Security Assessment as a Service Cross-Layered System for the Adoption of Digital, Personalised and Trusted Healthcare

Evangelos Markakis
Pasiphae research laboratory,
Technological Educational Institute of Crete
Heraklion, Greece
markakis@pasiphae.eu

Yannis Nikoloudakis
Pasiphae research laboratory,
Technological Educational Institute of Crete
Heraklion, Greece
nikoloudakis@pasiphae.eu

Evangelos Pallis
Pasiphae research laboratory,
Technological Educational Institute of Crete
Heraklion, Greece
pallis@pasiphae.eu

Marco Manso
EDGENEERING Ltd.
Lisbon, Portugal
marco@edgeneering.eu

***Abstract*—The healthcare sector is exploring the incorporation of digital solutions in order to improve access, reduce costs, increase quality and enhance their capacity in reaching a higher number of citizens. However, this opens healthcare organisations' systems to external elements used within or beyond their premises, new risks and vulnerabilities in what regards cyber threats and incidents. We propose the creation of a Security Assessment as a Service (SAaaS) cross-layered system that is able to identify vulnerabilities and proactively assess and mitigate threats in an IT healthcare ecosystem exposed to external devices and interfaces, considering that most users are not experts (even technologically illiterate") in cyber security and, thus, unaware of security tactics or policies whatsoever. The SAaaS can be integrated in an IT healthcare environment allowing the monitoring of existing and new devices, the limitation of connectivity and privileges to new devices, assess a device's cybersecurity risk and - based on the device's behaviour – the assignment and revoking of privileges. The SAaaS brings a controlled cyber aware environment that assures security, confidentiality and trust, even in the presence of non-trusted devices and environments.**

Keywords— Security Assessment as a Service, Cybersecurity, Healthcare, Internet-of-Things

I. Introduction

The European population is ageing and the average lifespan is increasing, resulting in the likelihood of facing age-related illnesses, disabilities and cognitive decline. Healthcare services are already facing an increased demand that challenges their capacity to provide adequate and timely response.

The healthcare sector is exploring the incorporation of digital solutions (e.g., Information and Communications Technologies, data exchange protocols, wearables and Internet-of-Things (IoT) devices) in order to improve access, reduce costs, increase quality and increase their capacity in reaching a higher number of citizens. More specifically, hospitals and care centres can already exploit the use of smart and personalised ambient intelligence solutions that provide assisted living environments for health and wellbeing at home [1]. Enabled by unobtrusive sensors and devices (seamlessly embedded in the living environment or worn) that interact with patients and collect relevant measurements on a periodic or continuous basis – and supported by intelligent data analytics, healthcare professionals can remotely monitor patients' condition on a continuous basis and receive alerts in case of health and wellbeing deterioration signs are detected, thus allowing an early and prompt response.

However, this rich and promising ecosystem, further opens healthcare organisations' systems to external elements used within, or beyond their premises (e.g., BYOD [1] /smartphones, Apps, smart devices), thus bringing new risks and vulnerabilities in what regards cyber threats and incidents. Considering the numerous recent cyber security incidents in the healthcare sector, which have caused serious breaches and loss of personal data, it is crucial that effective cyber security tools, frameworks and policies are set in order to build trust in digital solutions and contribute to their wide adoption.

In this paper, we propose the creation of a Security Assessment as a Service (SAaaS) cross-layered system that identifies vulnerabilities and proactively assesses and mitigates threats in an IT healthcare ecosystem, exposed to external devices and interfaces, especially considering that users (e.g., patients) are not cybersecurity experts (are even "technologically illiterate") and, thus, are unaware of any security tactics or policies whatsoever. We finalise the paper by presenting an application use-case that will be used to test and demonstrate the system involving the integration of health devices operating at home, with a hospital environment.

