guardtime

FMNiga koosvõimelise töötlussüsteemi paigaldamise automatiseerimise eeluuring

Study Report: Summary

(Automating the Deployment of FMN Compatible Systems)

REPUBLIC OF ESTONIA
MINISTRY OF DEFENCE

This research was commissioned by the Estonian Ministry of Defence as part of the "Valdkondliku teadus- ja arendustegevuse tugevdamine" (RITA) program. The project is funded 60% by the European Regional Development Fund and 40% by the Estonian Ministry of Defence.

Introduction

This report captures the finding of preliminary research into automating the deployment of Federated Mission Network (FMN) capabilities on a cyber range.

A cyber range is a set of technical solutions that allows the conduct of Concept Development and Experimentation (CD&E) activities, the training of specialists in realistic cyber situations, and the certification and accreditation of systems. Cyber ranges are virtual environments that can be used to simulate local networks, wide area networks, conventional information systems, industrial systems, users, and aspects of the Internet at various levels of fidelity. Recent developments in cloud services automation as well as continuous development and integration have led to increased efficiency in the use of cyber ranges, making them an ideal tool for testing and validating concepts and technologies, testing the cybersecurity of systems, and training cyber defenders on the latest cybersecurity tactics, helping them improve their cybersecurity skills in a realistic and safe version of their own critical IT systems

Within NATO, the concept of Federated Mission Network (FMN) is an initiative focused on the interoperability and operational effectiveness of NATO military forces through the rapid instantiation of mission networks. Developed over the past few years, the FMN initiative makes regular use of CD&E and testing activities, mostly using physical IT equipment. This approach for the setup, configuration, and operation of such a complex system hosting multiple hundreds of participants and supporting a wide number of different network configurations and functionalities requires significant resources, both in terms of equipment and effort. While setting up cyber ranges can also be time consuming as it requires special understanding of both the host infrastructure and the environment to be simulated, recent developments in automation introduce economies of scale for repeated activities that have common patterns.

The aim of this study is to understand whether it is possible to create a solution for describing in a machine-processable way FMN capabilities such that they can be deployed on a cyber range, creating connections between information systems, automating the installation of a given processing system and validating and testing the installed system. This is a new approach, the implementation of which has not been studied in Estonia or internationally.

At present, it is not known whether there is a suitable description language, whether it is possible to build connections between services in a virtual environment in an automated way using such a language, and whether it is possible to ensure the

correctness of systems so deployed. Due to this information gap, it is not possible to determine if the use of cyber-ranges can increase the efficiency of FMN activities, as without this automation, the preparation time for range-based activities will likely be similar to the preparation time required under the traditional approach of using conventional IT equipment. This preliminary study will take a first look at potential technologies, test their capabilities through a Proof-of-Concept (PoC), and assess the benefits of range-based automation (economic, human resources, etc.) for FMN activities. This includes having the system independently create an environment in which the automation creates connections, implements security measures, installs the necessary software, and creates users in accordance with FMN specifications and best practices.

Conclusion

The authors of this study found that automating the deployment of FMN compatible systems would be highly beneficial to NATO and has answered as many of the questions asked as possible within its time and information constraints. As well, further work towards using cyber ranges for FMN activities is clearly warranted based on the following key findings:

- Current technologies such as DSLs and CI/CD automation tools are sufficiently mature to be used as a basis for delivering orchestration that would save considerable manual work in FMN activities.
- The TOSCA standard seems likely to fulfill a good portion of the description language's requirement and can be extended to address gaps. It also provides a level of interoperability that will be valued by NATO Nations.
- The FMN specifications are well formed and sufficiently detailed, and thus suitable for transformation into the machinable-processable specifications required by an automation system.

Specific work items were identified in the recommendation for a follow-on detailed study estimated at 18 person-months of effort.

Finally, it is clear to the authors that the FMN Community has much to gain from making better use of cyber ranges in their activities, and that the use cases of the FMN Community are well aligned with the current and upcoming products and services offered by cyber range providers. For the FMN Community, pursuing further work in range-based automated deployment will lead to significant economies during experimentation, testing, and exercises, and may also lead to the development of production-grade capabilities that can be used during actual military missions in which mission networks based on FMN standards are deployed.