Cybersecurity in ICT Supply Chains

Subjects: Computer Science, Information Systems

Contributor: Xavi Masip-Bruin

According to the US National Institute for Standards and Technology (NIST), cyber resilience is defined as “the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources”. The specific demands of supply chains built upon large and complex IoT systems, make it a must to design a coordinated framework for cyber resilience provisioning, intended to guarantee trusted supply chains of ICT systems, built upon distributed, dynamic, potentially insecure, and heterogeneous ICT infrastructures. Today, the resilience of ICT systems is premium, and every ICT system is expected to implement at least a set of basic mechanisms to prevent, resist, and recover from any type of disruption in a timely manner, thus minimizing the impact on service quality and user experience. Particularly in complex ICT supply chain scenarios, the ICT implementation of physical supply chains, serving multiple actors in finance, manufacturing, healthcare, and many other sectors, not only individual parts of the supply chain need to be secured and reliably provisioned, but also the end-to-end process of securing the ICT supply chain. The concept of cyber resilience is expected to become the norm, and one of the key measures of an ICT system’s ability to continue its operations in the event of a cyber attack (be it either software or hardware) or incident.

Keywords: cybersecurity ; supply chains ; IoT systems

1. The State-of-the-Art

1.1. Information Security Assessment

Information security assessment (or cybersecurity assessment) can be defined in different ways, according to the standards already available (mainly from ISO/IEC, CEN, and NIST). Some of them are focused on the devices’ security requirements accomplishment, others on the environment’s threat levels, and others on the effectiveness of the security control in place [1]. Those standards also help to characterize the assessment process, usually based on the technical analysis of the components (including vulnerability analysis), working tests (typically taking the component as a black-box), or just surveying functioning perception by operators [2]. Whichever method is used, a key central issue is always the quality of the metrics used (frequently constrained by observability). In fact, the security metrics problem has been researched in the last years and, despite some solutions for particular cases (such as smart grids or nuclear plants), there are no recognized generic models satisfying most implementations, particularly those where system diversity is the main characteristic, such as in the IoT paradigm [3][4][5].

A good metric should have some fundamental properties (i.e., objective, measurable, attainable, repeatable, accurate, and time-dependent), and it can be linked to several system dimensions, such as networks, software, users, and policies, eventually with a more fine-grained sub-classification scheme [4][5][6]. Several scientific contributions addressing the metric definition problem may be found in the literature, from ontological classification schemes to models supporting the metrics definition, such as the MDGSM (method for designing good security metrics) [4]. The subject was also targeted by well-recognized standards (e.g., ISO 27004 and NIST SP 800-53), which normally include application guides [7][8]. Finally, there are some attempts to use more complex multi-criteria solutions that explore relations and dependencies between different metrics, aiming to improve the decision-making process [9]. However, none of the aforementioned works can support an efficient set of metrics addressing the complexity and diversity present in IoT-based solutions.

1.2. Policy-Based Systems

Networks are traditionally configured (and reconfigured) manually, or with a very limited support from automatic tools. The rapid adoption of new IoT technologies has furthermore increased the ever-growing complexity and heterogeneity of modern IT infrastructures. Having a fully protected and efficient network in this scenario is thus becoming increasingly difficult, requiring the use of automatic tools to handle it in a timely and error-free manner.

To ease the pain of configuring a network, the introduction of systems that can automatically refine high-level security policies into either specific configurations or lower-level policies, has been already proposed in the current scientific literature. Very few papers exist on this subject [10][11][12], and the adoption of an automatic refinement workflow in production systems has been scarce to non-existent for several reasons. First, automatically translating high-level policies to lower-level policies or configurations is pretty difficult and requires a significant level of intelligence, unless the policies are very simple, or the landscape has a trivial architecture. Intrusion prevention systems (IPS), such as Snort [13] and Suricata [14], can be thought as a form of simplified policy refinement system, since they can be effectively configured to automatically use different reaction policies when an attack is detected. Despite the adoption of IPS solutions in production environments, their “refinement engine” only limits their usability in situations when the countermeasure is nearly trivial (e.g., drop all the suspected attacker packets). Second, translating a policy is not enough in complex scenarios. Once a set of security configurations is generated, it is also important for this set to be deployed in the right order, to prevent a temporary insecure state where the network security level may be too low. Virtually, no policy refinement system, as of today, offers this capability.

1.3. Trust Monitoring

Traditional strong integrity verifications of IT infrastructure nodes are performed on physical nodes via the remote attestation procedure. This procedure was standardized by the Trusted Computing Group [15], as a method to provide hardware-based integrity verification of an IT system, via an ad hoc chip named the TPM (trusted platform module). This strategy allows the continuous checking of the status of the software, services, and configurations deployed on a host [16] [17]. This approach is, however, not necessarily ideal in highly virtualized environments, where most of the jobs are running into virtual machines and, especially, containers (lightweight virtual machines). In using this approach, in fact, virtual machines can be attested at deployment time, but cannot at runtime though.

While remote attestation allows the verification of the integrity of the software only, it cannot be used to check the traffic forwarded through the network. The classic way to detect unauthorized changes to the traffic flows is to make use of secure channels via specific protocols, such as TLS [18] or IPsec [19]. Although all these technologies ensure the confidentiality of a transmission (via encryption) or its authenticity/integrity (via digital signatures or MACs), unfortunately they do not verify if a packet was effectively sent, received, or traversed all nodes it was supposed to go through.

