FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

Hello

Subtitle

Bachelor Thesis

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science in Engineering

to the University of Applied Sciences FH Campus Wien
Bachelor Degree Program: Computer Science and Digital Communications

Author:

first name surname

Student identification number:

Number

Supervisor:

Title first name surname

Date:

dd.mm.yyyy

Declaration of authorship:

I declare that this thesis is my own work and that I did not use any aids other than those indicated or any other unauthorized help (e.g., ChatGPT or similar artificial intelligence-based programs). I certify that this work does not contain any personal data, and that I have clarified any copyright, license or image-law issues pertaining to the electronic publication of this thesis. Otherwise, I will indemnify and hold harmless the FH Campus Wien from any claims for compensation by third parties. I certify that I have not submitted this thesis (to an assessor for review) in Austria or abroad in any form as an examination paper. I further certify that the (printed and electronic) copies I have submitted are identical.

Date: Signature:

Abstract

(E.g. “This thesis investigates...”)

Kurzfassung

(Z.B. “Diese Arbeit untersucht...”)

List of Abbreviations

IoT	Internet of Things
IT	Information Technology
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
ZT	Zero Trust

Key Terms

Kubernetes

Cloud

Zero Trust

Least Privilege

Access Control

Contents

1 Introduction

Over the last years, there have been two significant shifts in enterprise IT systems.

One of these shifts addresses the way companies deploy, scale and maintain the lifecycle of their software services. Applications used to be primarily constructed as one large software unit that bundled all features, business logic, user interfaces and data access components. Increasing necessity for scalability, flexibility and maintainability made organizations transition from such monolithic architectures to microservices, which are smaller, separated but loosely coupled software units implementing one component of the larger system at hand. The release of the Docker container platform in 2013 had a significant impact on making transitions from monoliths to microservices feasible. Kubernetes has since emerged as the go-to choice for managing containerized applications at scale, particularly in cloud-native environments. Its ability to automate tasks, scale applications, and support a wide range of use cases makes it a powerful tool for both large enterprises and small teams.

The second shift pertains to how companies secure their computing infrastructure and the resource hosted on it. While there used to be single, easily identifiable network perimeters in the past, for example a single local area network at a company site, modern infrastructures may consist of multiple internal networks, remote offices, mobile workers, different types of virtualization and cloud services. This circumstance has rendered traditional, static, perimeter-based security no longer appropriate, because transgressing this perimeter once means further, unhindered access into a given system. Under a newer security model labeled "Zero Trust", the aim is to restrict such unhindered movement as much as possible by adhering to certain principles and guidelines, one of them being to never grant implicit trust to any actor on the network - hence the term "Zero" Trust. One fundamental piece of liteature on this topic is the NIST Special Publication 800-207, titled "Zero Trust Architecture", which put the term "Zero Trust" on the map research still fresh

Even though the principles of ZT have existed way before the term "Zero Trust" was coined but two fundamental pieces of literature on this topic

1.1 Sub-chapter 1

1.1.1 Under sub-chapter 11

1.1.2 Under sub-chapter 12

2 Chapter 2

2.1 Sub-chapter 21

2.2 Sub-chapter 23

3 Related Work

Since the emergence and popularization of the concept of "Zero-Trust", a lot of work has been done on the topic, tying it into various domains of IT: Cloud, on-premise infrastructure, IoT, Hardware, Blockchain and much more. Andrea Manzato, at the University of Padua, implements the Zero Trust model in an enterprise environement using solutions provided by Microsoft Azure. It is investigated how the capabilities and configuration options of Microsoft Defender and Active Directory can be leveraged to protect enterprise resources. Attack scenarios on these technologies are simulated and automated remediation actions are presented. The combination of Cloud and Zero Trust is heavily Dr. Wesam Almobaideen's master thesis, at Rochester Institute of Technology Dubai Campus, explores the topic of Zero-Trust specifically in the context of MFA. A framework combining principles of ZT and MFA is designed and evaluated in terms of performance, security and user satisfaction.

In the context of IoT, Cem Bicer at the technical university of Vienna, explores and evaluates ZT for edge networks. The implementation of the thesis follows ZT guidelines as proposed by the National Institute of Standards and Technology (NIST) and additionally places a blockchain network on top of the ZT architecture.

Kang et. al present a survey

Furthermore, zero trust in and of itself has been put under scrutiny. In "Theory and Application of Zero Trust Security: A Brief Survey", Kang et. al investigates the current challenges faced when making use of Zero Trust, as well as progress that has been achieved so far when doing so.

It must be noted that research and knowledge on the theory and application of Zero Trust has not yet matured, and more extensive work is still required to obtain a deeper understanding and more accurate implementation of the paradigm in academia and industry.

In his master's thesis at Utrecht university, Michel Modderkolk proposes a more mature model of Zero Trust, outlining

On Kubernetes security: -DESIGNING AN INTRUSION DETECTION SYSTEM FOR A KUBERNETES CLUSTER -ENHANCING CLOUD SECURITY AND PRIVACY WITH ZERO- KNOWLEDGE ENCRYPTION AND VULNERABILITY ASSESSMENT IN KUBERNETES DEPLOYMENTS -A Systematic evaluation of CVEs and mitigation strategies for a Kubernetes stack -My previous work? -Kubernetes Near Real-Time Monitoring and Secure Network Architectures -A security framework for multi-cluster Kubernetes architectures -Testing the Security of a Kubernetes Cluster in a Production Environment -Study of Security Issues in Kubernetes (K8s) Architectures; Tradeoffs and Opportunities

put this in objectives and methodology:

Lack of research on Zero Trust AND Kubernetes , how can zero trust principles be applied to kubernetes? There is no research done on Zero Trust specifically in the context of Kubernetes. The goal of this paper is to do exactly that: investigate how zero trust can be achieved in a Kubernetes setup.

The boundaries are the following

It is a self-managed Cluster (self managed control plane), instantiated by kubeadm or k3s, not a managed cluster like EKS, AKS, and GKE Free or opensource (or both) technolgies are used to

Free versions of otherwise paid-services are used A side goal is to do so with least possible vendor lock-in.

Use Ansible to have a replicable setup. 3 node cluster: 1 master, 2 worker nodes.

To formulate the goals outlined above, the single, coherent research question for this thesis is the following:

How can open-source..... be leveraged to achieve Zero Trust in Kubernetes? (from berhard mail)

technologies shall be presented to implement principles, one final technology shall be chosen, others might get explanation

also create dummy applications that must first fetch token from keycloak to then access another service in another namespace which is then protected by Istio AuthorizationPolicy and RequestAuthentication

4 Conclusion

5 Future work

Bibliography

List of Figures

List of Tables

Appendix

(Hier können Schaltpläne, Programme usw. eingefügt werden.)