ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in CPS IoT Architectures

Sebastien Ziegler
Mandat International
Geneva, Switzerland
sziegler@mandint.org

Antonio Skarmeta, Jorge Bernal
University of Murcia
Murcia, Spain
{*skarmeta, jorgebernal*}*@um.es*

Eunsook Eunah Kim
Device Gateway
Lausanne, Switzerland
eunah.kim@devicegateway.com

Stefano Bianchi
Softeco Sismat
Genova, Italy
Stefano.bianchi@softeco.it

***Abstract*—This article presents an innovative approach to address a rapidly evolving and polymorphic threat environment related to the emergence of the Internet of Things in the global Internet, with a focus on Cyber Physical Systems, Cloud architecture and SDN/NFV technologies. The article presents the view and methodological approach of ANASTACIA research project to address this evolution. ANASTACIA researches, develops and demonstrates a holistic solution enabling trust and security by-design for cyber physical systems (CPS) based on IoT and cloud architectures.**

***Keywords*-Internet of Things; Cyber Physical Systems; Software Defined Networks; Network Function Virtualization; Cyber-security; Privacy by design**

I. Introduction

The heterogeneous, distributed, and dynamically evolving nature of Cyber Physical Systems (CPS) based on Internet of Things (IoT) and virtualized cloud architectures introduces new and unexpected risks that cannot be solved by current state-of-the-art cyber-security solutions. For this, new paradigms and methods to build security and privacy protection systems are required at the outset of the design process of IoT systems in order to reduce the need to fix flaws at runtime after deployment and to provide the assurance that the IoT system is secure and trustworthy, which result in widening the acceptance of IoT systems and services.

The main objective of the ANASTACIA [1] is to address these concerns with consideration of security development paradigm. The project develops a holistic IoT security solution including a suite of distributed trust and security components and enablers, and a holistic dynamic security and privacy seal. The details of the project concept and technical approaches will be explained in the following sections.

The remaining sections of this article are organized as follows: in Section II we give an overview of the ANASTACIA project. Technical approaches of ANASTACIA are stated in Section III. In Section IV, V, and VI, the brief summaries of the core technical concept of ANASTACIA are given in the order of building an ecosystem of treat engines, holistic approaches of security and privacy, and dynamic security and privacy seal. In Section VII, the paper gives concluding remarks

II. ANASTACIA OVERVIEW

ANASTACIA [1] is a three-years-long H2020 European research project (G.A. N731558) started in January 2017, which aims at developing a new paradigm, new methods and tools to increase security and privacy reliability in a polymorphic and rapidly evolving environment. It will be researching, developing and demonstrating a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and cloud architectures.

ANASTACIA will develop a trustworthy-by-design autonomic security framework that allows testing, validating and optimizing security, from design to deployment and maintenance. The framework relies on diverse enablers to dynamically orchestrate and deploy user security preferences, facilitate the deployment of local agents, and enforce security in heterogeneous scenarios including those based on SDN/NFV and IoT networks. ANASTACIA will ultimately facilitate the testing and vulnerability analysis of the deployed components with simple and user-friendly security policy tools. The ANASTACIA framework will include:

- a security development paradigm based on the compliance to best practices and the use of the security components and enablers (to provide assisted security design, development and deployment cycles and thus assure security-by-design);
- a suite of distributed trust and security components and enablers, that are able to dynamically orchestrate and deploy user security policies and risk-assessed resilient actions within complex and dynamic CPS and IoT architectures (online monitoring and testing techniques will allow more automated adaptation of the system to mitigate new and unexpected security vulnerabilities);
- a holistic Dynamic Security and Privacy Seal, combining security and privacy standards and real-time monitoring and online testing (to provide quantitative and qualitative run-time evaluation of privacy risks and security levels, which can be easily understood and controlled by the final users).

The ultimate challenge of ANASTACIA is to provide a solution for addressing the increasing vulnerability of today's ICTs, based on smart, highly connected and dynamic CPS, by leveraging the same dynamic distributed and connected environment to enact smart security planning, enforcement and monitoring strategies

III. TECHNICAL APPROACH

The ANASTACIA architecture includes of a set of planes as it shown in Figure 1. The data plane establishes network communication between ANASTACIA components, and the control plane manages the resource usage and real-time operation of the services. The autonomic plane enforces security mechanisms and real-time reconfiguration and adaptation of the services, while the user plane provides interfaces and tools to end-users for policy definition, service monitoring and management. The seal management plane combines security and privacy standards with real time monitoring. The following sections explain roles and functions of each plane.

