DOCKER IMAGE SECURITY FOR DEVSECOPS

RESEARCH PROPOSAL

M.Sc IN INFORMATION TECHNOLOGY (CYBER SECURITY)

FACULTY OF GRADUATE STUDIES & RESEARCH

SUBMITTED BY
CSK Pathirana (MS21909078)

Feb 2021

LECTURER
Dr. Lakmal Rupasinghe

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

PROBLEM DEFINITION

1. Docker containers are private registry servers which wrap a piece of software in a complete file system that contains everything it needs to run: code, runtime, system tools, system libraries and anything that can install on a server, regardless of the environment it is running in.

2. Many organizations deploy private registry servers in their internal/external application development/deployment environment. Although Dockers are considered the standardized method for micro-services deployment, playing an important role in cloud computing emerging fields such as service meshes, it is understood that container security is the main concern and adoption barrier for many companies.

AIM OF THE RESEARCH

3. The aim of this project is to survey on container security and solutions which will help to understand container security requirements and obtain a clearer picture of possible vulnerabilities and attacks.

SCOPE OF THE RESEARCH

4. I have identified that the research should cover and not limited to the undermentioned points related to security requirements within the host-container threat landscape.

a. Protecting a container from applications inside it.
b. Inter-container protection.
c. Protecting the host from containers.
d. Protecting containers from a malicious or semi-honest host.

METHODOLOGY

5. This research will be carried out in three phases as depicted below in order to propose with the suitable security measures for Docker Image Security.

a. Survey the available literature on container security
b. Analyze the threat perception
c. Find solutions for identified threat perception

CONCLUSION

6. Containers are important for the future of cloud computing. Micro-services and containers are closely related, where containers are considered the standardized way for micro-service

deployment. Containers are important for the emerging field of service meshes that relies on micro-services, too.

7. However, one of the primary adoption barriers to container widespread deployment is the security issues they face. Therefor this research work is attempted to fill this gap by looking at the literature and identifying the main threats which are due to image, registry, orchestration, container, side channels, and host OS risks.