The Framework Programme for Research & Innovation
Innovation actions (IA)

Project Title:

FORTIKA - cybersecurity Accelerator for trusted SMEs IT Ecosystems

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement n°740690

FORTIKA White Paper #2:
FORTIKA Marketplace – Build your own Cybersecurity Solution

Responsible partners: XLAB

Contributing partners: CERTH-ITI, HMU (ex TEIC), HOPU, FINT

Contents

I. Introduction

This is the second white paper in the series of white papers of the FORTIKA project [1]. FORTIKA is an EU funded project under Horizon 2020 program with a budget of approximately 4.9 million euro. The project duration is three years, ending in May 2020. The FORTIKA consortium includes sixteen partners from nine countries, among them three Universities, two Research Institutes, six IT companies and five companies as end users.

FORTIKA aims to develop and demonstrate new technologies to minimise the exposure of small and medium sized businesses to cybersecurity risks and threats while relieving them from all efforts of identifying, acquiring and using the appropriate cybersecurity solutions.

One of the most innovative features of FORTIKA is that, along with its new cybersecurity technologies, the project developed a **marketplace** to deploy its technological products as well as cybersecurity products for SMEs (small-medium sized enterprises), offered by other, reviewed **third party** developers and vendors. Thus, the marketplace is considered not only as a FORTIKA promotion platform but also as an open platform for trading cybersecurity services targeted to SMEs worldwide.

The first white paper presented the overall concept of edge acceleration [2]. This white paper focuses on the services around the accelerated solutions - the marketplace, the offering and the technology enabling deployment of the services on an affordable device, namely FORTIKA Gateway.

II. The FORTIKA Marketplace as a paradigm of platform innovation

The international literature on innovation management distinguishes "platform innovation" from "product innovation". Further, an analogous distinction between "linear businesses" and "platform businesses" exists. A linear business directly creates and controls inventory via a supply chain. Platform businesses do not own the means of production. Instead, like Facebook, AirBnb or Alibaba, they create the means of connection.

A platform is a business model that creates value by facilitating exchanges between two or more interdependent groups, usually consumers and producers.

In order to make these exchanges happen, platforms grow and create large, networks of users and resources accessible on demand. By offering the means of connection, platforms create communities and markets that allow users to interact and transact.

The FORTIKA Marketplace is a typical example of **platform innovation** as it incorporates all of the above features.

III. The economic perspectives of the Marketplace

The financial potential of a platform such as the FORTIKA Marketplace is enormous, since it may address the needs of the entirety of SMEs by providing solutions from many different developers and vendors of cybersecurity goods.

The cybersecurity market is propelled by the increasing need among enterprises to minimize security risks. According to recent studies, the cybersecurity market size estimated at over 107 billion Euro in 2017 and is anticipated to grow at a Compound Annual Growth Rate (CAGR) of more than 12% from 2018 to 2024 [6].

The business challenge for the FORTIKA Marketplace is to attract the attention of enough customers and developers/vendors in order to reach a **critical size** allowing it to become a **focal poin**t in the cybersecurity market targeted to SMEs worldwide, and a recognizable **brand name**.

IV. The concept of FORTIKA Marketplace

The market of cybersecurity solutions is growing rapidly and provides many solutions for different needs of end-users with respect to mitigating cybersecurity threats. Having a marketplace of security solutions where end-users would express their demand and would be able to purchase and even quote for services they need, is very appealing. And this is exactly what FORTIKA is offering, a marketplace of cybersecurity services (bundles in FORTIKA terminology) that can be purchased using simple steps using the web-based user interface. The solution is targeted towards SMEs within the EU (but not limited only to the EU). The

services residing on the marketplace can be deployed on dedicated hardware, namely the FORTIKA Gateway, which is part of the FORTIKA offering. Since the services offered by the marketplace are designed to run on an FPGA (Field Programmable Gate Array) enabled device [2], the FORTIKA Gateway is a required component for SMEs that wish to benefit from the FORTIKA solution.

FORTIKA Marketplace consists of different core services enabling the main use cases to the target end-users:

- developers can publish their services in the marketplace
- end-users can search for suitable solutions that can be bought from the marketplace
- services running on the dedicated hardware can be managed and monitored from the web-based user interface

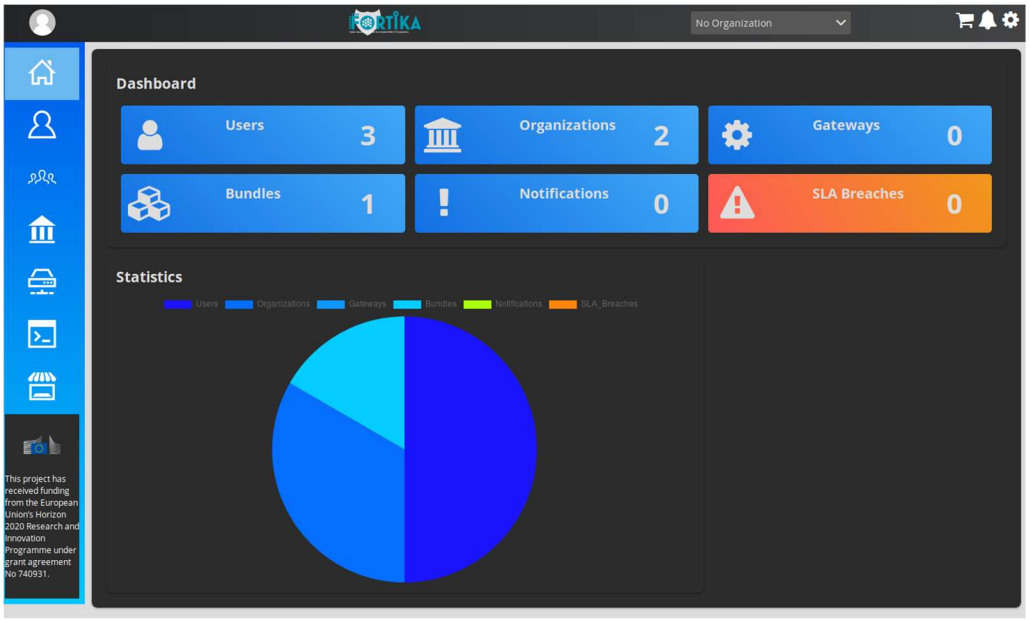

Figure 1: FORTIKA Marketplace's web-based user interface.