A. Data plane

The network communication between ANASTACIA components is handled in the Data plane. It includes both physical and virtual network elements responsible for tasks such as forwarding the traffic according to commands and rules received by the SDN controller through the southbound API. In virtualized scenarios, it employs cloud computing technologies (i.e., computing, storage and networking) to deliver virtual Infrastructure-as-a-Service (IaaS). Special controllers are used to control devices in more heterogeneous scenarios that include IoT or low power and lossy networks (LoWPANs). Security probes or sensors are deployed in the data plane to support the monitoring services.

B. Control plane

Control plane manages the usage of resources and real-time operation of services. It controls the behavior of the Data plane via the northbound API. A set of distributed SDN controllers in the Control plane takes charge of communicating with the network elements in the Data plane. NFV compliant orchestrator performs the main orchestration in the Control plan. The NFV-compliant orchestrator supports secure placement and management of services over the underlying infrastructure. As ANASTACIA aims to cover IoT derived scenarios, it will leverage NFV and SDN by considering additional components of the IoT control component an the Physical Network Functions (PNF) component that embrace the functionality required to support management of IoT devices and covers legacy scenarios that are not NFV/SDN-enabled.

C. Autonomic plane

Autonomic plane enforces security mechanisms and real-time reconfiguration and adaptation of services. It includes: monitoring component, reaction component, security enforcement manager and security orchestrator, which provide the framework with intelligent and dynamic behavior. The monitoring component collects security-focused information related to the system behavior from the Control plane and the Data plane. Its objective is to react and adapt to the prevailing security and trust circumstances. The reaction component receives inputs, triggers or requests from the monitoring services to perform the right decisions in order to keep the asset secure with no service disruption and optimal configuration at all times. The security enforcement manager analyses the reaction outcome and oversees the interactions among objects and components in order to ensure that security requirements defined in high-level policies are met. The security orchestrator organizes the resources to support the required enforcement. It uses peer-to-peer communication with other managers and components to overcome any resource limitations or run-time issues of the security components and policy deployment.

D. User plane

User plane provides interfaces, applications, services and tools to end-users for policy definition, system monitoring and service management. Its policy editor provides an intuitive and user-friendly tool to configure security policies governing the configuration of the system and network such as authentication, authorization, filtering, channel protection and forwarding. The high level policies serve as input to the security enforcement component to facilitate the orchestration and deployment of security components and configurations required to satisfy the policies.

E. Seal management plane

Seal management plane combines security and privacy standards with real time monitoring. It provides users with a real-time indication of the overall and holistic level of trust in the system being monitored, combining normative approaches and real-time monitoring and deep integration with the ANASTACIA security orchestrator and security monitoring features. Its normative approaches include analysis and integration with standards such as the regulation of the European General Data Protection and security related ISO standards and methodologies for security and privacy labeling.

In summary, the ANASTACIA framework provides self-protection, self-healing and self-repair capabilities through novel enablers and components. It is designed to dynamically orchestrate and deploy security policies and actions that can be instantiated on local agents. It makes security be enforced in different kinds of devices and heterogeneous networks such as IoT-based networks or SDN/NFV-based

