development team to create a microservice based application. We had many mentors that were enthusiastic to introduce this microservice architecture concept and the benefits of adopting the architecture. They described a concept of a microservice architecture as having different Lego pieces that represent components that have different functionality. Multiple and individual components can be used to build an application. These microservice applications can be customized easily to fit each of their needs by accessing the necessary component without having to recreate it within the application again.

Software development techniques and processes have evolved to deliver high quality software solutions. These solutions have become more complex with larger architectural designs to expand functionality and scalability. Architecture is an important element to consider when developing a software application. It is the backbone of every software application and determines how the application is developed and maintained by engineers. The architecture style of building a software application determines its scalability, resilience, and business functionality. It is important to determine the architectural design of the software product to fit its needs and purpose. Through architectural reviews, companies found value in incorporating architecture in the company’s software development methods (Maranzano et al., 2005). One of the problems that these companies experience is that projects fail or end up needing significant rework past their original schedules, which is why it is important to research these systems and architectures.

With increases in features of an application, the appropriate software metrics, and architecture must be determined (Milić & Makajić-Nikolić, 2022). Microservices is a new approach to how an application is structured and built. Microservice architecture revolves around the idea that self-contained components of functionality make up a larger system (O' Connor et al, 2017). It allows for an application to be built upon a collection of individual services that can be arranged, organized, and maintained into multiple applications. However, these microservice systems have more unknown security issues and vulnerabilities that are not fully understood or mitigated effectively.

Microservices are an example of how novelty in application development is prioritized over cybersecurity. The literature review will cover how cybersecurity will be impacted by the implementation of microservices. I will look at case studies and analyze how effective these microservice implementations are for security and application needs. I will find which implementations are best for the appropriate applications and how cybersecurity should be prioritized during the application development process. From these findings implementation methods can be recommended and the paper will be able to recognize and address security concerns for microservices and applications.

Literature Review

With the growing use of microservices, the potential of implementing microservice architecture transforms the way companies utilize cloud technology, as well (Ünlu et al., 2022). With the emerging popularity of cloud technology, microservice architecture has been paired with cloud computing technology as cloud services are transitioning into microservices for development and deployment (Wen et al., 2022). An example of microservices being implemented with cloud technology is that the cloud services used to help manage input/output data are produced by microservices within different data containers (Barron et al., 2022). With the use of automation on cloud platforms, microservices can be deployed and scaled quickly. Each microservice serves as a business need or functionality, meaning an application can easily be altered by choosing to include a microservice or not. Microservice architecture allows for technology to achieve scalability and high level of availability (Heidari et al., 2022). Applications with microservice architecture can handle a higher workload and deploy faster with this architecture. Implementing microservices also avoids duplications of objects, and reduced time to search and create them from their registers (Jarwar et al., 2018).

While microservices are a new architectural method for applications, there are drawbacks and unknown vulnerabilities to microservices. Microservices governance has concerns for application stability and arose new problems, such as load balancing, fault detection, and autoscaling (Wang et al., 2022). Implementing microservices increased management complexity and posed a challenge for the standardization of microservices across teams.

Another concern for microservices are its unknown vulnerabilities that serve as a potential security threat to sensor networks (Ying et al., 2022). Since microservices are being paired with cloud technology, security becomes a big concern and users' data are at risk with implementing microservices. Cybersecurity is not only a concern for the company developing the application, but also users that use the application want their data protected as well. Cybersecurity has the responsibility in computing and information technology to protect organization information from various malicious attacks and vulnerabilities (Hijji et al., 2022).

The goal of cybersecurity is to protect against attacks and prevent attacks from gaining advantage of the systems for malicious activity, such as preventing access to information or exposing private information to the public. Cybersecurity is a growing concern because cybercrimes have been continuously growing with an estimate that it will increase 15% every year for the next five years (Freeze, 2021). With growing trends of cybercrime, strong cybersecurity implementations have become a more important user value for applications. When adopting microservices into applications as a novice application architecture, cybersecurity is affected by this development decision and cybersecurity of microservice applications should be a concern of interest.

