infocom gr

SANCUS:

Redefining security and Privacy in Modern ICT Infrastructures

Dr. Nikolaos Pitropakis, Cybersecurity Domain Director

nikolaos.pitropakis@8bellsresearch.com

November 2020

EIGHTBELLS
Independent Research & Consultancy

Table of Contents

EIGHT BELLS at a glance 1/3

SANCUS

Our Company

Eight Bells (8BELLS) is a 4-years old **SME** based in Nicosia, Cyprus. In 2020 8BELLS established **a new branch** in Athens, Greece.

Delivers customizable solutions that enhance existing communication technologies relevant to **5G, Cloud Computing, Internet of Things, Cybersecurity.** Specializes **also** in modelling and analysis for businesses.

Has participated in more than 20 EU and national projects that have attracted more than €4 million**.**

Preparation, Execution, Management of R&D projects (mainly H2020), analysis, and quantification of results. Business and Technical Consulting.

EIGHT BELLS at a glance 2/3

SANCUS

Research Expertise & Consulting Services

Customizable solutions that enhance modern communications relevant to the area of 5G Mobile Technology

5G communications

Knowledge on Network Function Virtualization (NFV) and management solutions for Cloud infrastructures.

NVF

Cloud service

Portfolio of cybersecurity solutions that can be used for risk assessment, cyber-hygiene, anomaly detection, and threat remediation.

Cybersecurity solutions

Delivers special advisory services in ICT that help clients understand the market dynamics and profit from the ever-changing landscape. Advise and support other companies and organizations in every step of the process.

Advisory services

Business consulting includes also innovation management, technology transfer and exploitation (including market analysis, patenting, licensing, etc.).

Consulting

EIGHT BELLS at a glance 3/3

SANCUS

Technical Capabilities

Systems & Networks engineering: including design, implementation and integration.

Cloud Computing and Everything-as-a-Service: design, deployment and maintenance of cloud computing infrastructure, etc.

Privacy, Security & Data Protection: Cybersecurity Gap Analysis, Virtualized Cybersecurity, Privacy Impact Assessment, Privacy-by-design architectures.

Software development: for 5G security, wireless network security, software quality assurance, machine learning applications, data analysis and visualization, cloud computing, etc.

Dissemination, Communication and Exploitation Activities.

Ethical and legal compliance activities for various projects, including compliance to the GDPR.

Our Projects

SANCUS

RUNNING

SANCUS

TERMINET

5G CARMEN

5G-INDUCE

GUARD

TrustedFog

AFFORDABLE 5G

AI@EDGE

5GMed

CUREX
SECURE AND PRIVATE HEALTH DATA EXCHANGE

RESPOND-A

CPSoSe

SDN-µSense

THISEAS
Cyprus National Defense Project

SPIDER
5G CYBER RANGE

CARAMEL

SmArt5GrId

FINISHED

SOFTFIRE

Orca
Orchestration and Reconfiguration Control Architecture

FLAME

5G ESSENCE

WiSHFUL

FED4FIRE
FEDERATION FOR FIRE PLUS

SANCUS Overview

- Aims to design and develop an analySis software scheme of uNiform statistiCal sampling, aUdit and defence processes
- The name comes from the Roman god of Trust
- Involves 15 Partners from 8 European countries
- It will formalise the logic of expressing (for the first time) the notions of cyber security and digital privacy by means of final formulas
- SANCUS will fuse security and privacy into optimisation strategies to acquire the truly optimum defence recommendation in dynamic manner

Measurable Objectives 1/2

SANCUS

- To identify and classify the **technical requirements and the EU SELP policy** aspects for designing, developing and integrating the proposed solution.
- To design and implement methods of **automated firmware security validation (FiV) and testing** based on wide-ranging pipeline of analysers and samplers for maximising the surface of vulnerability and risk discovery.
- To design and develop new method of **automated code integrity verification (CiV)** by combining taint, fuzzing and symbolic execution analysis for improving security assessment accuracy, efficiency and searching speed.
- To design and develop new method of **automated network security validation and verification (SiD)** focusing on open-source network development environments based on Docker and Kubernetes technologies.