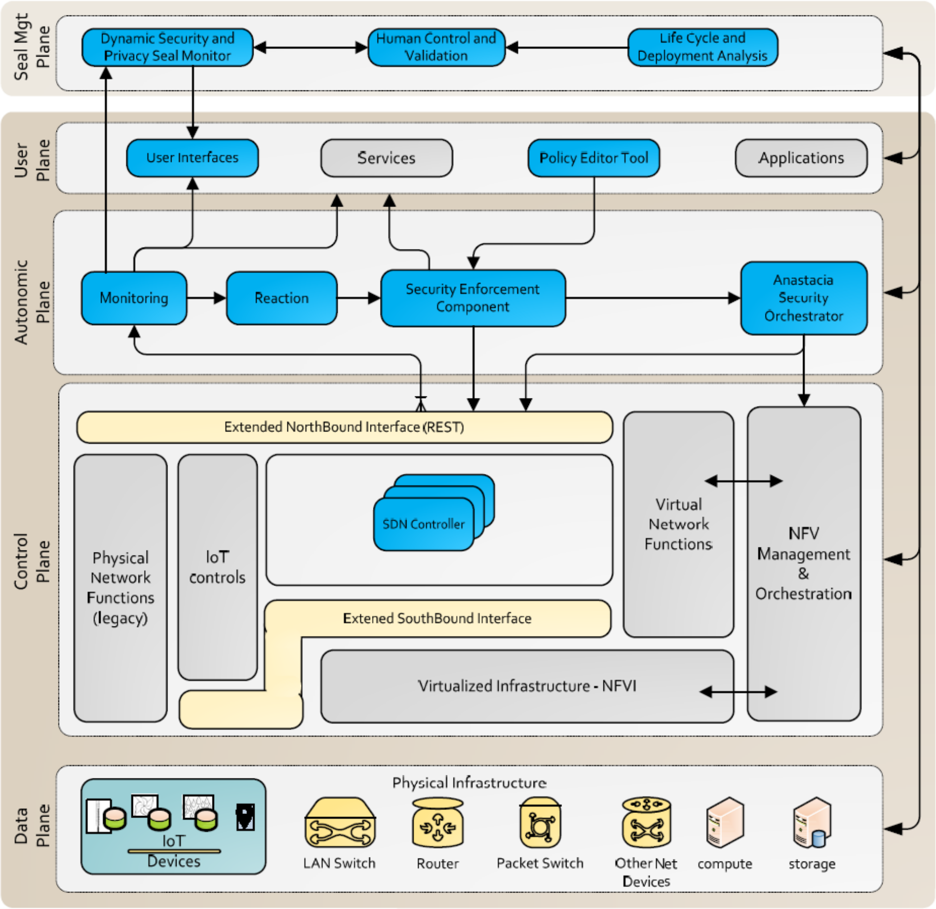
Seal Mgt Plane
Dynamic Security and Privacy Seal Monitor
Human Control and Validation
Life Cycle and Deployment Analysis
User Plane
User Interfaces
Services
Policy Editor Tool
Applications
Autonomic Plane
Monitoring
Reaction
Security Enforcement Component
Anastacia Security Orchestrator
Control Plane
Extended NorthBound Interface (REST)
Physical Network Functions (legacy)
IoT controls
SDN Controller
Virtual Network Functions
NFV Management & Orchestration
Extened SouthBound Interface
Virtualized Infrastructure - NFVI
Data Plane
Physical Infrastructure
IoT Devices
LAN Switch
Router
Packet Switch
Other Net Devices
compute
storage

Figure 1. Envisioned ANASTACIA Architecture

networks. The ANASTACIA framework is designed in full compliance to SDN/NFV standards as specified by ETSI NFV [2] and OFN SDN [3].

IV. Building an Open Ecosystem of Threat Engines

There exist several security issues that are changing the threat landscape and deserve further attention and study. Among them, we can find the leaks and breaches in communication protocol data exchange, the monitoring of limited number of protocol messages as well as the silent attackers, who generate a small amount of malicious data inside regular traffic. These issues make the detection a hard task for any traditional scheme, and therefore, require new dynamic security mechanisms. Additionally, the intrusion anomaly detection task is particularly challenging due to the diversity in form (e.g. password stealing, viruses, Trojan horses, Denial of Service (DoS), etc.) attacks exhibit. Traditional Intrusion Detection Systems (IDS) are still inadequate to face those kinds of attacks mainly because, until now, the analysis and the understanding of these attacks is quite limited to a-priori assumptions of their behavior. In current detection schemes the attacker could know in advance how detection works, meaning that sophisticated attackers might randomize their behavior to avoid detection, performing damage to a victim service.

To cope with these threats, ANASTACIA is addressing the development of different innovative cyber-threat solutions to counter cyber-threats. Anomaly detection and prevention systems facing 0-day/unknown cyber-threats are being devised to enhance the cyber threats protection capacity. ANASTACIA is working on the impact of self-adaptive attack and defense approaches in response to a-priori information available to each other. A cyclic refinement process will be adopted, following a loop of interactions between time-varying attack and defense mechanisms, which will allow to come up with more reliable detection and prevention tools.

Additionally, innovative protection algorithms are being designed in ANASTACIA to identify cyber-threats, through anomaly based intrusion detection approaches inferring certain features from live network traffic and applying techniques belonging to different fields to identify running unknown attacks (0-day) performed against specific services. These algorithms are complemented through the implementation of automated reaction components able to autonomously protect the system by integrating with the monitoring systems developed in ANASTACIA as well as developing appropriate mitigation plans able to counter identified threats.

The ANASTACIA framework will be tested, demonstrated and validated in two extremely influential business sectors: Mobile Edge Computing (MEC) and Smart Building Management.

