Attack and Behaviour Simulators User Manual

SPHINX

A Universal Cyber Security Toolkit for
Health-Care Industry

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

<u>The ABS is not a regular SPHINX component, which means that it is not intended for use by end users.</u>

It comprises a set of tools, virtual machines and scripts developed to serve the simulation needs of users and malicious agents inside a testbed environment. Hence, ABS functionalities are divided in two core subcomponents:

<u>Behaviour Simulator</u>

The Behaviour Simulator involves the behavioural analysis of network devices stemming from network (netflow1) traffic provided by the DYPE5 pilot along with their statistical reproduction.

Traffic is used to extract behavioural characteristics of different devices of the infrastructure, leading to various profiles of several user groups (e.g. doctors, lab users, IT employees etc.) based on their application usage patterns through time. Machine learning algorithms are first used to extract the application usage profiles and then deep generative neural networks (GANs) are deployed to reproduce / simulate similar ones depending on the desired group of the user. On the other side, a Python-based software has been developed, that can be installed on different network devices (either real or emulated by the SPHINX Sandbox). This tool can simulate client interactions of the device with specific services (social media, browsing, e-mail, ssh, HIS server, DICOM servers) through dedicated scripts based on automation frameworks (e.g Selenium). This tool requires as input a predefined behavioural class of profile as identified in the analysis section and starts to simulate the relevant behaviour inside the network infrastructure where it belongs. The tool also disposes an API as well as a simplified UI that permits the selection of the desired profile type for the device of interest.

The Behaviour Simulator will allow the SPHINX components to operate and be tested in realistic network conditions involving the user behaviours and interactions that would normally appear in a real healthcare environment.

<u>Attack Simulator</u>

This Attack Simulator involves the preparation of cyber-attacks and required environments for their triggering. The cyberattacks being prepared are mainly linked to the SPHINX use cases.

Various hacking techniques and malwares have been examined and documented according to the MITRE&ATTACK[2] framework. Additionally, new ones are being created so that can effectively simulate the kill chains described in the SPHINX use cases. Appropriate network topologies and operating systems are being selected based on virtual machine technologies (e.g. VirtualBox and VMware[3]) while all specifications, vulnerabilities and attack steps are being extensively documented in order to ensure their reproduceability in new environments such as the SPHINX Sandbox and the emulated pilot infrastructures to be used during the demonstration process.

The Attack Simulator will allow the SPHINX components to be tested for their effectiveness at detecting cyberattacks and kill chains that are very likely to be triggered in healthcare IT infrastructures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.