Homomorphic Encryption
User Manual

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Table of contents

Table of figures

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

The Homomorphic tool uses searchable encryption capabilities to provide data anonymization functionalities. It encrypts all network traffic that needs to be relayed outside the hospital network and thus ensures that no personal details leave the network. The recipient of the data can then ping the HE tool to search in the encrypted domain to gather information if needed.

The HE tool takes as input network traffic information and encrypts all personal data. This personal data is replaced with surrogate values which are then stored in a local database. The recipient of the information can query the HE tool to identify the existence or absence of any personal data in the database. The query made to the tool only reveals if the entry is true or not and does not reveal the actual entry. This ensures that an intruder cannot get vital information from the database. In case the query is made by a legitimate entity, then the decryption functionality of the HE tool can be used to gather plain text information.

1.1.1 Installation/Deployment

The installation of the HE tool is based on Docker image. The docker image initiates a Rest-Api interface which exercises three main end points namely, encrypt, search and decrypt. These interfaces interact with the DTM tool but can be accessed directly by making HTTP Post request.

1.1.1.1 Prerequisites and hardware

The HE tool works as a backend tool and makes use of the state of the art encryption techniques. For this to work the minimum hardware requirements that will ensure smooth execution are as follows:

- CPU: 4-cores
- RAM: 8 GB RAM
- Disk Space: For local database storage 20 GB

1.1.1.2 Deployment with Docker

The docker image of the tool is available on Intracom's GitLab server and can be downloaded from their using the following command

git clone https://sphinx-repo.intracom-telecom.com/sphinx-project/homomorphic-encryption/he-tool/-/tree/HE-Codebase/download_files

After cloning the tool, open the terminal window and go inside the created folder. When inside, you will have to build the docker image and then run it for execution. This can be done by following commands:

Build:

```
docker build -t registry.sphinx-repo.intracom-telecom.com/sphinx-project/homomorphic-encryption/he-tool .
```

Run:

```
docker run –name -he -p 9999:8080 -it registry.sphinx-repo.intracom-telecom.com/sphinx-project/homomorphic-encryption/he-tool
```

Now the HE tool is up and running and it should be accessible by the link http://localhost:9999. As there is no Web interface for this tool, so this link is accessible for making http get and post requests.

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.

1.1.1.3 Basic Example

The HE tool is tailored to take as input network traffic information. It takes this information and encrypts all incoming personal information such as IP address and MAC addresses and replaces them with surrogate values. In light to ensure that a malicious actor is still recognisable in the pseudo-anonymized data, the HE tool maintains a local database of the surrogate values and the actual IP address and MAC addresses. This database is encrypted using Homomorphic Encryption giving it the capability to search in the encrypted domain. The HE tool takes inputs such as :