Benefitting its proximity to the IoT devices, MEC is expecting to enable fast responses to the real-time events in the IoT domain and to perform data regulation and processing of IoT data at the edge. This, however, brings a need to orchestrate the different pieces and specially deploy and validate the different security and privacy components to fit an overall behavior. ANASTACIA will demonstrate its potential to address security threats with an example scenario, enable to add the possibility of both virtualizing the security functions, and allow the security functions to act on virtualized networks and functions. For instance, in the Mobile Edge Computing (MEC) scenario applied to IoT scenarios using video cameras, the ANASTACIA Monitoring component will enable continuous monitoring of different signals, event logs, status reports, video information, etc., in order to enable the detection of a behavior hiding a spoofing attack considering known policies, models, and threat signatures. e.g., malicious users using the MEC server IP address to obtain information from a camera. Such situations will be analyzed by the Reaction component that will evaluate the gravity of the situation. After that, isolation and predictive mechanisms will be activated to ensure that the rest of the camera security system is not affected. Policies and rules are activated, updated and enforced by the Security Enforcement component, e.g., frequently changing the MEC server IP address and making sure that trusted cameras know the new address.

Another example studied in the scope of ANASTACIA is the mitigation of threats in the Smart Buildings. In Smart building, all the electrical and mechanical devices are controlled and monitored by a centralized Building Automation System (BAS) and various types of threats to the buildings are on the rise. An obvious threat to the building is the physical damage, vandalism, attack, arson, etc., that affects various tightly integrated embedded systems in a building. Many diverse combinations of cascaded unpredictable events of the HVAC, elevator, energy management, fire-safety and security subsystems could occur. They could severely cripple most building operations and increase the hazard level immensely. Cyber-attacks to building operations are widespread because of increased internet-connectivity of equipment and devices in the building for various services (e.g., remote elevator monitoring, online energy management, offsite security management). Widespread complex integration of buildings cyber-physical systems and the accessibility of the networks in a building to potential miscreants are on the rise. Therefore, against waves of emerging and adapting threat patterns, effective security configuration for building automation systems is beyond manual analysis or human ability. It is implausible for human security administrators to have deep understanding of each security loophole of large, complex, intertwined, distributed and heterogeneous automation systems in smart buildings.

In this context, the ANASTACIA open ecosystem will develop new methodologies, and support tools that will offer resilience to building automation systems upon cyber-attacks. Various scenarios of cyber-attacks on the network of embedded systems, software systems and Internet connected devices that are part of the diverse building operations are under studying.

V. HOLISTIC APPROACH COMBINING SECURITY AND PRIVACY

Current policy-based security management solutions and models are not tailored for NFV and SDN architectures and, therefore, need to be reconsidered for these scenarios, including extended holistic scenarios that require combination of SDNs and IoT. ANASTACIA will endow end users and security experts with intuitive and user-friendly tools, models, guidelines and solutions to manage security, privacy and risk in a decentralized and virtualized architectures. To this aim, the project will carry out a deep analysis to provide a set of novel security and trust by design enablers tailored to cope with heterogeneous and holistic scenarios that may combine SDN-NFVs and IoT. Namely, policy based security management models, threat analysis and contingency mechanisms, privacy risk modelling as well as secure software development guidelines.

In this regard, the ANASTACIA will define declarative and interoperable policy modes that can be afterwards evaluated and enforced in NFV, IoT and SDN architectures. Policy models will serve as input for the Security Enforcement Manager for policy analysis and enforcement of security requirements in an end-to-end fashion. Security and privacy policies are going to be holistically enforced by the SDN controllers and the NFV MANO [4] orchestrator at the Control Plane of the system. In addition, different local agents will enforce security over devices, such as gateways and IoT devices, without specific support for SDN deployment.

The privacy risk analysis and modelling will identify measurement points as well as contingency measures to mitigate the risk. Additionally, the software development guidelines and procedures will allow developers to take into consideration the security from the design phase of their software components and systems to its implementation and deployment.

Furthermore, ANASTACIA will suggest an innovative policy-based access control framework to meet the security requirements more efficiently and more flexibly, so that:

- Access control policies are self-adaptive, based on dynamic evaluation of context and risk
- Policy intelligence is distributed across multiple decision nodes through decentralized architecture design
- Inference engines are used to support advanced reasoning about policies to e.g. find redundancies, anomalies and generate reports. As a result, the proposed mechanisms will allow devices not in hands of the organization to be easily recognized by the policy framework, acquire restricted access capabilities (only the persons owning the device can access it) and participate in the process of consuming access to another object.