II. Security Assessment as a Service cross-layered system

SAaaS can be integrated in a IT environment operated by institutions and provide the following features: Monitoring of existing and newly introduced devices in the network in real-time, by utilising an SDN infrastructure on top of legacy networks; Temporary and limited connectivity to new devices that join the network in a neutral network environment (e.g., Virtual Local Area Network (VLAN)), wherein testing and assessment will take place; Assessment of a device's cybersecurity risk-levels; Certification of devices against a standardized vulnerability scoring system; Assignment of connectivity/privileges to the appropriate VLAN; Authentication of services and services after their assessment; Access and privileges revocation in case abnormal behaviour is detected. In this way, SAaaS brings a controlled cyber aware environment that assures security, confidentiality and trust, even in the presence of non-trusted devices and environments.

[1] Bring your own device (BYOD) term is used to refer to equipment owned by individuals, such as smartphones and computers, but that are used nonetheless to access corporate networks.

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

The SAaaS architecture is structured into a three-layered ecosystem as depicted in Figure 1 (from [1]) and described next.

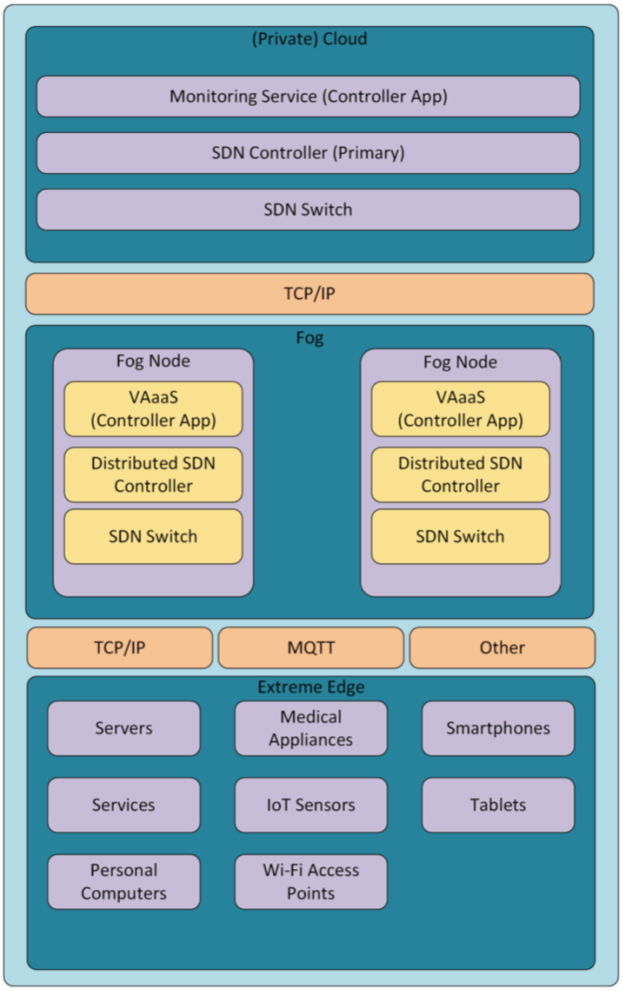

Fig. 1. SAaaS Architecture

The **Private Cloud layer** hosts the overall logic of the mechanism. It is usually physically hosted in the institution's premises. It comprises a Software Defined Network (SDN) controller that manages and controls the network of the infrastructure and the high-level network-slicing. It allows to segregate and manage multiple networks each having different privileges (like corporate, roaming, guest), thus granting and limiting access to resources and data. This layer includes the SDN-Controller - an important element in cybersecurity - that monitors and detects all connected network entities as well as newly introduced devices. The SDN-Controller also assesses and certifies a device's cybersecurity risk upon a device connection and periodically to ensure minimum risk-levels in the institution's network. The SDN-Controller has a distributed architecture, having its primary (or master) element in the private cloud layer.