A more efficient strategy for managing and standardizing microservices should be explored to maximize the potential of microservices in applications. From this study, the drawbacks, and advantages of microservices will be discussed and will be used to recommend potential implementation methods for microservices that will improve applications. Specifically, web applications, such as complex mobile and IoT applications, have been switching over from monolithic to microservices (Guo et al., 2022).

Understanding design of infrastructure can help with software development implementations, such as scaling up an application or managing large quantities of data. I will argue that microservices affect the way the company structure and the ability to develop these applications for users. According to Star (1999), understanding infrastructure design can help with software development implementations, such as scaling up an application or managing large quantities of data. Star (1999) also mentions that studying infrastructure can be boring and may be time consuming. However, it can reveal hidden processes that impact the development and functionality of a system, or in this case, a software application. With understanding infrastructure, it means there is a better grasp on the functionality of the application so developers can make more informed decisions as they develop and build the application.

Applications created by engineers are impactful to users and the relationship between engineers and the user is important. I will show that engineers must understand their relationship with users to make decisions on what to value more in an application. In an 18- month participant observation study at a medium sized company, it highlighted that "the technology is the machine's relations with its users" (Woolgar, 1990). Engineers understand the machine and users have a relationship to the machine where they are pushed to use the application in a certain way, but unexpected uses may come out of this. Pereira et al. (2013) defines the term "social software" as the determinant of transformations that are changing the way people relate to digital technology, and he suggests that we live in a world where social software is in all aspects of people's lives. Our relationship with technology is affected by emotions, sociability, and new values we hold like security and performance.

Cybersecurity measures may clash with ethical values of users, engineers, and stakeholders. Cybersecurity values have increasing importance as digital technologies are more and more embedded into our daily lives. If cybersecurity measures are not considered then, it can damage the trust with users and hurt the economy and society (Domingo-Ferrer & Blanco-Justicia, 2020). From this study, they found that the main values around cyber security, such as security, privacy, fairness and autonomy, conflict with one another. With the relationship between engineers and users, this is important for engineers to recognize and consider as they build their application to fit users' needs. From a different perspective, another study highlighted the relationship between investments in security and vulnerability and found that companies must keep investing in security for continuous unknown threats while vulnerabilities continue to arise and evolve (Mazzoccoli, 2022). Stakeholders seek to minimize expense of security measures that optimally mitigate growing vulnerabilities. The value of different users, engineers and stakeholders' conflict within cybersecurity concerns and ultimately becomes the responsibility of the engineer to determine what to prioritize.

Methods

I research case studies of existing implementations of microservices and compare the effectiveness of these different implementations. Looking at multiple case studies and environments can help pinpoint the pros and cons of microservices and how appropriate it may be for certain situations. While looking at the pros and cons of these case studies, I focus on the security of microservice applications since there is a lack of research on this due to the recent adoption of this architecture. I will get my sources from journals about case studies for companies. In my review of this evidence, I will examine case studies of microservice application implementations.

Analysis of Case Studies

Different implementations of microservices were analyzed through case studies of microservices. The case studies review the choices behind implementing microservice architecture, which has an impact on the security of the application. Through this case analysis, I will show how application security is negatively affected by microservice architecture and why the utilization of microservices is prioritized over its drawbacks through a socio-technical lens.

With the growing popularity of microservices since 2015, there is desire for technology companies to follow what the bigger technology companies are doing with microservices, due to their public success with the technology. A reason why those companies look to follow these big tech companies is because their success was praised and accounted for because of them switching to microservices. Amazon, LinkedIn, Netflix, SoundCloud, Uber, and Version are notable companies that set an example for implementing microservices (Ünlu et al., 2022). Amazon took their own initiative for microservices by presenting the approach that teams are responsible for the full development of a service, which became an integral part in how microservices are currently used (Dragoni et al., 2017). The movement to migrate to microservice architecture is also contributed by the growth and scale of Netflix after breaking up their monolith architecture into microservices (Thönes, 2015). Many companies have followed the steps of these big companies where they were able to build software using this approach and grow their company to a well-known success.

