Towards Secure Building Management System based on Internet of Things

Alie El-din Mady*, Ruben Trapero†, Antonio Skarmeta‡ and Stefano Bianchi§
*United Technologies Research Center, Cork Ireland
Email: madyaa@utrc.utc.com
†Cybersecurity Laboratory, Atos Research & Innovation, Spain
Email: ruben.trapero.external@atos.net
‡Universidad de Murcia, Murcia, Spain
Email: skarmeta@um.es
§Softeco Sismat, Genova, Italy
Email:stefano.bianchi@softeco.it

***Abstract*—Energy management systems are used to control energy usage in buildings and campuses in order to provide reliable energy supply and maximize user comfort while minimizing energy usage. The heterogeneous, distributed, and dynamically evolving nature of energy management systems based on internet of things introduces new and unexpected risks that cannot be solved by current state-of-the-art security solutions. For this, new paradigms and methods are required in order to i) build security into the Information Communication Technology (ICT) system at the outset, ii) adapt to changing security conditions, iii) reduce the need to fix flaws after deploying the system, and iv) provide the assurance that the ICT system is secure and trustworthy at all times. This paper provides a holistic overview of designing a secure framework for Internet of Things (IoT) system, where the framework will be implemented as part of an ongoing H2020 project called ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in Cyber-Physical System (CPS) based on IoT Architectures.**

Keywords–Cyber-physical systems; Intrusion detection; Cyber-security

I. Introduction

The aim of a modern Energy Management System (EMS) is to enhance the functionality of interactive control strategies leading towards energy efficiency and a more user friendly environment. Typically, the EMS operates several building systems, such as the supervisory control and data acquisition (SCADA), which controls the smartgrid of one or more buildings, and the Building Management System (BMS), which controls the building heating demand, security system, fire alarm system, etc. Heating, ventilation, and air conditioning (HVAC) is considered to be the highest source of energy consumption in the building operation, and the systems most affecting user comfort [1].

Historically, EMS systems were installed when potential security threats were only physical. In addition, having EMS connected on a segregated network reduces the risk of cyber and remote attacks. However, the evolving in building control requires connecting EMS to Internet of Things (IoT) to optimize accurately the user needs and building operations [2]. By connecting EMS to the building communication network, the possibility of EMS cyber-attack increases, which can lead to significant financial impact. The StuxNet cyber-attack supposedly targeting a nuclear-enrichment plant (by corrupting the measurements and actuator signals) in Iran [3], and BlackEnergy malware targeting several electricity distribution companies in Ukraine [4], are concrete examples of cyber-attacks. Thus, it is crucial to make the control of EMS to be resilient against cyber-crime.

The existing frameworks for EMS consider the system integration, connectivity and optimal control performance. The cyber-security in the EMS framework is mainly performed based on running tests and benchmarks to evaluate the possible cyber-attacks and their impact [5].

As part of an ongoing research in ANASTACIA project [6], this paper aims to propose a high-level framework architecture for Cyber-Physical System based on IoT, where EMS is an application of CPS. In this framework, we develop a trustworthy-by-design autonomic security framework with testing, validation and security optimization capabilities. ANASTACIA framework combines several elements from different domains: from IoT controllers to virtual functions accessible through Software Defined Network (SDN) interfaces, orchestration of security policies and enforcement of security preferences in heterogeneous scenarios.

II. Cyber-Physical System Model

ANASTACIA CPS model provides a representation of how ANASTACIA framework can be integrated within a CPS. Figure 1 depicts the ANASTACIA system model. ANASTACIA is envisioned to enable trust and security by-design for CPS based on IoT and cloud architectures. In general terms, an IoT Infrastructure can be seen as a system with two well differentiated planes. The *Data Plane* is closer to the physical domain and is composed of IoT devices, the network that interconnect them and in general, the elements providing resources, such as servers or routers. On top of the Data Plane is the *Control Plane* that enables the management of the underlying devices. This include either IoT controllers that directly control the devices resources (sometimes even integrated in the same device) or Virtual Interfaces (i.e., VNFs) that are able to control/access to the Data Plane resources through the cloud.

