CSCE689 Project 2 Proposal - Container Safety Determination

Qingqing Li, Shijin Tang, Mian Qin

1 Objectives

Our project aims to provide a cloud service to verify the security for docker development, preventing malicious code compromising the infrastructures. The safety scan contains two parts, first, we will check the docker image uploaded by the developer in the private registry. Second, we will scan the running docker containers in the production development. Thus to make sure the security of the docker development and deployment.

2 Background and motivation

Docker greatly simplifies the deployment and management of application. For example, to deploy an application consisting of a set of services one pulls corresponding docker images from a registry and wires them together.

However, there are plenty of security vulnerability across the development stacks. During the development, the developers may pull images which contains malicious code or the developers themselves maybe compromised to intentionally inject malicious code to the application. Besides, during the deployment of docker containers in the production environment. The docker image may get attacked, for example due to the security vulnerability of the production environment. In this project, we propose a solution to address these problems.

3 Methodology

In this project, we propose to build a prototype software to demonstrate our approach. The software mainly contains three parts:

1. A background crawler that pull the docker images that are pushed to the private registry.
2. A docker image scanner to determine whether the image is malicious or not. To determine if the given images are malicious or not, we intend to compare the suspicious images with the Reference Data Set (RDS) collected by National Software Reference Library (NSRL). The RDS incorporates application hash values in the hashset which may be considered malicious, i.e. steganography tools and hacking scripts.
3. A background scanner to scan the running docker containers in the production environment. We intend to implement scanning scheduling, while use 3rd party tools for container scan.

4 Expected outcome

The basic software we expect to implement contains the above docker image scan and docker container scan. Further, we may focus on the performance optimization for large scale system or we may consider more security vulnerabilities for docker development and deployment and implement approach to tackle them.

Reference

- https://okrieg.github.io/EC500/PROJECTS/2016/sastry.html
- https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl
- http://roussev.net/sdhash/sdhash.html