1.4. Authentication and Authorization/Security Requirement Management

It is widely accepted that the characteristics inherent to devices located at the edge of the network (such as the IoT devices) are making it difficult to provide security guarantees to their users, thus potentially hindering a large adoption of such devices to support innovative services. Although some contributions addressing this problem may be found in the literature, such as, for example, solutions based on the physical unclonable functions (PUF) concept [20], additional research efforts are still needed to suitably handle aspects such as the device mobility, heterogeneity, and low computing capacity, which may add serious risks to all scenarios where these devices are to be deployed. Thus, any system, platform, or solution leveraging IoT devices to run services must support several security requirements as those listed below [21]:

- Authentication: Edge devices must be authenticated to both the cloud (upper layer) and other edge devices (lower layer), allowing only authorized nodes to communicate and retrieve data. One of the main challenges here is to authenticate constrained IoT devices.
- Secure data sharing and data aggregation: Data sharing between the edge and cloud must be encrypted, and data aggregation in intermediate layers must be similarly managed. However, handling data sharing and aggregation in a distributed way demands for a novel security management approach to be designed.
- Secure service discovery: In order to only provide services to authorized users, services must be discovered and delivered in a secure manner, to avoid fake users and fake nodes.
- Malicious nodes detection: Distributed nodes are vulnerable to external and internal hardware or software attacks. Hence, a mechanism is needed to detect malicious nodes.
- Secure virtualization: Nodes must provide a secure virtualization environment to avoid malicious virtual machines, virtualization attacks, as well as to prevent an attacker to take control over either the hardware or the operating system, to launch attacks.

All these requirements must be met in a highly heterogeneous environment, where multiple nodes (IoT devices) are unstoppably joining and leaving.

1.5. Threat and Anomaly Detection

The automatic detection of traffic anomalies and network cyber attacks is not a novelty. Intrusion detection systems (IDS), such as Snort, Bro [22], and Suricata, are frequently used in production IT infrastructures. They usually detect threats by looking at specific patterns in the traffic, using advanced pattern matching rules. IDS are not trained, but are configured by experts with ad hoc pattern matching expressions, thus limiting their effective usage for at least two reasons. On one hand, writing detection rules for new attacks requires a significant amount of expertise and knowledge about a threat. On the other hand, zero-day attacks and recently discovered ones can pass through an IDS undetected, unless their fingerprint is very similar to another one in the intrusion detection system internal database.

To overcome such limitations, the current scientific literature started using supervised and unsupervised machine learning approaches to provide trainable attack detection tools with high accuracy. However, the current state-of-the-art is mostly focused on detecting anomalous traffic [23], without classifying the attacks, and the few articles devoted to attack classification are mostly limited to denial-of-services and volumetric attacks [24], as well as hazard detection and differentiation [25].

1.6. Threat Intelligence and Information Sharing

Security information and event management (SIEM) solutions aim at providing real time analysis and management of security alerts. They are commonly used in production environments, to have a global picture of the security status of an IT infrastructure, and can allow administrators to perceive a threat before it can maximize its damage [26].

Despite that Internet of Things devices are starting to become ubiquitous, unfortunately, traditional SIEM systems have limited capacities to interface with IoT devices and embedded systems. Consequently, research efforts are required to facilitate SIEM operations in IoT-based scenarios. One potential improvement may reside on minimizing the number of possible false positives, through improving SIEM import capabilities by facilitating SIEM to receive relevant structured data from multiple data sources. To this end, MISP (malware information sharing platform), along with the addition of the trust and reputation module, which will perform the needed analysis and enrichment before injecting the data into the SIEM itself, may be adopted. Another area of improvement would refer to the possibility of extracting new IDS rules from these enriched events through MISP, later to be dynamically sent to the SIEM, thus exploiting the built-in sharing capabilities of the former.

1.7. Identity Management and Accountability

The current identity management (IdM) systems are mostly based on centralized solutions, such as corporate directory services, domain name registries, federated services, or certificate authorities. However, these approaches are facing several issues, being fragmented and siloed between various service providers, thus limiting the adoption of a holistic view and delivering poor user experience. The upcoming reliance on billions of IoT devices makes it untenable to have all those devices controlled by a centralized identity provider, since a breach of this provider would be disastrous not only for revealing personal data and misallocation of virtual resources, but also for attacking the physical infrastructure, including the IoT devices.

The emergence of distributed ledger technology (DLT) offers a promising solution, easing the deployment of fully decentralized identity management strategies [27]. This technology pushes the ownership of identity away from centralized services to the edges, i.e., to individuals, so that the identities themselves are in control [28]. In this way, distributed ledgers provide a mechanism for managing a root of trust, with no need for a centralized authority, thus removing the single point of failure issue. Recently, DLT-based IdM solutions have been classified into the following two main categories: self-sovereign digital identities and decentralized trusted identity. The solutions in the first category offer self-sovereign identity through block-chain technology, where the owner has control over what information they share, without any external administrative authority [29]. Differently, the second set of applications offers a centralized service that provides identity proofing through existing identifications, such as a passport and driving license. With respect to the self-sovereign approaches, there are already a few of them providing authentication and authorization capabilities. Bitid [30] is an open protocol that allows simple and secure user login to cloud/web services, by authenticating the user based on the public key and block-chain-based network. The authentication proves the identity of the user to a service by signing a challenge. OpenID [31] is an open protocol that allows a user to authenticate to multiple services without the need for creating multiple different identities and passwords. It provides one unique identity to the user from some trusted identity provider, which can be used to sign into other OpenID-enabled services. Based on OpenID, NameID [32] is an experimental technology, which allows a user to register names that can be associated with the user data. These data can be verified by everyone in the block-chain network, but cannot be forged or censored by unauthorized attackers, and no one can