The **Fog layer** serves as a distributed extension of the (private) cloud, effectively conducting all assessment and classification of network entities. It encompasses one or more Fog Nodes deployed throughout the institution's premises, each hosting an SDN-Controller relay to manage the underlying network and enforce the network slicing directed by the master controller. In the Fog layer, an SDN-Controller application (distributed element) that implements the vulnerability assessment tools and procedures (OpenVas Agent [2]) is deployed and is instructed by the master controller (hosted in the private cloud layer). The distributed SDN-Controller is used to assess a new device or conduct a periodic assessment of the network.

The **Extreme Edge layer** hosts all connected (known and newly added) entities, such as network devices, sensors, actuators, servers and virtual appliances. Herein, entities are connected to the local and remote institution's network to interact and exchange data. The connection is realised through SDN switches, or SDN-enabled access-points, duly supervised by the SDN-Controller that triggers the assessment procedure when a new device is connected.

The proposed SAaaS is based on the OpenVas framework (leveraging on the cloud-fog-extreme-edge paradigm) and considers the requirements of a novel and connected ecosystem that includes a large number of heterogeneous devices - such as IoT-based home and healthcare), network components, servers and IT appliances – a few operating outside the institution's facilities perimeter.

It ensures continuous network monitoring over existing and newly connected devices, granting (or denying) permissions based on a device credentials and determined cybersecurity safety level. Moreover, before being granted network access, new devices will be subjected to a vulnerability assessment process in a "neutral virtual LAN". In this process, a Common Vulnerability Scoring System (CVSS) standardised vulnerability scoring system [3] is determined that represents the cybersecurity safety level of the assessed device. Thus, depending on the assessment result, the device is assigned to the appropriate virtual LAN (e.g., if assessed as completely safe is granted "Full Access", if assessed as dangerous is assigned to the "No Access" virtual LAN). Moreover, vulnerability assessment process is repeated periodically to assure the network's integrity and availability.

Our proposed SAaaS considers the new paradigm of the Social Internet of Things (SIoT) that merges IoT with humans, as part of a social network. This combination, however, brings additional vulnerabilities (e.g., exploit IoT limited resources and humans through social engineering). Based on [9], we will follow the define taxonomic analysis categorised in three layers (perception, transportation and application) to identify critical elements and subsequently applying the SAaaS cross-layered system.

III. Application Case: Remote Patient Monitoring in Home Environment

As part of the SPHINX project [4], the proposed SAaaS system will be tested and demonstrated in the healthcare domain in a study that involves the integration of IoT devices operating at home with hospital processes. The integration will incorporate connected medical and health devices supporting patient care, as well as other types of ambient sensors. It aims to remotely monitor (on a 24/7 basis) patients placed in homecare environments. Accompanying hospital staff (doctors and nurses) may consult their patients' health condition and are alerted in case complications are forecasted or detected, allowing them to act upon critical patient information. The connected platform is based on EDGE's eCare [5] platform that combines connected devices (personal, home and health) in order to deliver an ambient intelligence platform aware of a patient's health and wellbeing. As such, the platform gathers a wide range of measurements acquired through sensors and devices that are seamlessly embedded in the living environment, worn or interacted with by patients.