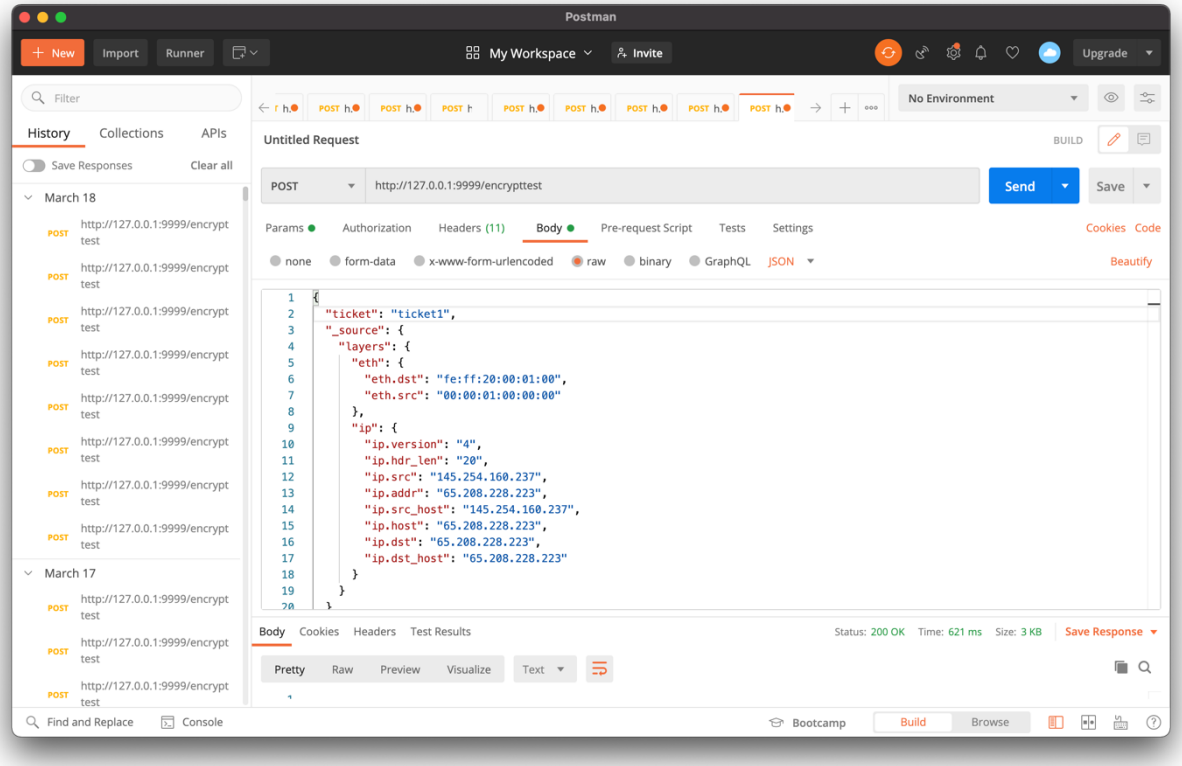

Figure 1 HE – Basic Example

The tool replaces IP address to surrogate values such as 0.0.0.1 and MAC addresses are replaced with surrogate values such as 0:0:0:0:0:0. The surrogate values are in the same format in which the original data exists and this ensures that the remaining tools can recognize these field as IP addresses and MAC addresses respectively.

The search operation assumes that one of the tool has identified that there is a malicious actor in the database, now in order to identify what other traffic information is related to the intruder. The tool can be used to search in the encrypted database. The tools takes a input the actual IP address of the malicious actor or any IP that needs to be searched for. The tool in return responds with the surrogate IP that is being used to represent that particular IP in the database. This can be performed as such:

142.168.1.2 (Actual IP as input) -> (Surrogate IP as response) 0.0.0.1

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.

