Moving Target Defense Security

Being a Cyber Chameleon to Eliminate Asymmetric Advantages of Cyber Attackers

Introduction

A New Paradigm

Moving Target Defense (MTD) is considered today to be the most effective innovation in the field of cyber security.

Until now, IT infrastructures were regarded as unchangeable and stationary. A great deal of effort has been invested in protecting these infrastructures by identifying, preventing and eliminating threats. MTD is a completely new paradigm in the arena. MTD creates a dynamic attack surface for moving targets, thus creating asymmetric disadvantages for the attacker. The playing field between defender and attacker becomes more even.

A possible implementation of MTD is done by using Software Defined Networking. As described by Cyel, this continuously changes the attack interface. Attackers will find it difficult to identify and track targets in the first place as their targets seem to hop around in the colosseum.

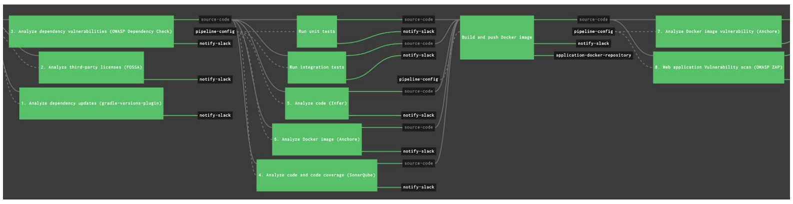
This white paper can be seen as the starting point of MTD for Traversals' Data Fusion Platform. The ideas described herein will be constantly further developed to increase the cyber security of Traversals' solutions.

Technical Overview

Secure Software Supply Chain

In Secure Software Supply Chain, Traversals described its new CI/CD tool for secure artifact creation and deployment. This pipeline helps us to address security issues, prevent license violations and to keep dependencies up to date with lowest efforts.

Every commit to the version control system results in triggering the CI/CD pipeline and finally in a new deployment unit of the affected application. The time between commit and final deployment is currently about 30 minutes. If necessary, the time can be reduced by deactivating time-consuming checks.



A block diagram showing an exemplary pipeline for creating a secure artifact with the CI tool Concourse.

A good CI/CD solution is one of the entry points when it comes to designing the attack surface dynamically. The faster new software versions can be deployed, the faster the structure of a complex software solution changes. This approach can certainly not keep up with the speed of Cyel's Software-Defined-Network solution. It can be seen as a supplement to this and thus further increases the security of a system.

The mentioned CI/CD tool is flexible and configurable. Thus, the same toolset can now be used to implement the following MTD ideas.

Autoscaling as Security

A large part of the Data Fusion Platform is based on the serverless concept. In the past there was a large monolithic architecture, but now the large application was divided into many small functions. In case of the Data Fusion Platform, there are functions for providing the static and web-based user interface, functions for persisting data or functions for processing data. These functions can be written in different programming languages such as Java, Python or NodeJS. All functions have in common that they are containerized and stateless.

The orchestrator of the functions decides on the basis of criteria which function is needed how often and scales it up and down automatically. If there is no load on the system, then in extreme cases no function runs. Technically this means that no container is started for any of the functions resulting in a decreased attack surface.

The orchestration of the functions uses features of Kubernetes. When the functions are started, it is not possible to predict on which Kubernetes node the functions will ultimately run.

This serverless concept, which was implemented in the Data Fusion Platform, creates a completely dynamic system that can look different every minute.

Using Credential Managers

With distributed systems, one is inevitably confronted with the question of when and how to transfer access credentials, for example to databases, to the containers. There are already introduced and sufficiently tested solutions for this, which take over the administration of credentials.

Using Hashicorp Vault and its Spring Cloud integration, it is possible to query access credentials to a Cassandra database at the start of an application. Hashicorp Vault generates a combination of user and password in the background, which is securely transferred to the application.

These credentials are stored within the Cassandra database by Hashicorp Vault with a certain time-to-live. The combination loses its validity after a certain period of time, e.g. 1 day, and can no longer be used. If an application is ever compromised, the damage can be limited in time.

The heart of the system is the credential manager, which makes credential handling safer and more dynamic. It must of course be assumed that the credential manager can be trusted.

Changing Base Images

All modules of the Data Fusion Platform are containerized by using Docker and orchestrated by Kubernetes. In most of the cases, the base image relies on Official Docker Images, e.g. Alpine Linux images from AdoptOpenJDK. Alpine Linux is a security-oriented, lightweight Linux distribution based on musl instead of glibc as C/C++ compiler. In case of Java, Clojure, Kotlin or Scala, the JVM runs on musl instead of glibc.

In order to change the attack surface, the development team can select and validate various base images for the DFP modules and let the CI/CD tool decide randomly which one is selected for deployment. In case of Java and all derivatives it can be a randomized decision between Alpine and non-Alpine Linux distributions.

Changing Host Images

As already described, Kubernetes is used as central container orchestration. The Kubernetes master dynamically distributes the load to the Kubernetes node. The Kubernetes software runs on machines with a Linux operating system.

The machines can run as bare metal or as a virtual machine installation.

In the past we could successfully create fully automated ISOs for the operating system installation, which already contained all necessary software packages, patches, etc.. This makes it possible for machines to boot the ISO over a network by using the PXE protocol. Immediately after booting the ISO, the respective machine is ready for operation and does not need to reload any further packages.

In case of the Kubernetes nodes, this would mean that they are also stateless, will get their operating system installation over the network when they are powered on and don't need any hardware disc any longer.

For the MTD concept this means that the CI/CD solution would be used to create different and trusted operating system installations in regular intervals. Linux distributions could be Ubuntu or CentOS. The decision which node would boot which ISO would also be randomized and controlled by the CI/CD solution.

Switching to Micro VMs

Within the Data Fusion Platform, containerd is the runtime that manages the entire lifecycle of a container. Containerd fully leverages the OCI Runtime Specification, image format specifications and OCI reference implementation (runc). In addition, there is a Docker daemon on top of containerd, which provides further necessary features for the management.

The big weakness of the Docker daemon is that it runs with root privileges. This means that if a service were to break out of the docker container, it would immediately have root privileges on the respective Kubernetes node. The damage as written in CVE-2018-15664 would be severe.

On way to prevent this is by introducing another abstraction layer. In contrast to conventional containers, the so-called micro-VMs can provide an additional isolation layer via the KVM hypervisor. Firecracker is one implementation of the micro-VM idea. Like traditional containers, Firecracker micro-VMs offer fast start-up and shut-down and minimal overhead. The big advantage of Firecracker is, it offers strong hardware-virtualization-based security and workload isolation. Containerd is still the runtime that manages the entire life cycle of a container. It keeps the benefits of containerization but eliminates the security concerns.

There are first tests planned for Q4 of 2019 to replace Docker with micro-VMs such as Firecracker.

Summary

Consequences and Roadmap

All the ideas described in this paper make an implementation of the Data Fusion Platform look differently within short time. Adversaries will lose their asymmetric advantage in having time to study a system, identifying its vulnerabilities and choosing the time place of attacks. The described approaches are tested and some of them are already implemented, and the rest are part of our road map.

The paper is intended to show that cyber security is a major concern of Traversals and that both knowledge and competences are available to implement this effectively and efficiently.

Make Data Speak Your Language

Traversals is an analysis and intelligence company based in Erlangen/Germany. It offers software products and related services for companies and authorities. Traversals plays a decisive role in making data understandable for people who are not data scientists.

For More Information

If you have questions or would like to discuss this data sheet, please contact us. As an advocate of innovative IT solutions, we are committed to keeping a dialogue open on technologies, processes and best practices that will help us to support our customers.

Contact

Web: www.traversals.com

Phone: +49 9131 92790 0

Fax: +49 9131 92790 99

Email: info@traversals.com

traversals