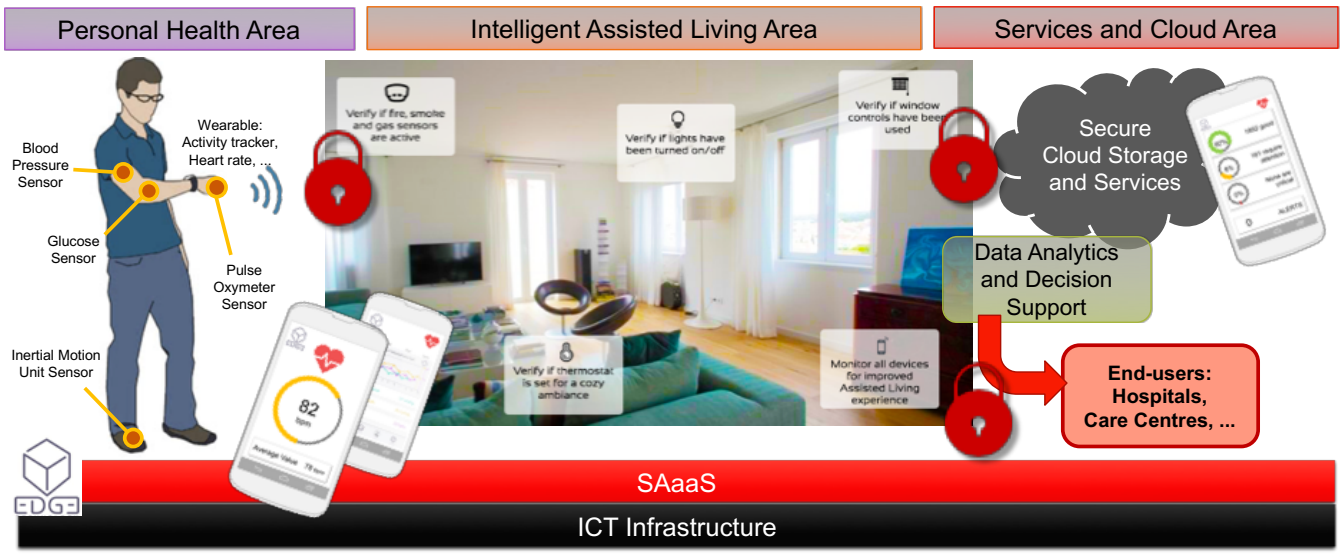

Fig. 2. EDGE eCare: Intelligent Health and Care System

The eCare platform concept to use in the study is depicted in Figure 2. The concept comprises three main areas: Personal (consisting of devices worn or interacted with by the patient, such as activity bands and heart rate sensors), Living (consisting of smart home devices, like presence detectors, smoke and gas sensors) and Cloud Services (consisting of data repositories, analytics and access). Through eCare, hospitals are able to remotely monitor patients' health and wellbeing conditions and be alerted in case anomalies are detected.

Related and complementary activities have been conducted that applied IoT platforms for health purposes. In [6], an edge computing paradigm was proposed for personal healthcare as a way to *reduce the interaction timing and the huge amount of data coming from Internet of Things (IoT) devices toward the Internet*. In this way, an edge gateway is introduced supporting multi-radio and multi-technology communications allowing collecting information from various personal devices. Moreover, the edge gateway supports local data processing capabilities (delivering fast results) while reducing data throughput. In this regard, the eCare platform complies with this paradigm by considering a 5G-ready gateway supporting heterogeneous devices and local processing [10].

In [7], an approach was proposed combining medical (e.g., blood pressure sensor) and lifestyle (e.g., activity (wearables) band) devices in order to monitor a person's physical activity, physiological parameters and nutrition aspects to detect unhealthy indicators (e.g., food disorders) and produce recommendations aiming to improve the individual's quality of life and contribute towards a healthy lifestyle. The initiative also demonstrated capability for solutions provided by different vendors to interoperate, as demonstrated as a part of the interoperability strategy of the INTER-IoT project [8]. Consequently, eCare shall pursue interoperability by allowing standardised access by third parties (having INTER-IoT as a reference) and support multiple device access (no vendor "lock"). This will contribute to a rich ecosystem of IoT devices and solutions (plug'n'play) protected by a robust security framework.

The integration of ICT systems, in-hospital connected devices and remote connected health devices at homecare environment, considering the wide SIoT dimension, brings numerous challenges and concerns in what respects cybersecurity incidents (e.g., compromised devices initiating a data flood or a denial of service attempt) and the patients' privacy, data protection, confidentiality and trust. Therefore, a SAaaS layer is introduced, supporting a distributed (cloud) environment, that provides monitoring and control over the network and all connected devices on a continuous basis, thus assuring the network's proper functioning and data confidentiality.