retrieve the data without explicit user consent. Finally, uPort [33] is a platform that allows end users to establish a digital identity, which can be used as a user identity across multiple services, without any password. It gives full control of the user's sensitive data to the user, by allowing users to own and control their digital assets, as well as to securely and selectively disclose their data to counterparts to access digital services. Moreover, it allows users to digitally sign and encrypt documents, data, messages, transactions, and to send these contents over the distributed ledger network to interact with decentralized applications.

1.8. Intent-Based Services

The automatic network management can reduce the network administrator's tasks (network configuration, configuration change, etc.), and may leverage the concepts of policy or intent.

Policy-based network management (PBNM) [34] is a technique that enables the updating of network configurations with network administrator's policies. PBNM enables policies to be defined, which manages network resources and ensures that network resources are appropriately allocated to users. Policies are formulated using the event–condition–action (ECA) rule and are described using the "if condition then action" rule. The common open policy service (COPS) [35] protocol has been standardized in the Internet Engineering Task Force (IETF). It has a simple query and response form, and it exchanges policy information between a policy server and its clients. Recently, the Simplified Use of Policy Abstraction (SUPA) working group has discussed data models of policies in the IETF. In the conventional management of network states, the simple network management protocol (SNMP) has been widely deployed based on a request–response form. Recently, the network configuration protocol (NETCONF) [36] has been discussed in the IETF NETCONF working group. The NETCONF is a management protocol for correcting the states of network devices and updating their configuration, and is based on an XML form. Yet another next generation (YANG) [37] is a data modelling language that is used to design configuration and state data on the NETCONF protocol.

The concept of intent-based networking (IBN) has been proposed as a new network management framework in OpenDaylight network intent composition [38]. An intent-based interface has been pursued rigorously by IETF, and major open-source project communities (ONF [39], ONOS [40], and OpenDaylight [41]) are working to provide a standardized intent-based northbound interface for SDN. An intent of a network administrator is used to be expressed in the concrete description of configurations stored on devices, to update configurations. To describe the intent, the concept of the intent-based network modelling language has been discussed in IETF IB-Nemo [42] BoF, and a draft specification and implementation of it is developed in the NEMO project [43][44][45]. Another specification method was also developed by policy graph (e.g., PGA [46]).

1.9. Artificial Intelligence

Network management and orchestration can require real-time (i.e., latency around milliseconds) complex decision making as softwarization and virtualization of network resources. Using artificial intelligence (AI) techniques enable historical, temporal, and frequency network data to be analyzed. Indeed, artificial intelligence techniques, especially machine learning (ML) and statistical learning algorithms [47], can help the FISHY framework to be intelligent as well as autonomous, i.e., to make network self-aware, self-configurable, self-optimization, self-healing, and self-protecting systems [48]. Simultaneously, the AI-enabled functionalities taking advantage of intent-based networking, NFV, SDN, network slicing, and security, will enable cognitive network management for 5G and beyond. The current development of network management solutions, including CogNet, Selfnet, SONATA, and 5GeX [49], are focused on cognitive network management for 5G devices. Thus, the work towards beyond 5G management solutions would require an optimizing network as an entity in a secure, resilient, and cognitive IoT-fog-cloud infrastructure, taking advantage of in-network computing and communication to minimize the overall energy footprint. However, the success of an intelligent and autonomous system is defined by the AI techniques that can effectively be adopted in different parts of the network management infrastructure. Thus, the intent orchestrator needs to provide not only the handcrafted policies, but should also utilize the power of big data and computing dynamic resources, making intelligent decision based on the processed data near the end users, providing low latency, as well security, as required by critical surveillance, medical applications, and many commercial applications [50]. Moreover, the work proposed in this paper, towards defining the FISHY architecture, will exploit natural language processing (NLP), i.e., the science of extracting the intention of text and relevant information from text, to support the management of intents by the intent-based resilience orchestrator block. Some popular "NLP as a service" platforms are as follows: (i) LUIS.ai [51] by Microsoft; (ii) Wit.ai [52] by Facebook; (iii) Api.ai [53] by Google; and (iv) Watson [54] by IBM.

For the sake of illustration, **Table 1** summarizes the review of the art in the research fields related to the proposed cybersecurity solution.

Table 1. Relevant research areas for IoT complex supply chains including current advances and key issues.

