Security of Docker containers

Report for the Computer Security exam at the Politecnico di Torino

Carmine D'Amico (239540)
tutor: Antonio Lioy

July 2018

Contents

1 Introduction

Explain here why the XYZ protocol is important and what was the purpose of the present work.

If you want to reference a web site you can do like this: http://www.polito.it.

2 State of the art

In computer science, the term *virtualisation* is referred to the creation of virtual computational resources. These resources, normally supplied as hardware, are provided instead to the user by the operating system through the creation of a new abstraction layer. OSs, storage devices or network resources could all be virtualised. Virtualisation can be obtained at different levels and using different techniques.

Virtual machines have represented for many years the state of the art of the virtualisation, being used in both consumer and enterprise contexts. In the last years a new technology, based on *containers*, has started to gain more attention, thanks to its benefits. Docker is an open source container technology, stepped into the limelight thanks to its simple interface, which allows to create and control containers.

2.1 From virtual machines...

With the term virtual machines it is often intended an *hypervisor*-based virtualisation, that is a type of virtualisation that acts at hardware level. Virtual machines (VMs) are established on top of the host operating system, providing applications with their dependencies, but also an entire guest OS and a separate kernel. One or more virtual machines can be run on the same machine. Hypervisors are distinguished in two different types, the one that works directly on top of the host's hardware (**bare metal hypervisor**) and the one that is on top host's OS (**hosted hypervisor**).

Bare metal hypervisor provides better performances, not having the overhead of the extra layer of the host's operating system. It manages directly hardware and the guest's operating system. On the contrary hosted hypervisor can be manged in an easier way, running as a normal computer program on the user's operating system.

As said before, the hypervisor needs to run on the user's computer, which is defined as *host machine*, while each virtual machines is called *guest machine*. It is important to remember this terminology, because it will be used also in the following, referring to containers.

2.2 ...to containers

2.3 Docker

2.3.1 History

2.3.2 Implementation

3 Hardening Docker

References

[1] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, A. Lioy, "Impact of vehicular communication security on transportation safety", MOVE 2008: IEEE INFOCOM-2008 workshop on Mobile Networking for Vehicular Environments, Phoenix (AZ, USA), April 13-18, 2008, pp. 1-6

[2] W. Diffie, M.E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, pp. 644–654

[3] R. Shirey, RFC-4949 "Internet Security Glossary, Version 2", August 2007