VI. DYNAMIC SECURITY AND PRIVACY SEAL (DSPS)

The Dynamic Security and Privacy Seal (DSPS) provides to the end user to get an instantaneous view and understanding on the trust level of the system. The DSPS system combines real-time dynamic security and privacy monitoring with conventional certification schemes applying ISO certification models. It also combines normative requirements from General Data Protection Regulation (GDPR) [5] and ISO standards [6] [7] [8] [9]. The developing technical enablers for real-time security and privacy monitoring will be applied to monitor functionalities on provision of real-time indication on the trustability of a deployed system. It will be the first ICT-based seal addressing the new European General Data Protection Regulation (GDPR).

Starting with the analysis of the potential privacy risk from a systemic perspective, the DSPS will research and develop innovative models and solutions to prevent any risk of counterfeiting of the seal. It will make a quantitative and qualitative run-time evaluation of the quality of security and privacy risks and exploit strong authentication and block chain-based record of seal emission.

The seal is designing to be easily understood and controlled by the final users and ensure that an ICT system is secure and trustworthy by design. It provides certified levels of assurance where security and privacy are fundamental. The users will see an instantaneous view and understanding on the trust level through supporting tools with a holistic real-time view of the level of trust both in security and privacy for the system being monitored. On evaluation of the trust level of a monitoring system, the DSPS will collect the history of the system security and privacy monitoring results, and reflect the historical reliability collected over the time as well as the instantaneous state.

The Seal is expected to provide various level of trusts, including:

- Gold Seal (three stars): to illustrate systems whose monitoring indicates a secured state since 12 months without any breach;
- Green Seal (two stars): to illustrate systems whose monitoring indicates a secured state since 3 months without any breach;
- Green Seal: to illustrate systems whose monitoring indicates a secured state since less than 3 months, and the breach took less than 3hours.
- Orange Seal: to illustrate a system that have had a recent breach of more than 3 hours, in the last three months; and,
- Red Seal: to illustrate systems which are not fully reliable.

In DSPS, new models of secured certificate registry will be also researched in order to prevent the risk of counterfeiting. It will focus on strong authentication and encryption, as well as block-chain based secured data storing in order to provide the highest possible level of the confidence on the genuine and authenticated nature of the seal. The technology developed is expected to increase public trust in the system.

VII. Conclusions

The ANASTACIA project aims at providing a holistic solution for addressing the increasing vulnerability of modern ICT which is based on smart, highly connected and dynamic CPS. This objective will be pursued by leveraging the same underlying environment (dynamic, distributed and connected) to enact smart security planning, enforcement and monitoring strategies. SDN and NFV technologies will be used and improved to ensure that the holistic framework is technically implemented at different architectural levels. Results will also include a novel cyber-security labeling system based on Dynamic Security and Privacy Seal, compliant with the new European GDPR. The ANASTACIA project will be delivering a first prototype of the main functional components in June 2018, to initially test and validate the holistic framework in the two envisaged pilot cases (Mobile Edge Computing and Smart Building Management).

Acknowledgment

This article has been written in the context of the dissemination activities of the project ANASTACIA (www.anastacia-h2020.eu), which has received funding from the European Unions Horizon 2020 Research and Innovation Programme under Grant Agreement N 731558 and from the Swiss State Secretariat for Education, Research and Innovation. Authors would like to thank all project beneficiaries for the support to the preparation of this article

References

[1] “ANASTACIA project web site,” http://www.anastacia-h2020.eu, 2017.

[2] European Telecommunications Standards Institute, ETSI, “ NETWORK FUNCTIONS VIRTUALIZATION,” http://www.etsi.org/technologies-clusters/technologies/nfv, 2017.

[3] "Open Networking Foundation, ONF," https://www.opennetworking.org, 2017.

[4] European Telecommunications Standards Institute, ETSI, "Network Functions Virtualisation (NFV); Management and Orchestration ," 2014.

[5] "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016.

[6] International Organization for Standardization, "ISO/IEC 27001, Information security management," 2013.

[7] "ISO/IEC 27018, Information technology - Security techniques," 2014.

[8] "ISO/IEC 15408, Information technology Security techniques Evaluation Criteria for IT security - Part 1 Introduction and General Model," 2009.

[9] "ISO/IEC 29100, Information technology Security techniques Privacy Framework," 2011.