Research Area	State-of-the-Art	Key Issues
Information Security Assessment	**Device security requirements, environment threat levels, assessment process characterization**	**Quality of security metrics, metrics properties, general model**
Policy-based Systems	**Traditional manual configuration or some tools for limited automatization**	**Full protected scenario, high- to low-level policies translation in non-simple scenarios, configuration orchestration**
Trust Monitoring	**Remote attestation procedure (TPM)**	**Considering virtualized environments, traffic attestation (at packet-node level)**
Authentication and Authorization	**Edge devices security provisioning is an open challenge**	**Different authentication levels considering constrained edge systems, distributed data sharing, secure nodes discovery, secure virtualization**
Threat and Anomaly Detection	**IDS is commonly deployed in IT infrastructures**	**No trained systems rather limited configurable systems, using ML for training**
Threat Intelligence and Information Sharing	**SIEM solutions**	**Current SIEM limitations to face IoT systems, using MISP**
Identity Management and Accountability	**Centralized solutions, recent DLT-based IdM solutions**	**No holistic view, exploit existing solutions to edge systems**
Intent-based services	**Current automatized management solutions based on policies or intents**	**Deploy intent-based solutions to orchestrate security actions in a human friendly scenario**
Artificial Intelligence	**Several network management solutions and NLP platforms exist, benefiting from AI**	**Adopting AI to facilitate overall system smartness and autonomy, considering intents orchestration and NLP, deciding where decisions should be taken**

2. Architecture for Cybersecurity Provisioning

2.1. Concept and Approach

The proposed FISHY architecture aims at delivering a coordinated cyber-resilient platform that would provide the appropriate set of tools and methods towards establishing trusted supply chains of ICT systems, through novel evidence-based security assurance methodologies and metrics, as well as innovative strategies for risk estimation and vulnerabilities forecasting leveraging state-of-the-art solutions, leading to resilient complex ICT systems, comprising the complete supply chain, particularly focusing on the IoT devices at the edge and the network systems connecting them.

Addressing the challenges 1 to 5, the proposed architecture is not envisioned as an incremental integrated cybersecurity solution, but rather as an extensible and programmable framework that can flexibly orchestrate the whole set of ICT systems and security controls. The aim is to provide an innovative cyber resilience framework, where complex ICT systems performance in an entire supply chain may be analyzed, in terms of the security, trust, and privacy impact on performance. To this end, the proposed architecture seamlessly combines advancements in several domains, including software-defined networking (SDN), network function virtualization (NFV), intent-based networking, AI-based techniques, and distributed ledger technologies (DLT).

The high-level architecture is depicted in **Figure 2**, where the entire supply chain, including the involved stakeholders, is also shown. Each stakeholder participates in the supply chain through resources and infrastructure, from data to IT infrastructure, either as provided by the stakeholder itself or reachable through other stakeholders via core network and clouds. The main concept relies on designing a security, trustworthy, and certification layer, transversal to the whole set of stakeholders in the supply chain, intended to make the entire ICT supply chain system resilient, but also to correctly measure the complete security compliance and consequently trigger the required actions (mitigation, reconfiguration, etc.), making sure that guarantees for a certain level of cyber resilience are provided. It is worth mentioning that the proposed solution is envisioned to be deployed on the entire set of devices and systems in the supply chain, most notably including the IoT ecosystem. The latter includes heterogeneous IoT devices at various localities and assumes their connections to gateways or hubs, edge, and cloud systems, as well as the network infrastructure to connect them all. **Figure 2** also introduces the proposed functional architecture, where the following four principal functional modules are proposed: intent-based resilience orchestrator and dashboard (IRO), security and certification manager (SCM), trust manager (TM), and the secure infrastructure abstraction (SIA). The figure also shows the key blocks within the SCM module, namely, the secure assurance and certification management, and the enforcement and dynamic configuration, as

well as the trust and incident manager, and the security and privacy data space infrastructure, both into the TM module. Starting from top to bottom, the intent-based resilience orchestrator and dashboard (IRO) module is designed to work as the user-centric interface, which is responsible for translating and orchestrating input actions into intents, to be used by other components. The security assurance and certification management is responsible for the provision of the auditable, evidence-based evaluation and certification of the assurance posture of complex ICT systems, based on identified security claims and metrics, setting the roots for the definition of a pan-European process for the certification of devices, processes, and systems, as required in today's European market. The trust and incident manager provides tools for assessing the security of the stakeholder's device, component or/and system. The enforcement and dynamic configuration block is responsible for making the entire system cyber-resilient, even when including potentially insecure components, based on the concepts of dynamic self-configuration. The security and privacy data space infrastructure is responsible for the collection and storage of data generated from the devices, processes, and components of the stakeholders' ICT systems, being part of the supply chain. Finally, secure infrastructure abstraction (SIA) is the infrastructure-centric interface, and it works as a data interface between different edge/IoT or cloud infrastructures and the FISHY platform.

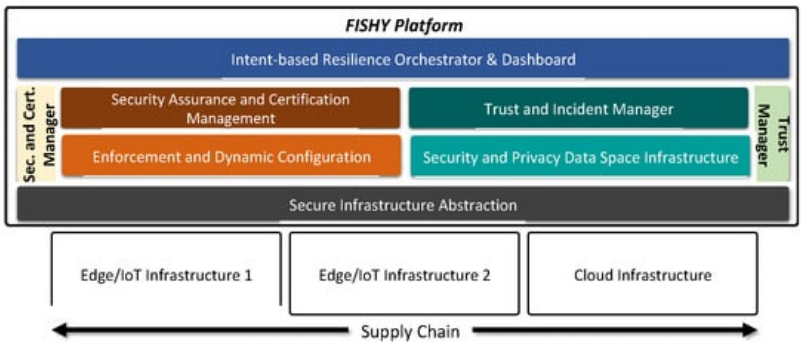

Figure 2. The technical overall concept.