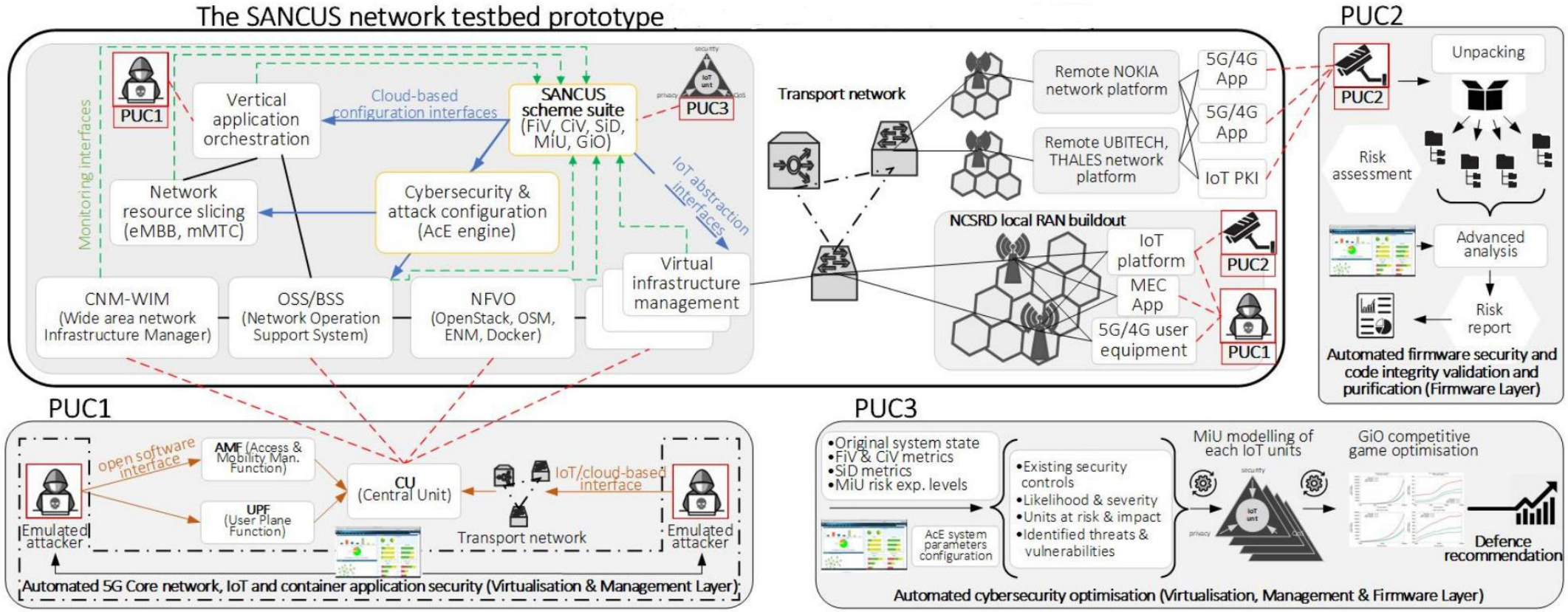
Measurable Objectives 2/2

- To design and develop **new network attack configuration and emulation tool** (AcE) using **state-of-the-art AI/ML** techniques for emulating complex cyber-attacks and generating traffic in container environments.
- To propose revolutionary **MiU modelling of the IoT** unit for expressing the trade-off between cyber security, digital privacy and QoS reliability by means of final formulas based on fundamental mathematical theories.
- To design **game implicit optimisation (GiO)** approach for maximising the security-vs-privacy-vs-reliability efficiency using effective duality-free solution methods.
- To design and establish **operational cloud-native network platform** that integrates the enabling 5G technologies and the engines, mechanisms, tools, solutions developed.

Main Deliverables

- Analysing a firmware image using the developed FiV and CiV modules
  - The FiV engine will perform automated validation of firmware images at massive scale.
  - The CiV engine will perform automated verification and auditing of the unpacked OEM firmware images against risk factors
- Developing and using the SID engine
  - The proposed SiD engine is linked to the CiV and FiV engines for dimensioning different insights on vulnerabilities from both code and system levels
- Transferring the 5G network core processes in a containerized environment
- Cloud native core services
- The Attack Configuration Engine (AcE) will be used for configuring and emulating container services, applications and security mechanisms, as well as, modelling complex cyber-attacks

Use Cases


The SANCUS network testbed prototype
PUC1
Monitoring interfaces
Vertical application orchestration
Cloud-based configuration interfaces
SANCUS scheme suite (FiV, CiV, SiD, MiU, GiO)
PUC3
Network resource slicing (eMBB, mMTC)
Cybersecurity & attack configuration (AcE engine)
IoT abstraction interfaces
Virtual infrastructure management
CNM-WIM (Wide area network Infrastructure Manager)
OSS/BSS (Network Operation Support System)
NFVO (OpenStack, OSM, ENM, Docker)
Transport network
Remote NOKIA network platform
Remote UBITECH, THALES network platform
5G/4G App
5G/4G App
IoT PKI
NCSRD local RAN buildout
IoT platform
MEC App
5G/4G user equipment
PUC2
PUC1
PUC2
Unpacking
Risk assessment
Advanced analysis
Risk report
Automated firmware security and code integrity validation and purification (Firmware Layer)
PUC1
open software interface
AMF (Access & Mobility Man. Function)
UPF (User Plane Function)
CU (Central Unit)
IoT/cloud-based interface
Transport network
Emulated attacker
Emulated attacker
Automated 5G Core network, IoT and container application security (Virtualisation & Management Layer)
PUC3
•Original system state
•FiV & CiV metrics
•SiD metrics
•MiU risk exp. levels
AcE system parameters configuration
•Existing security controls
•Likelihood & severity
•Units at risk & impact
•Identified threats & vulnerabilities
MiU modelling of each IoT units
GiO competitive game optimisation
Defence recommendation
Automated cybersecurity optimisation (Virtualisation, Management & Firmware Layer)