IoT platforms are currently threatened by a myriad of external dangers. Advanced attacks targets IoT platforms by taking in account the existing vulnerabilities in devices with poorly managed/configured security settings (i.e., default passwords) or even by using social engineering techniques that engage users to install malwares or disclose passwords. ANASTACIA is built on top of IoT platforms to protect them against such threats. ANASTACIA is conceived as a policy based framework where system admins, at the *User plane*,

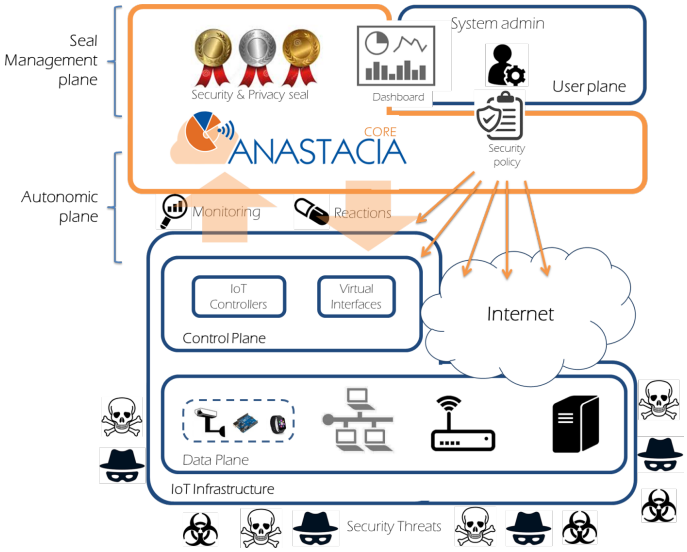

Figure 1. CPS Modeling

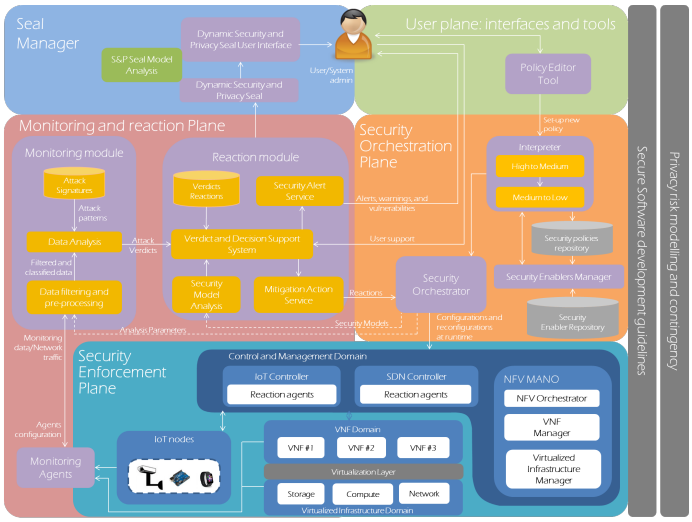

Figure 2. ANASTACIA Cyber-Security Framework Architecture

set a specific security policy that must be fulfilled within an IoT platform. This security policy is enforced within the IoT platform by orchestrating its resources (devices, services, etc.). The control of the fulfillment of the security policy is carried out by the ANASTACIA framework at the *Autonomic plane* by monitoring the IoT platform and detecting threats and ongoing attacks. Additionally, the ANASTACIA framework is able to create and trigger reactions that mitigate the effects of attacks, prevent against threats and guarantee the fulfillment of the security policy.

One of the most novel features of ANASTACIA is carried out at the *Seal Management plane*, built on top of the ANASTACIA framework. At this plane, a dynamic seal is created, representing the current level of security of the IoT platform.

III. Cyber-security Framework Architecture

The ANASTACIA system model (as presented in Figure 1) is structured as a set of layers that provide a broad view of the framework and stand out its integration within IoT infrastructures. ANASTACIA is envisioned as a framework built on top of an IoT infrastructure where network elements, physical and virtual network elements interact in the Data Plane. The interaction with these elements is done by using virtual interfaces with cloud computing networks for the usage of external resources (such as computing or storage). On top of that, the Control Plane manages the Data Plane by using APIs and by orchestrating Network Function Virtualization (NFV).

