SANCUS – Towards Unifying the Analysis and Control of Security, Privacy and Service Reliability

Charilaos Zarakovitis*, Nikolaos Pitropakis†, Dimitrios Klonidis‡ and Hicham Khalife§
*Media Networks Laboratory, NCSR "DEMOKRITOS", c.zarakovitis@iit.demokritos.gr
†Eight Bells LTD, Athens, Greece, nikolaos.pitropakis@8bellsresearch.com
‡UBITECH LTD, Athens, Greece, dkonidis@ubitech.eu
§Thales Communications & Security - France, hicham.khalife@thalesgroup.com

***Abstract*—The arrival of new technologies change the global digital landscape in many ways. In the past years, for example, network virtualization and cloud computing have given raise to organizations for meeting their everyday needs in an elastic manner without continuously investing on physical infrastructure. Things combined with fifth-generation (5G) technology standards speeded up the communication speeds providing, thereby, new perspectives to verticals and especially, Industry 4.0. However, the increasing popularity of such technologies have also attracted the attention of malicious parties, and thereby, conventional cybersecurity solutions start becoming obsolete. The analysis software scheme of uniform statistical sampling, audit and defence processes (SANCUS) draws on formalising the logic of expressing – for the first time – the notions of cyber security and digital privacy by means of final formulas and fuse these formulas into optimisation strategies to acquire the truly optimal defense recommendation in dynamic manner. In this respect, we aim at investigating inclusive solutions in the form of unified security-vs-privacy-vs-reliability trade-offs, for manipulating the system network cybersecurity, privacy and quality of service performance jointly, explicitly and automatically.**

***Keywords*—5G, game theory, IoT, privacy, security, service**

I. Introduction

Conventional cybersecurity solutions may no longer cope with several security challenges that are issued by modern technology trends [1]. For instance, so far, little is known on the synergistic effect of cyber security and privacy to the 5G-related devices and applications. Typically, the performance of applications is evaluated through the Quality-of-Service (QoS) reliability, which is a Key Performance Indicator (KPI) related to traffic bit rate, packet delay and packet loss rate. On the other hand, security and privacy are holistic attributes that are highly influential to the overall aspects of QoS reliability at both communication and application levels.

SANCUS aims to tackle such challenges through a ground-breaking design paradigm of a systematic and all-inclusive solution of true network protection. Our solution sits on six efficient engines, namely, FiV, Firmware Inspection engine (FiV), Code Integrity Verification engine (CiV), System Intelligent Defense engine (SiD), Attack Configuration engine (AcE), Modelling of Individual Unit engine (MiU) and Game Implicit Optimisation engine (GiO), which combine unique modelling of the Internet of Thing (IoT) units, cutting-edge methods for automated Original Equipment Manufacturer (OEM) firmware and software validation and verification, and innovative Artificial Intelligence driven game techniques for the automated optimisation of the control and trust of digital services. The high-level architectural logic and main components of the proposed scheme are illustrated in Fig. 1, where the operational logic is outlined over a threefold *firmware-runtime-optimisation* analysis viewpoint.

II. Proposed Solution

The ground-breaking features of the unique *firmware-runtime-optimisation* analysis solution in SANCUS are listed below.

Novel intelligent scheme design: SANCUS opens the door to a completely new way of tackling the cybersecurity of next-generation ICT systems by relying on a holistic scheme design for incorporating AI-driven and automated FiV, CiV and SiD engines of code-level risk assessment coordinated by revolutionary and unique MiU modelling and GiO game optimisation approach for expressing the joint security, privacy and reliability performance by means of final formulas and maximising its revenue explicitly.

Automated cybersecurity firmware validation using new analysis methods: Code-level inspection is an important and difficult point to address due to the many problems in the development of vulnerability detection technology. To cope with these challenges, SANCUS will design and develop an automated vulnerability inspection management engine to combine static (symbolic) and dynamic analysers into a wide-range pipeline for maximising the surface of vulnerability discovery, where a highly extensible pipeline of multiple different unpackers and samplers will allow for searching through monolithic binary firmware images and recompose fragmented code portions into continuous component parts for smoother and faster verification.

Automated cybersecurity firmware verification using new analysis methods: Taint analysis enables deep and exhaustive tracking of suspicious information and control data flows for detection of potential leakage and integrity violations, such as cross-site scripting, SQL injection, log forging, etc. Research in this area has been taken on two techniques, namely, program slicing and type systems, which, however, both suffer from a high rate of false findings, limiting that way the usability of most existing analysis tools [4]. SANCUS introduces a new method for enabling precise, yet scalable taint analysis based on the observation that taint analysis is a demand-driven problem, which enables lazy computation of vulnerable information flows, instead of eagerly computing a complete data-flow solution, which is the reason for the traditional dichotomy between scalability and precision.

Automated cybersecurity risk assessment for open-source software: Modern communications networks that rely on open-license deployment runtimes should feature continuous risk analysis to minimize potentially compromised open-source coding and executables. On the other hand, continuous risk analysis requires multiple different monitoring agents to better-detect vulnerabilities at both the code and network levels. That means, the increase in analysis precision comes with

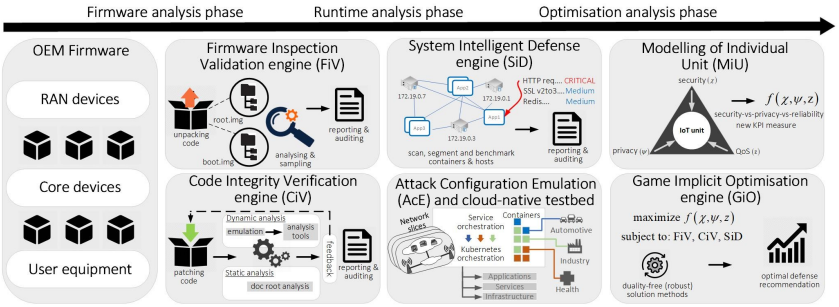

Fig. 1: Illustration of the high-level architectural logic and main components of the SANCUS solution.

an increase in system complexity. How to apply lightweight distributed network analysis into each container to assess the robustness of the running software, so as, the DevOps complexity can be shortened and provide continuous delivery with high software quality in real-time is a non-trivial question, which will be answered by this component.

Revolutionary modellings of the IoT unit: Typically, the IoT device QoS reliability is evaluated at the communication level by traffic bit rate, packet delay and packet loss rate [2]. On the other hand, security and privacy are highly conflicting to each other and influential to the aspects of QoS reliability at both communication and service levels, evaluated by communication protocols, cryptographic algorithms, key management protocols, attack detections and preventions, etc. SANCUS will shed light on how to approach and explicitly model the synergistic effect of security, privacy and reliability to the IoT unit and its related network applications, services and end-user QoS requirements, thus expanding and digesting new notions of cybersecurity within multi-objective security-vs-privacy-vs-reliability efficiency functions.

Automated cybersecurity performance optimisation using intelligent game implicit approach: The fairness principle is important for capturing the degree of the ICT system and its components' heterogeneity, while boosting the system performances, yet it is mostly interpreted in terms of symmetric equilibria. Unfortunately, symmetry is rather restrictive since network devices and components impose various security and privacy threats, while end-users have different application and service requirements. Instead, we will explore asymmetric equilibria via competitive game theoretic paradigms, which provide weighted-proportionally fair unit distribution with higher degree of cooperation and potentially better performances [3].

Robust computational algorithms: Trade-offs between KPIs (like security-vs-privacy-vs-reliability, energy-vs-spectral efficiency, throughput-vs-latency, etc.) are often achieved by relying on fractional optimization problems, which are commonly solved via dual programming. This component will develop novel solution methods that avoid duality gap and complex searching processes, thus helping to build robust computational algorithms and improve the processing capacity and level of accuracy of the proposed engines.

Unique cloud-native network testbed prototype: Tomorrow's networks are shown to be driven by Docker and Kubernetes technologies for better linking between the Cloud and services than traditional OpenStack-based deployments. However, neither much information is available to build such networks, nor their security has been thoroughly assessed and optimised to take advantage of the functionality of the Cloud, meaning that container risk detection and mitigation can be delayed or incomplete. SANCUS will develop a unique cloud-native network testbed that will be among the most contemporary in Industry and Academia, and integrate all the suggested engines to secure the Continuous Integration / Continuous Delivery (CI/CD) pipeline of Docker and Kubernetes from build to ship-to-run, and validate its cyber security performance under various conditions.

III. Conclusion

In this pager, we outlined the scope and main architectural elements of SANCUS, a novel cybersecurity suite to automate in-depth inspection and analysis of OEM firmware, continuous software risk assessment, adaptive modelling of the network unit and dynamic security-vs-privacy-vs-reliability efficiency optimization. We also presented those features that make our solution unique and different than existing approaches, while we provided insights in how we are targeting to address open challenges in firmware and software analysis, system intelligence and automation, game modelling, formulation of cybersecurity optimization strategies and algorithm computation challenges. We finally highlighted how to build a new testbed prototype, which will be used for the system implementation and the validation of the intended use cases. We believe that SANCUS constitutes a paradigm shift in the design of next-generation cybersecurity solutions with much potential to improve trust and confidence in our global digital ecosystem.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 952672. The content of this article reflects the author's view and the Commission is not responsible for any use that may be made of the information it contains.

References

[1] COMMISSION, T.E. Cybersecurity of 5G networks. Official Journal of the European Union 2019, 88.

[2] J. M. Liang, J. J. Chen, H. H. Cheng, Y. C. Tseng, "An energy efficient sleep scheduling with QoS consideration in 3GPP LTE-advanced networks for Internet of Things", IEEE Emerging and Selected Topics in Circuits and Systems, vol. 3, pp. 13–22, 2013.

[3] C. C. Zarakovitis and Q Ni, "Nash Bargaining Game Theoretic Scheduling for Joint Channel & Power Allocation in Cognitive Radio System," IEEE J. Sel. Areas Commun., vol. 30, no. 1, pp. 70-81, Jan 2012.

[4] Muller, L., Chrysoulas, C., Pitropakis, N., & Barclay, P. J. (2020). A Traffic Analysis on Serverless Computing Based on the Example of a File Upload Stream on AWS Lambda. Big Data and Cognitive Computing, 4(4), 38.