A more detailed description of each individual module in the architecture is depicted in **Figure 3**, also including the interaction with the infrastructure along the whole supply chain. Indeed, the whole set of individual components within the modules and blocks defined in **Figure 2** are represented in **Figure 3**. Each module, block, and component are described next, to facilitate the overall understanding.

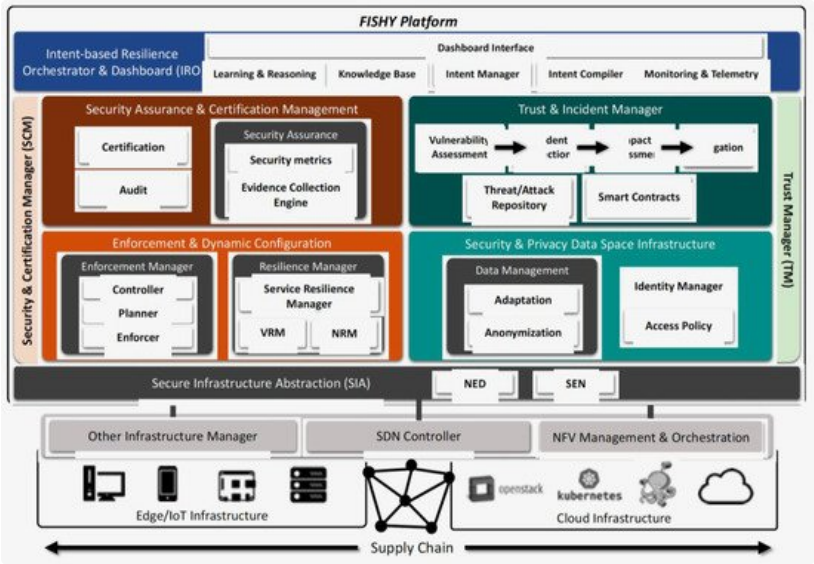

Figure 3. FISHY functional architecture in the entire ICT system.

2.2. Intent-Based Resilience Orchestrator & Dashboard (IRO)

The intent-based resilience orchestrator and dashboard (IRO) aims at automating the processing, storage, and management of intents, using natural language processing (NLP) into security workflows, which will be translated to security functions within the FISHY architecture. The processing and optimization of intents use AI, while keeping the human-in-the-loop, depending on the desired level of automation, in order to control and enforce a specific workflow that is able to react to new threats. The intent-based resilience orchestrator is divided into six main components, the dashboard interface, learning and reasoning, the knowledge base, the intent manager, intent compiler, and monitoring and

telemetry. The main objective of the dashboard interface is to provide a unified, harmonized, and consistent application, interfacing the human serving as security administrator and the FISHY platform, showing as services, high-level policies, risks and vulnerabilities exposure, warnings, performance, metrics, etc. The inputs entered by the users of the dashboard will be managed by the rest of the components in the IRO. The learning and reasoning module receives rules or metrics from other blocks (e.g., TIM) and uses AI techniques to learn from the experience acquired in previous executions (e.g., considering how the ICT systems react to security alerts, which policies fit better to different scenarios, and learning from feedbacks from other modules), to predict the best decisions to be made, and to help the FISHY administrator understand which policies to choose. This component generates recommendations for the infrastructure operator, to drive automation to dynamically fix policies and optimize the performance of the intent manager. The knowledge base stores the relation between intents, corresponding workflows, and security policies. The intent manager is responsible for handling the intents, while checking the conflicting policies and guaranteeing the optimal implementation, depending on the dynamic rules chosen by the infrastructure operator. The intent compiler deploys the configuration obtained from the intent manager and will feed other modules in the FISHY architecture. Finally, unlike the current commercial solutions, our implementation of the monitoring and telemetry component is as follows: (i) able to dynamically monitor deployment changes enforced by continuous dynamic scheduling, provisioning, and auto-scaling; (ii) lightweight, yet effective and non-intrusive; and (iii) independent of any specific infrastructure technology. FISHY will containerize a monitoring and telemetry solution, collecting and storing data from different sources, including NFV infrastructure monitoring, Kubernetes infrastructure monitoring, VNF monitoring, SDN monitoring, etc.

2.3. Security Assurance and Certification Management

Security assurance and certification management (SACM) is responsible for providing an auditable, evidence-based evaluation and certification strategy for the assurance posture of complex ICT systems, based on identified security claims and metrics, also intended to boot strap the development of new models and tools that would lead to the definition and future establishment of a pan-European process, to be followed for the certification of devices, processes, and systems in the European market. The set of security metrics to be applied at the device, component, and system level are stored in the respective component, while the security assurance component is utilized for the proper configuration of the tests to be executed. The real-time, continuous assessment of the security posture of the complex ICT systems will be enabled by a purpose-built evidence collection engine, which will be responsible for aggregating the required evidence from multiple sources related to the operation of individual components, as well as the overarching processes that these components are involved in. This functional group of modules will also include audit and certification functions, leveraging the evidence-based approach of the assurance solution integrated into the FISHY platform. The certification block will provide evidence-based security, reporting, and certification to the needs of different stakeholders, ranging from senior management to external auditors and regulators, incorporating different access levels to the respective users. Finally, the audit block will be responsible for initiating, coordinating, and reporting to the IRO dashboard the auditing process results.