Figure 2 represents ANASTACIA framework, which extends the ANASTACIA system model by expanding the functions of the ANASTACIA core. The Autonomic Plane includes the components that provide the ANASTACIA framework with its intelligence and dynamic behavior. This plane can be divided into three sub-planes, which carry out specific activities within the framework as follows:

- **Security Orchestrator Plane** organizes the resources that support the *Enforcement Plane*, carrying out activities such as the transformation of security properties to configuration rules and aligning the security policies defined by the security interpreter with the provisioning of relevant security mechanisms. It has the whole vision of the underlying infrastructure and the resources and interfaces available at the *Security Enforcement Plane*.
- **Security Enforcement Plane** connects the ANASTACIA core with the IoT Platform, managing the interactions among objects and components for the enforcement of the security policy defined at the *User Plane*. This plane supports the enforcement of configurations and reactions triggered by the *Security Orchestrator Plane*, in order to preserve the expected security level. At this plane the agents that support the monitoring of IoT devices or the enforcement of reactions are instantiated, either if they are operating on remote or directly attached to the device.
- **Monitoring and Reaction Plane** connects to the IoT Platform through the *Security Enforcement Plane* in order to collect security-focused information related to the system behavior. At this plane, intelligent data-driven automated and contextual monitoring of activities at embedded devices, legacy systems and IoT devices by retrieving signals, event logs, traces, heartbeats signals, status reports or operational information. This plane also evaluates the fulfilment of the security policy by checking security models or threats signatures, detecting anomalies and creating reactions to mitigate such anomalies, in terms or reconfigurations and alerts to system administrators [1] [7].

Additionally, on top of the architecture the *User Plane* and the *Seal Management Plane* interact with the Autonomic plane:

- The User Plane includes interfaces, applications and tools that help system administrators to manage the IoT platform through the ANASTACIA framework. For example, at this plane system admins are able to edit the security policies that govern the underlying IoT platform.

- The Seal Manager is in charge of providing users with a real-time indicator of the overall security level.

The high level architecture can be used to identify the main activities to be carried out by the ANASTACIA framework, which is used to identify the specific components that are part of every identified plane. By analysis several use-cases for EMS application, we can identify five main activities to be supported by the platform:

- **Security policy set-up** This is the initial process triggered once a security policy has been defined by the user. In this process the policy has to be configured in the platform in order to be enforced. The interpretation of the security policy claims, the configurations required to monitor the security controls associated to a policy or the definition of thresholds to identify policy violations, are some activities carried out by this process.
- **Security policy orchestration** Once the policy has been set-up, it is necessary to enforce the controls specified at the policy. The interfaces and IoT controllers must be orchestrated according to the security policy.
- **Security monitoring** In this process the monitoring information is extracted from the devices through monitoring agents and according to the security controls interpreted from the security policy. In this activity, the monitoring data is filtered and aggregated in order to carry out its analysis and the detection of anomalies.
- **Security reaction** In this process, the detected anomalies are evaluated to design counter measures in order to mitigate the effects of attacks and potential threats.
- **Dynamic security and privacy seal** In this process, relevant information about detected threats, monitored information is evaluated to create a seal that determines the level of security guaranteed/offered by an IoT platform.

IV. ANASTACIA Framework Validation

In order to perform quick, scalable and automated testing over the architecture several interconnected virtual machines have been deployed covering the functionality for policy enforcement over IoT and SDN integration, specifically, the test has been realized for the isolation sensor use-case. As shown in Figure 3, the deployment includes the next seven virtual machines or isolated containers like docker:

1) IoT Application.
2) Micro Orchestrator.
3) SECURED Policy Interpreter.
4) ONOS SDN Controller [8].
5) OpenDayLight SDN Controller [9].
6) Open Virtual Switch.
7) Contiki emulator [10].

The idea of the scenario is that the *IoT Application* can establish communication with a mote using a global IPv6 address and the communication can be interrupted through the enforcement of security policies applied by the *SDN controller*. To this purpose we have develop a little python script for the *IoT Application*, a python micro orchestrator