However, even though these companies have had success with microservices, the path to safe microservices was not completely smooth and there are still many issues microservices have including security concerns. With the hype of microservices, there is a lack of emphasis on the security issues of microservices over other benefits, such as business focused factors. One of the factors is the costs of using microservices on cloud platforms are lower, where the microservice only needs to be run on-demand and it costs less to run these services (Tallman, 2021). With these lower costs, companies that use microservices can allocate costs elsewhere to expand their business. Other factors that are being highlighted are being able to expand their company more efficiently since the microservice system is a representation of the organization's communication structure (Killalea, 2016). By bringing in this system that mimics the separation of business priorities better, business managers and engineers are forced to look at trust in a different way by allowing each service to govern on their own through autonomy and accountability. This type of system fosters more effective communication and allows the organization to scale up further. The factor of having market goals, such as being able to lower costs and expand business, has more priority than the security issues of user data.

Microservice enables failure in its design and companies are okay with designing into the inevitable failure, but at the detriment of users and their data through security vulnerabilities. These systems allow engineers to practice “permissionless innovation”, which is the ability to innovate things that are against the communication constructs in place (Killalea, 2016). This has fueled many of the innovations of the internet and a higher risk of experimentation. This is supported by implementation of microservice and management around it because services within a microservices can easily be scaled up or deprecated as wished. The combination of having more autonomy and accountability between services and embracing failure of services can result in compromising whole microservice systems. Netflix is an example of how their entire microservice application was compromised because the malicious hacker was able to access any subdomain of netflix.com by tampering with one of subdomains, gaining access to Netflix subscribers and their data (Dragoni et al., 2017). This approach may be an efficient approach for innovation, but it allows for higher risk of the company and at the expense of user’s safety.

From these case studies, it is apparent that microservice architectures have tons of application benefits and market driving factors but have security issues that come with having this type of distributed system. The case studies also help identify other reasons that are favored over security issues, even though these security issues lead to a significant impact on user’s safety of data and other potential malicious attacks. Considering Woolgar’s Configuring the User framework, microservices are seen to satisfy many business needs and overcome technical obstacles, but it is not fully recognized for its impact on security of these applications, which have detrimental impact on users' safety (Woolgar, 1990). Engineers and business leaders must investigate good implementation strategies and innovative approaches to microservices that consider user's safety.

Conclusion

There is a growing concern for how user data is collected and protected. When new technologies are quickly adopted, there are many unknown security risks that must be addressed. Microservice architecture implementations must consider security concerns and application development, especially since the adoption of this technology is relatively new to the industry. By looking at these case studies, there are many different things to consider when moving on. One of them is to think about whether the fast adoption of microservices with the "permissionless innovation" approach is more beneficial or harmful to the development and use of the technology we create. The way that microservices have been rapidly popularized may have similarities with how we treat other types of new technologies, and it may be worth looking further into the adoption of other recent popular technology. Another thing to consider is how security is seen as an afterthought for technology under business needs and it would be useful to continue researching how to improve application security and why there are hurdles for companies to take initiative to implement security measures.

From this paper, engineers can find appropriate implementations for the application they develop, whether that decision includes using microservice architecture or not. Further research can be done on a wider variety of microservice applications with different functionalities. Researchers should also continue to monitor and analyze case studies of microservice adoption. Microservices can be seen as a promising architecture for cloud technologies and with the right tools and environment, it can be further enhanced to improve application development and user experience.

References

Barron, A., Sanchez-Gallegos, D. D., Carrizales-Espinoza, D., Gonzalez-Compean, J. L., & Morales-Sandoval, M. (2022). On the Efficient Delivery and Storage of IoT Data in Edge–Fog–Cloud Environments. *Sensors* (14248220), 22(18), 7016–N.PAG. https://doi.org/10.3390/s22187016

Domingo-Ferrer, J., & Blanco-Justicia, A. (2020). Ethical Value-Centric Cybersecurity: A Methodology Based on a Value Graph. *Science & Engineering Ethics*, 26(3), 1267–1285. https://doi.org/10.1007/s11948-019-00138-8

Dragoni, N., Giallorenzo, S., Lafuente, A., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: Yesterday, Today, and Tomorrow. *Present and Ulterior Software Engineering*, 195-216. https://doi.org/10.1007/978-3-319-67425-4_12