2.4. Enforcement and Dynamic Configuration

The enforcement and dynamic configuration (EDC) block is responsible for both making the supply chain measurably reliable end-to-end, and assessing the reliable and secure operation, even in the presence of potentially insecure components, based on the concepts of dynamic self-configuration. The general approach includes a predefined set of security features, based on an agnostic feature description language. This taxonomy allows the identification and translation of dynamically intent-based cybersecurity responses into specific configurations. Configurations are applied simultaneously at the network topology level and at each network security function (NSF) configuration leveraging the NFV technology. The main components in this functional block are the controller, planner, and enforcer. The controller is a network controller, mapping from the network-specific cyber threat solution to the actual NSF deployment and configuration. It can implement changes to the edge network topology and to the configuration of the running NSFs, based on the centralized FISHY intent-based resilience orchestration. This element will rely on an existing NFV orchestrator (NFVO) northbound interface, mapping the intent-based security policies to be translated and enforced on it. The register and planner is the component where the NSFs will register their security capabilities to be used in enforcement actions, using open standard interfaces, such as I2NSF [55]. The planner will use this information to combine and decide the best NSFs to use, their topologies, and the configurations to apply. Finally, the enforcer is the lower-level block of the EDC, continuously reconfiguring the whole ICT system via the existing NSFs, based on the available capabilities. This block will use standard (I2NSF) interfaces to NSFs whenever possible and support specific ones when no standard is available.

2.5. Trust and Incident Manager

The trust and incident manager provides the tools to be used for assessing the security of the stakeholder’s device, component or/and system. The vulnerability assessment tools will move beyond state-of-the-art (e.g., w3af [56]), providing,

among others, automated vulnerability and risks analysis, or estimation and detection in source codes using deep representation learning techniques. Indeed, the functionalities of this module cover the following three important sub-processes: (i) determining and establishing assets on the infrastructure; (ii) determining, naming, and prioritizing the vulnerabilities found in the analyzed system, component, or environment; and (iii) proposing the most effective mitigation actions. The vulnerability assessment will be in charge of providing the insight of how the detected vulnerabilities may entail a risk, and understanding the degree of weakness that the monitored infrastructure may present. Applying this to the FISHY supply chain platform will make supply chains more resilient to threats and, more specifically, to vulnerabilities. Moreover, although several kinds of vulnerability assessments (performed on network, host, database, applications, etc.) may be found, from the FISHY perspective, an assessment of the monitored ICT platform for the entire supply chain would make more sense, given that supply chain platforms are usually made up of various components. Consequently, it would also be appropriate to assess IoT devices if they are going to contribute to the ICT infrastructure of the supply chain. Incident detection tools will be based on the outcome of the vulnerability assessment and will be based on machine learning techniques. This component will provide smart processing based on the collected data, thus covering several different research areas. FISHY plans to integrate incident detection into a holistic process of cybersecurity hardening, increasing resilience and enabling faster response time to incidents over the whole ICT infrastructure of a supply chain, by leveraging existing open-source technologies, such as Wazuh [57], and integrating and expanding the capabilities of the XL-SIEM (cross-layer security information and event management), an event management tool that is oriented around enhancing normal SIEM capabilities [58]. In FISHY, the functionality of the impact assessment block is oriented around defining and outlining the existent relation between the status of the system and the changes happening, involving the employment of both qualitative and quantitative data, which are normally expected to be faced to various indicators within the assessed item. Indeed, this block will help in determining how and to what extent the supply chain will be affected should a change happen in the overall platform. The functionality of performing the assessment within this block will be guided and assisted by cybersecurity tools, such as the risk assessment engine (RAE) [59], as they can enhance the results in terms of accuracy, saving time, and reliability. The mitigation component should be responsible for limiting the scope of the expected impact analyzed on the impact assessment component, by detecting anomalies from network/IoT data based on machine learning algorithms. In FISHY, the mitigation mechanisms based on ML algorithms are proposed to work in the following two different ways: online mode and offline mode. The threat/attack repository will store the outcome of the trust and incident manager module whenever the analysis leads to a threat or attack (be it software or hardware). The tools to be used to develop this block are still to be decided; it is recognized that some repositories already exist and that data sharing will be highly useful. Based on the immutability principle, the repository will store the result, so the information may be used for the expected evidence-based assessment, and also timely informing of other involved stakeholders. Finally, the smart contract is the realization of the component that would alert the stakeholders when a security-related service level agreement is violated.

2.6. Security and Privacy Data Space Infrastructure

The security and privacy data space infrastructure is responsible for the proper collection and storage of data generated from the devices, processes, and components of the stakeholders' ICT systems, being part of the supply chain. It is based on the concept of the distributed and decentralized data storage concept (e.g., IPFS or data lakes), in which users hold a portion of the overall data, creating a resilient system for data storage and sharing. The data adaptation component is responsible for the homogenization of data coming at different intervals, in different data models (XML, JSON, small chunks of sensor data, logfiles, etc.) and following different communication means (REST APIs, Pub/Sub, etc.). Moreover, the identity manager is based on DLT, and is responsible for authenticating the users/processes connected to the secure and distributed data space, while the access policy component caters for preserving privacy per user accessing the data, according to specific policies set by the stakeholder responsible for the dataset. In this respect, not all users can access the whole set of data. Finally, the data anonymization component takes care of the privacy of the dataset shared by the stakeholders.