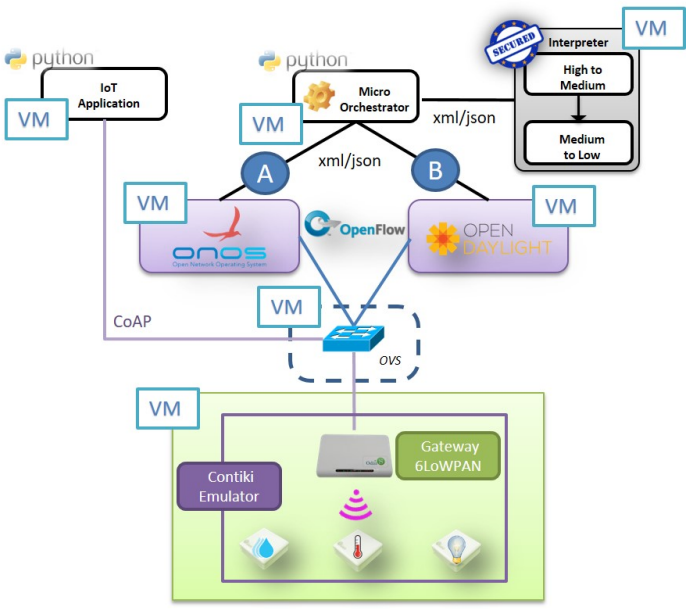

Figure 3. ANASTACIA Virtual TESTBED Deployment

and basic SDN plugins on the interpreter (for each of the mainstream controllers, this is *OpenDayLight* and *ONOS*). For the IoT application, the script sends sporadically CoAP request messages to the motes using global IPv6 addresses as source and destination. The CoAP message is received by the SDN Network (the OVS instance in this case) and forwarded to the virtual machine that contains the *Contiki* emulator. The *Contiki* emulator provides the capability to deploy a gateway between the 6LoWPAN network and the host virtual machine network, so the CoAP message is received by the Gateway and forwarded to the mote. During the communication, we decide to isolate the sensor, so we start in the *micro orchestrator* the policy enforcement. The *micro orchestrator* sends a refinement request to the interpreter and after the high to medium refinement process, the interpreter transforms the policy on a SDN configuration. At this point we can to use *ODL-SDN* plugin or *ONOS-SDN* plugin in order to get the appropriate configuration for the selected platform. Once the policy refinement process has been finished, the *micro orchestrator* receives the SDN configuration file and invokes a specific call for the *SDN controller's* Northbound API according to the controller election. Specifically, for the sensor isolation use case we are installing a flow rule on the OVS indicating that all traffic containing the sensor's IPv6 address must be dropped.

We are currently working on the integration of the virtual IoT environment with the physical one, this means, allowing the connectivity from/to the emulator to leave the machine and be connected to a real SDN deployment. Therefore, the emulator could speak with real IoT devices or mimic them so that the SDN could redirect an attacker to a cloned scenario like a honeynet.

V. Conclusion

The paper has presented a preliminary design of secure framework for cyber-physical system based on IoT. The design

of the framework was derived by energy management system, which can be a critical CPS application considering safety critical infrastructure, such as hospitals, airports, etc. The novelty of the framework is based on the integrating and the coordination of serval security stages, leading to (semi) automatic security platform for CPS based IoT system. The future work under ANASTACIA project will focus on developing each component of the framework and validate it with different applications of CPS.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731558.

REFERENCES

[1] K. Paridari, A. Mady, S. L. Porta, R. Chabukswar, J. Blanco, A. Teixeira, H. Sandberg, and M. Boubekeur, "Cyber-physical-security framework for building energy management system," ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), April 2016.

[2] D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot considerations, requirements, and architectures for smart buildings—energy optimization and next-generation building management systems," IEEE Internet of Things Journal, vol. 4, January 2017, pp. 269–283.

[3] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," Survival, vol. 53, 2011, pp. 23–40.

[4] O. Available. Blackenergy. [Online]. Available: http://www.securityweek.com/blackenergy-group-uses-destructive-plugin-ukraine-attacks (2015)

[5] S. Gold, "The scada challenge: securing critical infrastructure," Network Security, vol. 8, 2009, pp. 18–20.

[6] [Online]. Anastacia h2020 project. [Online]. Available: http://www.anastacia-h2020.eu/

[7] A. Mady, D. Mehta, D. M. Shila, and M. Boubekeur, "Towards resilient cyber security for embedded devices on internet," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (2016), vol. 0, Dec. 2016, pp. 1–2.

[8] [Online]. Open network operating system (onos). [Online]. Available: https://www.sdxcentral.com/projects/on-lab-open-network-operating-system-onos/

[9] O. (ODL). opendaylight sdn. [Online]. Available: https://www.opendaylight.org/

[10] Contiki. Contiki: The open source os for the internet of things. [Online]. Available: http://www.contiki-os.org/