PUC1

Automated 5G Core network, IoT and container application security (Virtualization & Management Layer)

I. provides effective detection of cyber threats in the early stages of an attack

II. mitigates and reduces the impact of the attacks in the network and in the end-users' equipment, in order to take the necessary actions to protect them

III. applies its security functions, benchmarks the degree of protection against the current model of security management and over a number of advanced security threats

IV. protects against container attacks, within, between and outside containers

PUC2

Automated firmware security and code integrity validation and purification (Firmware Layer)

I. provides effective detection of malicious firmware

II. mitigates the impact of the malicious firmware on the network and its devices

III. accurately reports the security risks, by only relying on its automated analysis of the binary firmware's of its devices. Emphasis will be given on auditing the outcomes with respect to each device

PUC3

Automated cybersecurity optimization in distributed networks (Virtualization, Management, Firmware Layer)

- Keeping firewalls, routers, switches and other devices configured along with effective security policy management is a complicated process.
- The key is to design, deploy and support these solutions for ensuring that the network can dynamically run optimally and that organizations can benefit from latest policy updates and solutions offerings.
- SANCUS aims to support cybersecurity assessments at Virtualization, Management & Firmware Layers and to evaluate its capacity for optimizing the security-vs-privacy-vs-reliability performance of the network dynamically and automatically.

EIGHT BELLS Role

EIGHT BELLS is:

- leading Exploitation plan, business analysis and knowledge transfer
- contributing to designing the use-cases, defining the requirements and the architecture of SANCUS
- helping with identification and classification of security concerns in the OEM supply chain, connectivity approaches in the scope of 5G cloud-native system network
- contributing to digital security in the cloud-native core services and model complex cyber-attacks.
- contributing to the system demonstration validation and integration WP6, specifically in the planning of the demonstration and validation scenarios, in the scenario-driven attacks and the framework of evaluation.

Synergies

SANCUS

SANCUS

TERMINET

SPEAR

CARAMEL

GUARD

TrustedFog

5G CARMEN

5G ESSENCE

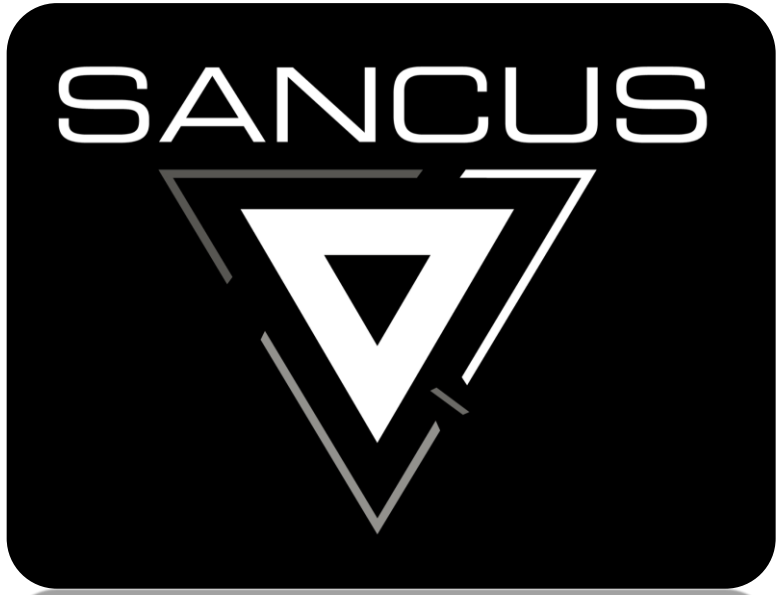
CPSoSe

AFFORDABLE 5G

SPIDER
5G CYBER RANGE

SDN-µSense

THISEAS
Cyprus National Defense Project



Thank you for your attention

Dr. Nikolaos Pitropakis, Cybersecurity Domain Director

nikolaos.pitropakis@8bellsresearch.com