2.7. Secure Infrastructure Abstraction (SIA)

The main goal of the secure infrastructure abstraction (SIA) is two-fold. On one hand, it is intended to endow IoT systems with as many security guarantees as possible, assuming the inherent trend for IoT or edge devices to be potentially insecure. Two components are considered. The secure edge node (SEN) [60] is a software component designed to reside at the edge layer, and aimed at providing, by default authentication to IoT/edge devices, leveraging of an extensible blockchain architecture. This architecture provides a totally distributed and fault-tolerant chain of trust to IoT/edge devices, to be used to verify device signatures and establish secure TLS connections between the devices. The network edge device (NED) element will be in charge of controlling the network access of the protected environments, providing assurance for traffic flows, and ensuring a proper deployment and topology of the necessary monitoring and threat

response functions. Security decisions and actions, as defined by any FISHY component, will be translated into an enforcement configuration in the NED, whenever appropriate. On the other hand, the secure infrastructure abstraction provides the proper means to the enforcement and dynamic configuration, and the trust and incident manager to interact with the NFVI resources, regardless of the particular technologies that are to be used (OpenStack, Kubernetes, AWS, OpenDaylight, ONOS), SDN controllers, or other infrastructure managers. A technology agnostic view of the infrastructure is foreseen in the proposed FISHY architecture. To this end, exposed API endpoints can be used for the management of the network services and VNF instances. The APIs can be further used to collect monitoring data from the NFVIs and the network services, providing useful information about the infrastructure status, allocation of resources for service deployment, VNF performance, etc.

References

1. Leszczyna, R. Standards on Cybersecurity Assessment of Smart Grid. Int. J. Crit. Infrastruct. Prot. 2018, 22, 70–89. Available online: https://www.sciencedirect.com/science/article/pii/S1874548216301421 (accessed on 16 April 2021).
2. Scarfone, K.; Souppaya, M.; Cody, A.; Orebaugh, A. Special Publication 800-115 Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology; DIANE Publishing: Collingdale, PA, USA, 2009.
3. Pendleton, M.; Garcia-Lebron, R.; Cho, J.-H.; Xu, S. A Survey on Systems Security Metrics. ACM Comput. Surv. 2016, 49, 1–35.
4. Yee, G.O.M. Designing Good Security Metrics. In Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 15–19 July 2019; pp. 580–585.
5. Wang, L.; Jajodia, S.; Singhal, A. Network Security Metrics; Springer International Publishing: Cham, Switzerland, 2017.
6. Behi, M.; Ghasemigol, M.; Nejad, H.V. A New Approach to Quantify Network Security by Ranking of Security Metrics and Considering Their Relationships. Int. J. Netw. Secur. 2018, 20, 141–148.
7. Aldya, A.P.; Sutikno, S.; Rosmansyah, Y. Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard. In IOP Conference Series: Materials Science and Engineering; IOP Publishing: Bristol, UK, 2019; Volume 550, p. 12020.
8. Houngbo, P.J.; Hounsou, J.T. Measuring information security: Understanding and selecting appropriate metrics. Int. J. Comput. Sci. Secur. 2015, 9, 108.
9. Bhol, S.G.; Mohanty, J.R.; Pattnaik, P.-K. Cybersecurity Metrics Evaluation Using Multi-criteria Decision-Making Approach. In Smart Intelligent Computing and Applications. Smart Innovation, Systems and Technologies; Springer Nature: Singapore, 2020; pp. 665–675.
10. Craven, R.; Lobo, J.; Lupu, E.; Russo, A.; Sloman, M. Security policy refinement using data integration: A position paper. In Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration, Chicago, IL, USA, 9 November 2009.
11. Laborde, R.; Kamel, M.; Barrère, F.; Benzekri, A. Implementation of a Formal Security Policy Refinement Process in WBEM Architecture. J. Netw. Syst. Manag. 2007, 15, 241–266.
12. Han, W.; Lei, C. A Survey on Policy Languages in Network and Security Management. Comput. Netw. 2012, 56, 477–489.
13. Available online: https://www.snort.org/ (accessed on 16 April 2021).
14. Available online: https://suricata-ids.org/ (accessed on 16 April 2021).
15. Available online: http://www.trustedcomputinggroup.org/ (accessed on 16 April 2021).
16. Cesena, E.; Ramunno, G.; Sassu, R.; Vernizzi, D.; Lioy, A. On scalability of remote attestation. In Proceedings of the Sixth ACM Workshop on Scalable Trusted Computing, Chicago, IL USA, 17 October 2011.
17. Sailer, R.; Zhang, X.; Jaeger, T.; van Doorn, L. Design and implementation of a TCG-based integrity measurement architecture. In Proceedings of the 13th Conference on USENIX Security Symposium, San Diego, CA, USA, 9–13 August 2004.
18. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC8446. 2018. Available online: https://datatracker.ietf.org/doc/html/rfc8446 (accessed on 16 April 2021).
19. Frankel, S.; Krishnan, S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap, RFC6071. 2011. Available online: https://tools.ietf.org/html/rfc6071 (accessed on 16 April 2021).