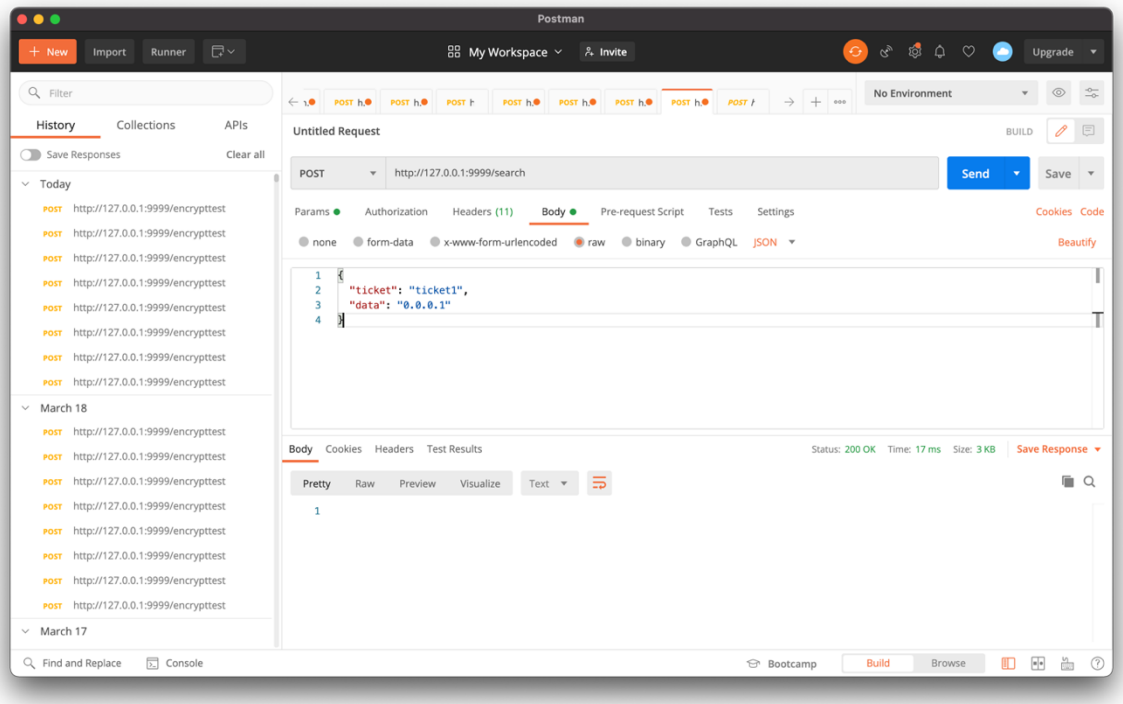

Figure 2 HE – Basic example fig. 2

The decryption operation is used to decrypt surrogate IP addresses to actual IP addresses. It must be noted that IP address is chosen as an example, the same procedure is used for both IP address and MAC address. The tool takes as input the surrogate IP and returns the actual IP from the database. This functionality is mainly used for testing tool and will not be made available in all instances to ensure data privacy.

(Surrogate IP as response) 0.0.0.1 -> 142.168.1.2 (Actual IP as input)

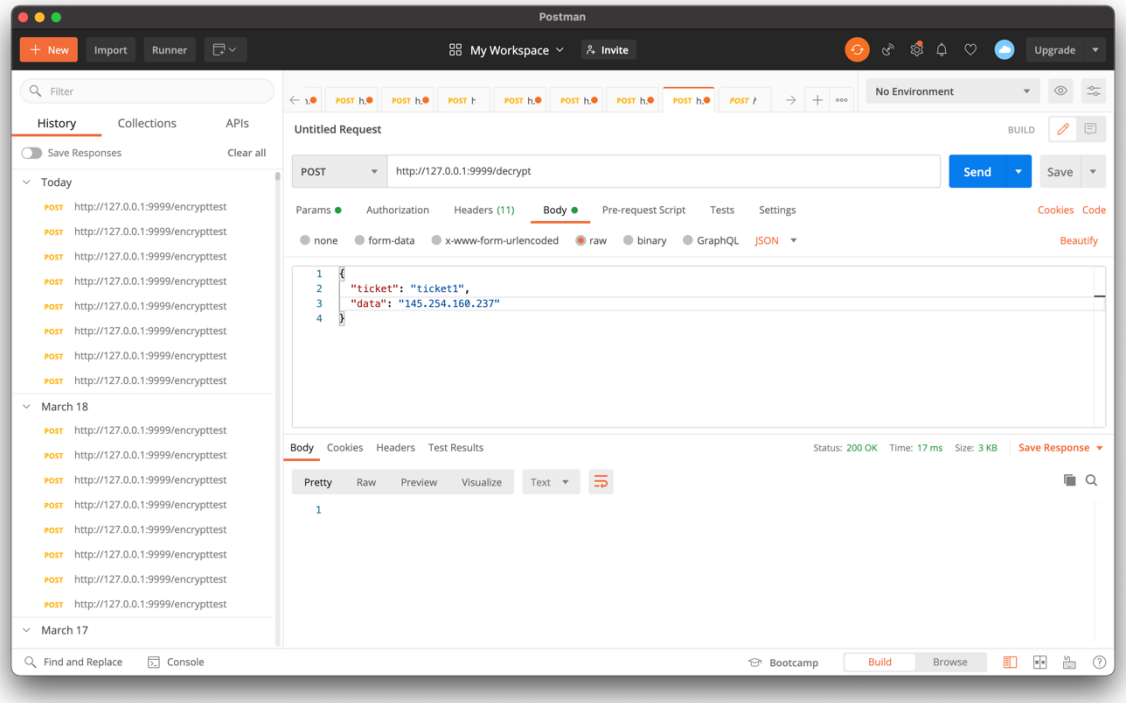

Figure 3 HE – Basic example fig. 3

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.