Freeze, D. (2021, April 27). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. Retrieved April 5, 2023, from https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Guo, F., Tang, B., & Tang, M. (2022). Joint optimization of delay and cost for microservice composition in mobile edge computing. *World Wide Web*, 25(5), 2019–2047. https://doi-org/10.1007/s11280-022-01017-2

Heidari, S. M., & Paznikov, A. A. (2022). Multipurpose Cloud-Based Compiler Based on Microservice Architecture and Container Orchestration. *Symmetry* (20738994), 14(9), 1818–N.PAG. https://doi.org/10.3390/sym14091818

Hijji, M., & Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors* (14248220), 22(22), 8663. https://doi.org/10.3390/s22228663

Jarwar, M. A., Kibria, M. G., Ali, S., & Chong, I. (2018). Microservices in Web Objects Enabled IoT Environment for Enhancing Reusability. *Sensors* (14248220), 18(2), 352. https://doi.org/10.3390/s18020352

Killalea, T. (2016). The Hidden Dividends of Microservices. *Communications of the ACM*,

59(8), 42–45. https://doi-org/10.1145/2948985

Maranzano, J. F., Rozsypal, S. A., Zimmerman, G. H., Warnken, G. W., Wirth, P. E., & Weiss, D. M. (2005). Architecture Reviews: Practice and Experience. *IEEE Software*, 22(2), 34–43. https://doi.org/10.1109/MS.2005.28

Mazzoccoli, A., & Naldi, M. (2022). Optimizing Cybersecurity Investments over Time.

Algorithms, 15(6), 211. https://doi.org/10.3390/a15060211

Milić, M., & Makajić-Nikolić, D. (2022). Development of a Quality-Based Model for Software Architecture Optimization: A Case Study of Monolith and Microservice Architectures. *Symmetry* (20738994), 14(9), 1824–N.PAG. https://doi.org/10.3390/sym14091824

O'Connor, R. V., Elger, P., & Clarke, P. M. (2017). Continuous software engineering-A microservices architecture perspective. *Journal of Software: Evolution & Process*, 29(11), n/a-N.PAG. https://doi.org/10.1002/smr.1866

Pereira, R., Baranauskas, M. C. C., & da Silva, S. R. P. (2013). Social Software and Educational Technology: Informal, Formal and Technical Values. *Journal of Educational Technology & Society*, 16(1), 4–14.

Star, S. L. (1999). The Ethnography of Infrastructure. American Behavioral Scientist, 43(3), 377.

https://doi.org/10.1177/00027649921955326

Tallman, N. (2021). A 21st Century Technical Infrastructure for Digital Preservation. *Information*

Technology & Libraries, 40(4), 1–20. https://doi-org.proxy1.library.virginia.edu/10.6017/ital.v40i4.13355

Thönes J, Microservices, IEEE Softw, 2015, 32, 1, 116, 116, 10.1109/MS.2015.11

Wang, L., Jiang, Y. X., Wang, Z., Huo, Q. E., Dai, J., Xie, S. L., Li, R., Feng, M. T., Xu, Y. S., & Jiang, Z. P. (2022). The operation and maintenance governance of microservices architecture systems: A systematic literature review. *Journal of Software: Evolution & Process*, https://doi-org.proxy1.library.virginia.edu/10.1002/smr.2433

Woolgar, S. (1990). Configuring the user: the case of usability trials. *Sociological Review*, 38(1),

58–99. https://doi.org/10.1111/j.1467-954X.1990.tb03349.x

Wen, Y., Cheng, G., Deng, S., & Yin, J. (2022). Characterizing and synthesizing the workflow structure of microservices in ByteDance Cloud. Journal of Software: Evolution & Process, 34(8), 1–18. https://doi-org.proxy1.library.virginia.edu/10.1002/smr.2467

Ying, F., Zhao, S., & Deng, H. (2022). Microservice Security Framework for IoT by Mimic

Defense Mechanism. *Sensors* (14248220), 22(6), 2418.

https://doi.org/10.3390/s22062418