20. Aman, M.N.; Chua, K.C.; Sikdar, B. Mutual Authentication in IoT Systems using Physical Unclonable Functions. IEEE I nternet Things J. 2017, 4, 1327–1340.
21. Adat, V.; Gupta, B.B. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. Telecommun. Syst. 2018, 67, 423–441.
22. Available online: https://www.bro.org/ (accessed on 16 April 2021).
23. Shon, T.; Moon, J. A hybrid machine learning approach to network anomaly detection. Inf. Sci. 2007, 177, 3799–3821.
24. Livadas, C.; Walsh, R.; Lapsley, D.; Strayer, W.T. Using Machine Learning Techniques to Identify Botnet Traffic. In Proc eedings of the 2006 31st Conference on Local Computer Networks, Tampa, FL, USA, 14–16 November 2006.
25. Moradbeikie, A.; Jamshidi, K.; Bohlooli, A.; Garcia, J.; Masip, X. An IIoT based ICS to improve safety through fast and a ccurate hazard detection and differentiation. IEEE Access 2020, 8, 206942–206957.
26. Fotiadou, K.; Velivassaki, T.-H.; Voulkidis, A.; Railis, K.; Trakadas, P.; Zahariadis, T. Incidents Information Sharing Platfo rm for Distributed Attack Detection. IEEE Open J. Commun. Soc. 2020, 1, 593–605.
27. Lagutin, D.; Bellesini, F.; Bragatto, T.; Cavadenti, A.; Croce, V.; Kortesniemi, Y.; Leligou, H.C.; Oikonomidis, Y.; Polyzos, G.C.; Raveduto, G.; et al. Secure open federation of IoT platforms through interledger technologies-the SOFIE approac h. In Proceedings of the European Conference on Networks and Communications (EuCNC), Valencia, Spain, 18–21 Ju ne 2019; pp. 518–522.
28. Ibáñez, L.-D.; Simperl, E.; Gandon, F.; Story, H. Redecentralizing the Web with Distributed Ledgers. IEEE Intell. Syst. 2 017, 32, 92–95.
29. Dunphy, P.; Petitcolas, F.A.P. A First Look at Identity Management Schemes on the Blockchain. IEEE Secur. Priv. 2018, 16, 20–29.
30. Larchevêque, E. Bitcoin Address Authentication Protocol (Bitid). August 2016. Available online: https://github.com/bitid/ bitid/blob/master/BIP_draft (accessed on 16 April 2021).
31. What Is Openid, Openid. 2005. Available online: http://openid.net/get-an-openid/what-is-openid/ (accessed on 16 April 2021).
32. Kraft, D. Nameid: Your Crypto-Openid. 2013. Available online: https://nameid.org/ (accessed on 16 April 2021).
33. Lundkvist, C.; Heck, R.; Torestensson, J.; Mitton, Z.; Sena, M. Uport: A Platform for Self-Sovereign Identity. Technical R eport. October 2016. Available online: http://whitepaper.uport.me/uPort_whitepaper_DRAFT20161020.pdf (accessed o n 16 April 2021).
34. Raouf, B.; Aib, I. Policy-based management: A historical perspective. J. Netw. Syst. Manag. 2007, 15, 447–480.
35. Walker, J.; Kulkarni, A. Common Open Policy Service (COPS) over Transport Layer Security (TLS), RFC4261. 2005. A vailable online: https://datatracker.ietf.org/doc/rfc4261/ (accessed on 16 April 2021).
36. Enns, R.; Bjorklund, M.; Schoenwaelder, J.; Bierman, A. NETCONF Configuration Protocol, RFC6241. 2011. Available online: https://datatracker.ietf.org/doc/rfc6241/ (accessed on 16 April 2021).
37. Bjorklund, M. YANG—A Data Modeling Language for the Network Configuration Protocol (NETCONF); IETF: Fremont, CA, USA, 2010.
38. OpenDaylight. Network Intent Composition:Main. Available online: https://wiki.opendaylight.org/view/Network_Intent_C omposition:Main (accessed on 16 April 2021).
39. Open Networking Foundation. Project Boulder: Intent Northbound Interface (NBI). Available online: https://github.com/O penNetworkingFoundation/BOULDER-Intent-NBI (accessed on 8 January 2021).
40. Berde, P.; Gerola, M.; Hart, J.; Higuchi, Y.; Kobayashi, M.; Koide, T.; Lantz, B.; O'Connor, B.; Radoslavov, P.; Snow, W.; et al. ONOS: Towards an open, distributed SDN OS. In Proceedings of the Third Workshop on Hot Topics in Software D efined Networking, New York, NY, USA, 22 August 2014; pp. 1–6.
41. The OpenDaylight Project, Inc. Available online: https://www.opendaylight.org (accessed on 16 April 2021).
42. Ibnemo. About Ibnemo. Available online: https://www.ietf.org/mailman/listinfo/ibnemo (accessed on 16 April 2021).
43. OpenDaylight. NEMO:Main. Available online: https://wiki.opendaylight.org/view/NEMO:Main (accessed on 16 April 202 1).
44. Hares, S. Intent-Based Nemo Overview, IETF Internet-Draft Draft-Hares-Ibnemo-Overview-01. 2016. Available online: https://datatracker.ietf.org/doc/html/draft-hares-ibnemo-overview-00 (accessed on 16 April 2021).
45. Xia, Y.; Jiang, S.; Zhou, T.; Hares, S.; Zhang, Y. NEMO (NEtwork MOdeling) Language, Internet Engineering Task Forc e, Internet-Draft Draft-Xia-Sdnrg-Nemo-Language-04. 2016. Available online: https://datatracker.ietf.org/doc/html/draft-x

ia-sdnrg-nemo-language-04 (accessed on 16 April 2021).

46. Prakash, C.; Lee, J.; