SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Project overview

Meeting place: VUB

Meeting title: Workshop on CYBERSEC4HEALTH

Presenter name:Evangelos Markakis

Presenter organisation: Hellenic Mediterranean University

Date:10/7/201

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

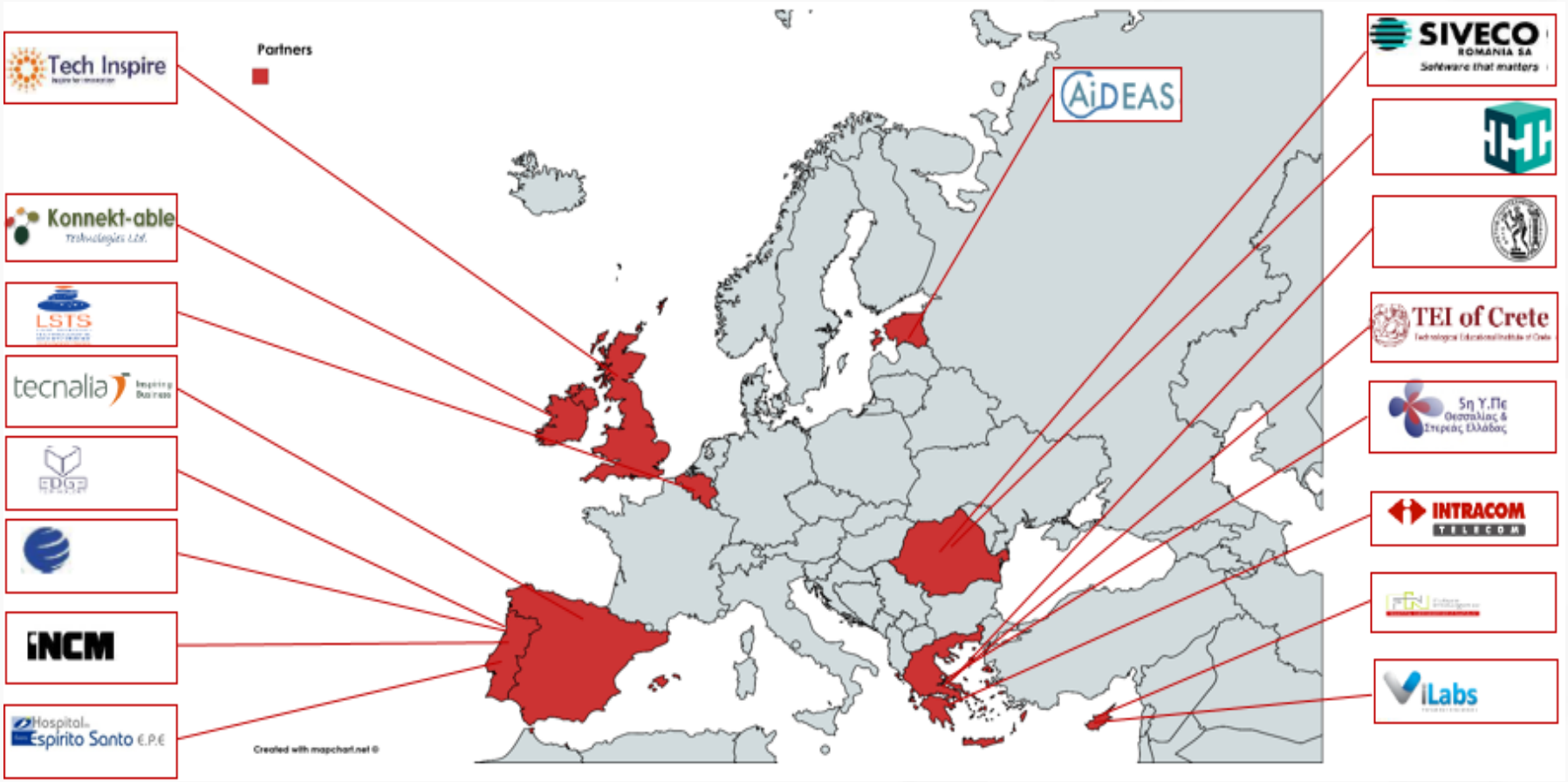
SPHINX IDENTITY

SPHINX Factsheet

SPHINX	A Universal Cyber Security Toolkit for Health-Care Industry
Project Number	826183
Starting Date	1/1/2019
Project duration	36 months
Call(part) Identifier	SU-TDS-02-2018
Topic	Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures
Budget	5 M

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

SPHINX consortium



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

SPHINX POSITIONING

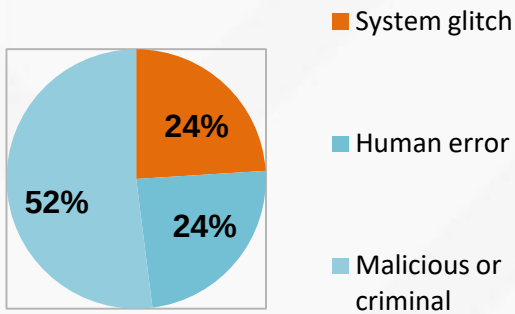
Breached Health Data

- Hospitals and care centres store and exchange large amounts of sensitive patient data, so they are prime targets for cyber criminals
- Medical devices and wearables collecting personal data, become more sophisticated and connected
- Vulnerability of the increasing healthcare ecosystem brought by smartphones

Threats
Advanced persistant threats
Ransomware
Human threat
DDoS
Lost info
Active attacks
etc.