There are different user roles in the marketplace: administrators of an organisation can manage users of the organisation, users of an organisation that can purchase services, developers of an organisation can publish new services, and the master administrator managing FORTIKA Marketplace itself.

V. Technology behind the marketplace

FORTIKA Marketplace exposes a RESTful API for all the functionalities offered. Developers can reuse their existing tools and scripts in order to interact with the marketplace. All communication with cloud services required for managing devices and services running in the end-user's domain is exchanged over a secure channel. The channel is provided by Light Weight Machine to Machine Protocol (LWM2M) [5]. This protocol is one of the most appropriate for this application due to was designed for sensor networks and the demands of a machine-to-machine (M2M) environment. LWM2M2 is efficient and secure client-server protocol for managing resource constrained devices. In addition, it offers a wide variety of ready-to-use standard objects (OMNA, IPSO, GSMA Objects) supported by a well-defined data and communication model.

Some of the main features that make this protocol the most appropriate for the application is the connectivity monitoring, remote device actions and structured FOTA (firmware-over-the-

air) and SOTA (software-over-the-air) updates, which are its main advantages over similar protocols such as MQTT [7] or AMQP [8].

In terms of security, LWM2M uses OSCORE [9] to ensure end-to-end application-layer, also include natively support the DLTS 1.2+ and TLS 1.2+ protocols. All these functionalities are implemented without compromising protocol performance.

FORTIKA Marketplace allows developers to publish bundles either by using a wizard in the web-based UI, or by uploading a YAML descriptor file that describes the bundle using the TOSCA standard (*Topology and Orchestration Specification for Cloud Applications)* [4]. TOSCA is an OASIS standard language to describe the topology of cloud-based web services, their components, relationships, and the processes that manage them. FORTIKA allows developers to easily exchange specifications of their services using the TOSCA format. Moreover, service versioning is easier and makes the service more interoperable (easier to transfer).

VI. The solutions offered and the next steps

Currently, FORTIKA Marketplace provides seven distinct cybersecurity solutions, namely the Attribute Based Access Control (ABAC), Real Time Network Traffic Analysis (RTNTA), Risk Detection Module, Social Engineering Attack Recognition System (SEARS), Virtual Security Appliance (VSA), and Security Information and Event Management (SIEM). The ABAC provides a versatile and robust solution towards controlling the access to the various resources existing in an SME environment, especially in the light of Bring Your Own Device (BYOD) trend that currently exists in many companies. RTNTA module is capable of collecting and processing network flow, log, and traffic data. It can also convert the traffic data into netflow v5, netflow v9, ipfix or sflow. SEARS operates in the application layer and is able to detect communication risks, informing other bundles and SME users about the detected threats (preventing personal or corporate data leakage). VSA module is a component that protects the network of SMEs from potentially malicious traffic similar to existing intrusion detection and protection solutions (firewalls). It detects numerous types of network attacks and reports these threats to the end-user (administrator of the organization) in real-time. FORTIKA SIEM bundle is a solution able to analyse information and events collected at the different levels of the monitored system to discover possible ongoing attacks, or anomalous situations. It comprises several modules (risk detection module, anomaly detection service, decision support service, visual analytics service, deep packet inspection tools, automated asset discovery service).

As a next step, it is envisaged that FORTIKA enables third party developers to offer also their cybersecurity solutions, via the Marketplace, to the end users (SMEs) reachable though the FORTIKA Marketplace. Making the marketplace easily reachable, and capable of offering a plethora of different managed cybersecurity solutions through one umbrella cloud service such as FORTIKA Marketplace, is one of the main goals of FORTIKA project. This would make the platform a compelling ecosystem that would propel itself and make it self-sustainable and growing.

VII. References

[1] FORTIKA project's official home page, FORTIKA Consortium, 2017, https://fortika-project.eu/

[2] FORTIKA White Paper #1 Edge Acceleration and Cyber-security for SMEs: The FORTIKA perspective, FORTIKA Consortium, 2019, https://fortika-project.eu/system/files/presskit/fortika_white_paper_1v0.3.pdf

[3] Lunt, T. F., Jagannathan, R., Lee, R., Whitehurst, A., & Listgarten, S. (1989, March). Knowledge-based intrusion detection. In AI Systems in Government Conference, 1989., Proceedings of the Annual (pp. 102-107). IEEE.

[4] OASIS Topology and Orchestration Specification for Cloud Applications (TOSCA) TC, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca, last accessed 1.7.2019
[5] Lightweight M2M (LWM2M) specifications, http://openmobilealliance.org/release/LightweightM2M/, last accessed 1.7.2019
[6] Cybersecurity Market Size, Ankita Bhutani, Preeti Wadhwani, Global Market Insights, Report ID: GMI3078, Jan 2019, https://www.gminsights.com/industry-analysis/cybersecurity-market
[7] MQTT specifications, http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html , accessed 9.12.2019
[8] AMQP specifications, https://www.rabbitmq.com/protocol.html, accessed 9.12.2019
[9] Object Security for Constrained RESTful Environments (OSCORE), https://www.rfc-editor.org/info/rfc8613 , July 2019