1.1.1.1 Extra functionality

The HE tool works as a backend tool in the SPHINX toolkit but it also has some additional capabilities that can be exploited with a web interface. This web interface can be accessed with the help of a docker image. This extra functionality can be deployed by cloning the secondary image that is placed on Intracom's git repository. This is specifically made to tailor the web interface. You can access the repository by:

git clone https://sphinx-repo.intracom-telecom.com/sphinx-project/homomorphic-encryption/he-tool/-/tree/HE-Codebase-Multiuser-Search/linux-clientformvn

After cloning the HE tool's web interface, this can be built and deployed using the command line interface. The tool can be built using the following command:

Build:

```
docker build -t registry.sphinx-repo.intracom-telecom.com/sphinx-project/homomorphic-encryption/he-tool-2 .
```

Run:

```
docker run –name -he-web -p 9998:8080 -it registry.sphinx-repo.intracom-telecom.com/sphinx-project/homomorphic-encryption/he-tool-2
```

Now the web interface for the HE tool is up and running and it can be accessed by http:localhost:9998/sphinx. It is necessary to ensure that the back end tool mentioned previously is up and running as this web interface exploits functionalities that are already present in that interface. The web interface would load up to the following page:

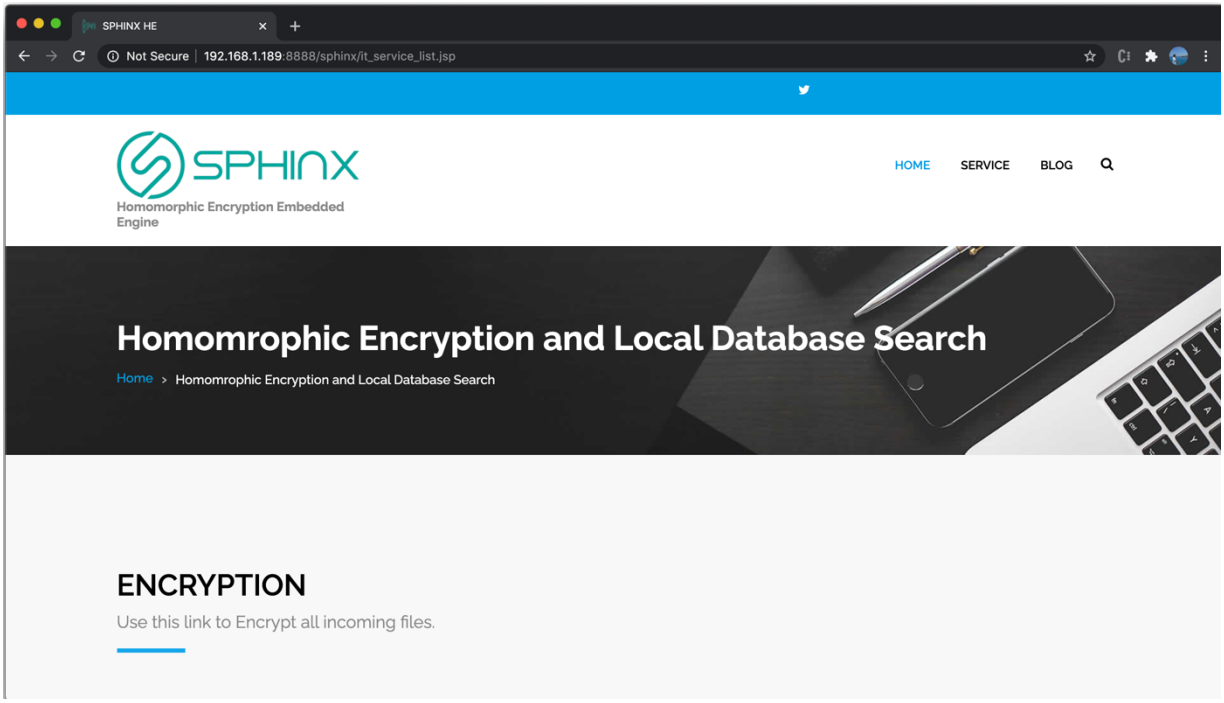

Figure 4 HE – Extra functionality

The users of this tool can use the encryption, decryption and search tool to encrypt any text file and then search in the encrypted domain. The tool lets users to upload any text file and creates searchable cipher from the text file. It then lets the user to search in the encrypted domain. The user can input any keyword and the tool responds with the file that contains that particular search query. It will respond with file names. If a search query is not present in the files that have been encrypted then the tool returns an empty list.

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.