IV. Conclusion

The incorporation of digital solutions into the healthcare sector supported by the remote monitoring of patients in home environments is regarded as a way to overcome the increase in demand due to the prolonged life expectancy and population ageing phenomenon. However, opening the healthcare environment to external devices results in adding additional risks and vulnerabilities in what regards cyber threats and incidents. This paper suggested the creation of a SAaaS cross-layered system that identifies vulnerabilities and assesses and mitigates threats in such an environment. Developed as part of the H2020 SPHINX Project, the SAaaS will be demonstrated in a study involving the EDGE eCare platform that combines home and healthcare connected devices in order to deliver an ambient intelligence platform aware of a patient's health and wellbeing. The eCare platform will be integrated in a local hospital environment, thus allowing testing the SAaaS in realistic conditions.

Our next steps include the deploying the SAaaS system in the hospital environment and embed components in the eCare platform in order to evaluate the SAaaS capability to correctly assess the devices' cybersecurity safety level and assign the proper access levels and corresponding VLAN. Moreover, in addition to recreate cyberattacks (e.g., port scanning, DDoS), tests will include the deployment of "clean" and "compromised" devices. The main objectives of the study will be to reduce (eventually neutralise) the incidence of cyberattacks and associated reduction of the damage caused to the patients, as well as improve the security and privacy of highly sensitive patient data, in order to increase the level of trust and acceptance of remote monitoring services by patients and healthcare professionals for their own benefit.

V. REFERENCES

[1] Yannis Nikoloudakis, Evangelos Pallis, George Mastorakis, Constandinos X. Mavromoustakis, Charalabos Skianis and Evangelos K. Markakis. *Vulnerability Assessment as a Service for Fog-Centric Healthcare ICT Ecosystems*. Peer-to-Peer Networking and Applications. January 2019.

[2] DOI: 10.1007/s12083-019-0716-y

[3] *OpenVas - Open Source vulnerability scanner*. Available at: http://www.openvas.org . Accessed: January 2019.

[4] *Common Vulnerability Scoring System*. Available at: https://www.first.org/cvss/ . Accessed: January 2019.

[5] *SPHINX - A Universal Cyber Security Toolkit for Health-Care Industry*. Online project page. Source: https://cordis.europa.eu/project/rcn/220226/factsheet/en . Accessed: January 2019.

[6] https://edgeneering.eu . Accessed: January 2019.

[7] Pasquale Pace, Gianluca Aloi, Raffaele Gravina, Giuseppe Caliciuri, Giancarlo Fortino. *An Edge-Based Architecture to Support Efficient Applications for Healthcare Industry 4.0*. IEEE Transactions on Industrial Informatics 15(1): 481-489 (2019). DOI: 10.1109/TII.2018.2843169

[8] P. Pace, R. Gravina, G. Aloi, G. Fortino, Fides-Valero, G. Ibanez-Sanchez, V. Traver, C. E. Palau, D. C. Yacchirema. *IoT platforms interoperability for active and assisted living healthcare services support*. Global Internet of Things Summit (GIoTS) 2017: 1-6 (6-9 June 2017). DOI: 10.1109/GIOTS.2017.8016250

[9] *INTER-IoT: Interoperability of Heterogeneous IoT Platforms*. Online project page. Source: https://cordis.europa.eu/project/rcn/199587/factsheet/en. Accessed: February 2019.

[10] Mario Frustaci, Pasquale Pace, Gianluca Aloi, Giancarlo Fortino. *Evaluating Critical Security Issues of the IoT World: Present and Future Challenges*. IEEE Internet of Things Journal (Volume: 5, Issue: 4 , 2483-2495) Aug. 2018. DOI: 10.1109/JIOT.2017.2767291

[11] E. K. Markakis, K. Karras, A. Sideris, G. Alexiou, and E. Pallis, "Computing, Caching, and Communication at the Edge: The Cornerstone for Building a Versatile 5G Ecosystem," IEEE Commun. Mag., vol. 55, no. 11, pp. 152–157, Nov. 2017.

VI. ACKNOWLEDGEMENTS

This paper is elaborated as part of the SPHINX project that 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.