Moving Target Defense

F. J. González Rodríguez, E. Aguirre Anaya, M. Salinas Rosales,

Keywords

Moving Target Defense; Cybersecurity; Structural Equation Modeling; MTD Technique; MTD Strategy; MTD Evaluation; SDN.

Abstract

Moving Target Defense aims to secure a system by changing the attack surface. To achieve this goal, the MTD model contains techniques to execute the changes in the system. An algorthm known as strategy analyzes the posible changes based on the techniques to propose a change (movement). Finally, the movement is evaluated previous its deplayment.

1. MTD vs Traditional security

Traditional security focuses on minimizing the attack surface. The reduce of the surface is shown in Figure 1 (a), where the white circle is the whole system and the gray circle is the exposed surface. The removal of unnecessary services, tools, and othe features, reduce the exposed surface which the counterpart can interact. On the other hand, in Figure 1 (b) is shown a system that contains a gray circle, which can move to different areas inside the white circle, and even increase or reduce its attack surface. Such behaviour misleads the offensive side on the information gathering phase.

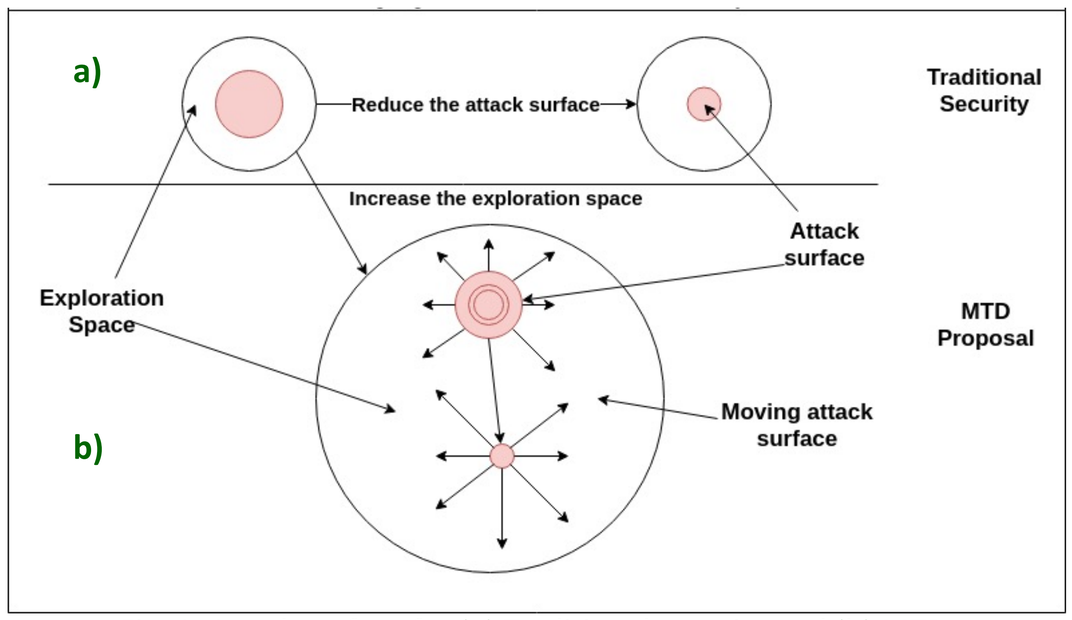

Fig. 1. Attack surface for (a) Traditional security and (b) MTD.

2. MTD on logic containers

Containers are an abstraction in the application layer, where the code and dependencies of an application are grouped, allowing them to be executed in different environments, such as the cloud, which allows access to a computing infrastructure through the Internet that offers high computing capacity and data storage on demand, nevertheless, this could generate a security problem, since by hosting information in the cloud, direct control of the data is renounced and certain control is being given to an external source over the container data. Consequently, the owner of the data should have to rely on good management by the supplier. From a zero-trust approach was designed a new moving-based defensive control for the logical container file system.

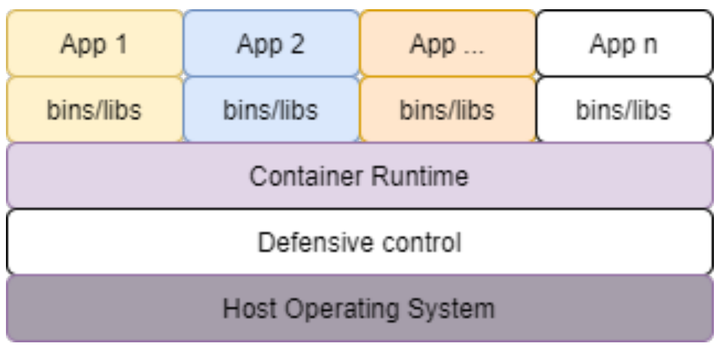

Fig. 2. Logic containers with a defensive control layer

3. Interruption minimization for MTD movements

In this research a hybrid strategy for Moving Target Defense (MTD) is presented, designed to minimize interruption times when performing an MTD movement. This strategy combines the advantage of a soft handover with the network centralized management that provides the Software Defined Networks (SDN). The handover process used is soft handover, which is based on starting next connection before breaking the last, giving theoretical downtimes equals to zero when executing a handover

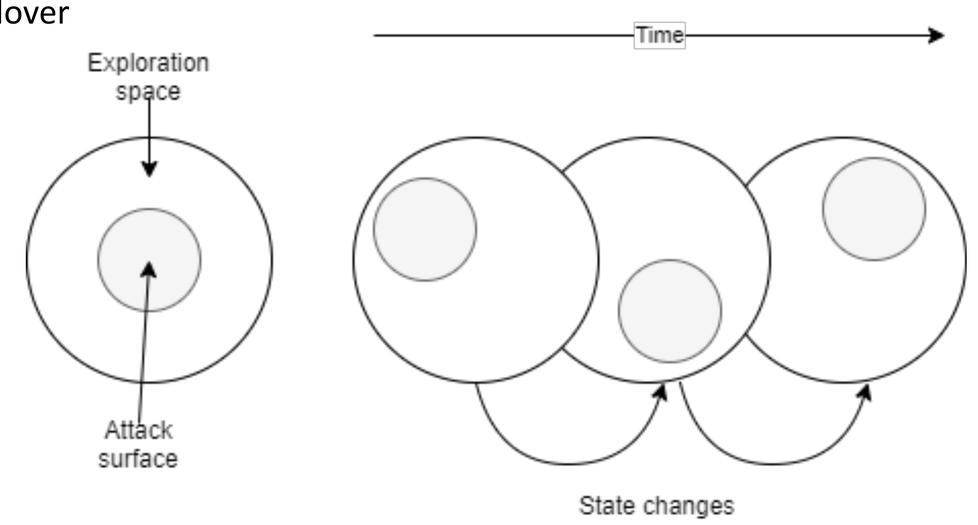

Fig. 3. MTD movements through the time and overlapping to keep the service availability

4. MTD impact on business logic

The movements deployed by MTD, aims to improve the security but also could affect the service level. Therefore, it is important to measure the impact of a target movement, based on the current infrastructure or the ideal service level. In this sense, we proposed a novel approach to correlacte the functional model, and the movement model, and measure the correlation of the assets based on their assets value.

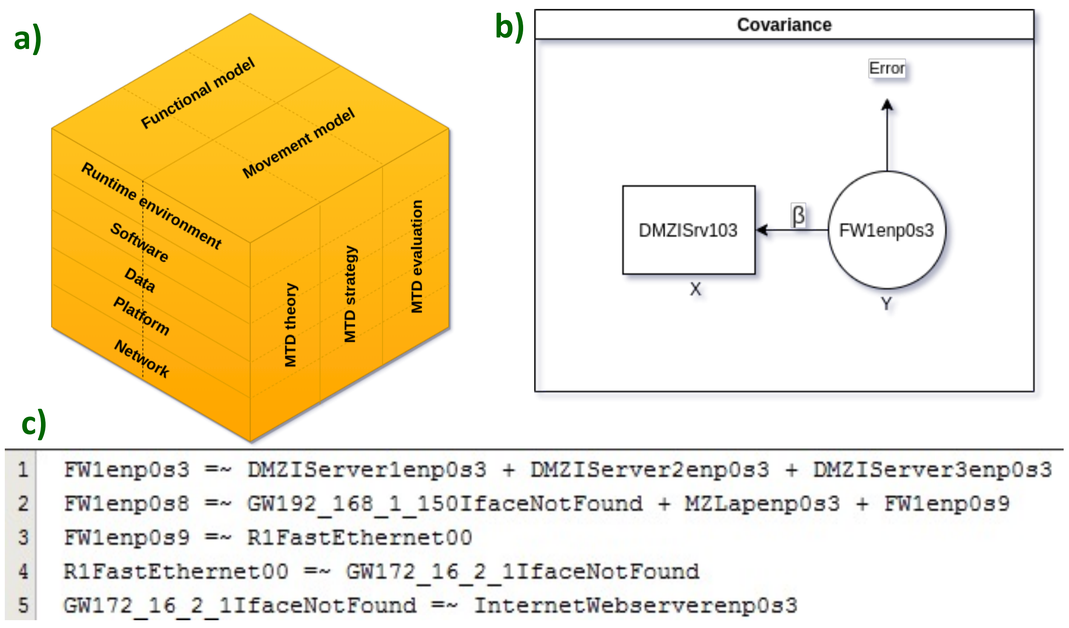

Fig. 4. a) MTD layers intersects with five system layers resulting in a functional side, and the movement side. b) Assets can be modeled as equations (c) to measure their correlation.

5. Conclusions

Moving Target Denfese requires techniques to execute changes at different levels. Therefore, we developed some of them considering other components in an MTD system, as the strategy algorthm, the technical impact, and the impact on the business. Our contributions are the base to develope algorithms on realistic scenarios and consider limitations further than the technical ones. As future work, once we implement MTD on a realistic scenario, we Will try to test MTD environments with an offensive approach. This can be used during penetration testing services.