FACTS

- Electronic medical records could be worth up to $USD 1000
- WannaCry caused the "biggest ransomware attack in history" with 57,000 infections in 99 countries, which included several hospitals
- Only in 2014, almost 1.6 million people in the U.S. had their medical information stolen from healthcare providers
- Predictions for more than 25 million people, will have their medical and/ or personal information stolen from their healthcare provider's digitized records between 2015 and 2019



Source: Ponemon

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

Key challenges

- Limited patient or user (e.g. doctor, nurse etc.) awareness and lack of understanding on cyber-security/ privacy issues and processes
- Low usability and underperformance (in terms of effectiveness) of cyber-security solutions
- Vulnerability of current cyber-security solutions

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

SPHINX at a glance

SPHINX aims to introduce a health tailored Universal Cyber Security Toolkit, thus enhancing the cyber protection of the Health and care IT Ecosystem and ensuring patient data privacy and integrity

- Provide an automated zero-touch device and service verification toolkit
- Adapt or embed on existing infrastructures
- Provide cyber-security services through the SPHINX cyber-security toolkit, in a secure and easy-to-use interface
- Address the threats to public critical infrastructure and cyber terrorism

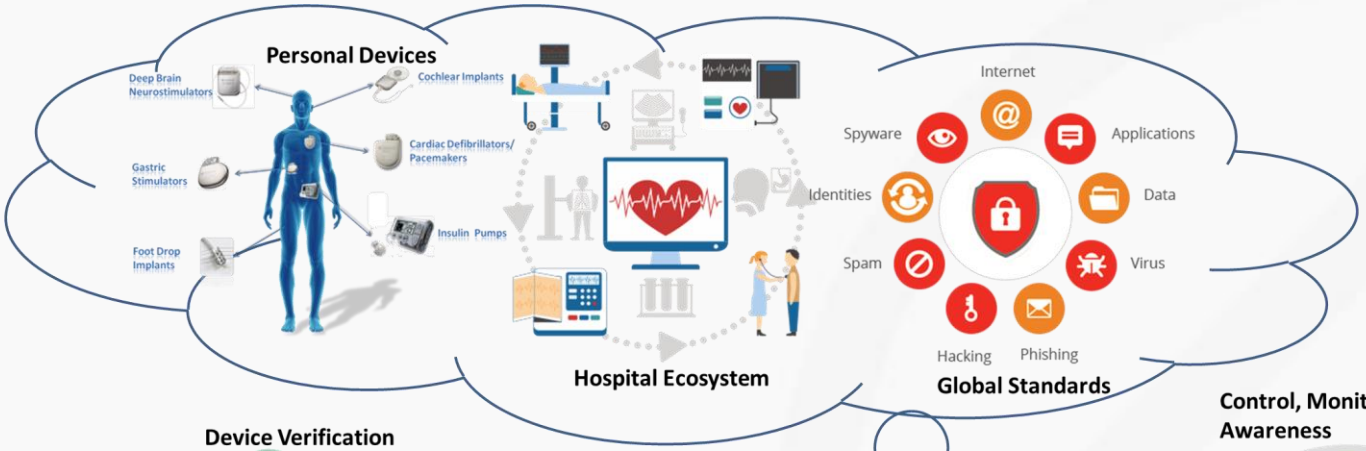
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

SPHINX APPROACH

OBJECTIVES

FOCUSING PILLARS

RELATION TO WORK PROGRAMME



Device Verification

Intercept & Inspect

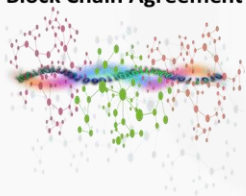
Stream Analysis & Packet Inspection

Context profiling and building
- per device context
- user context

Risk Assessment

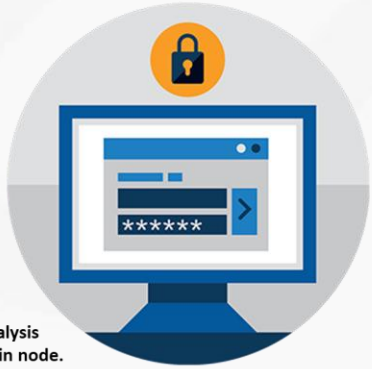
The active data is analysed on its risk by linking associated contexts and process with active risk heuristics

Block Chain Agreement



Guarantee internal integrity. The risk analysis and result is validated by each block chain node. Upon agreement the ruling on the data is executed

Control, Monitoring and Awareness



Provide end-user overview through risk radar application
- Rik status (advanced threats and vulnerabilities)
- Real-time & historical security analytics
- Security insights
- Decision support
- Cybersecurity rules

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

SPHINX Objectives

- SPHINX security awareness ecosystem
- Medical Device CyberSecurity Sandbox
- Vulnerability Assessment as a Service & Automated Cybersecurity Certification
- Model Security Awareness Architecture
- Custom-tailored Security Services
- Behavioural Risk Level Assessment
- Effective response to multiple cybersecurity known or unknown threats
- Automated Mechanisms for sustaining or swiftly restoring end-users trust
- Continuous validation and Proof of concept demonstrations
- SPHINX system commercialisation and exploitation

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

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Questions?

https://sphinx-project.eu

Twitter: https://twitter.com/ProjectSphinx

Facebook: Sphinx-project.eu

LinkedIn page: linkedin.com/company/sphinx-project

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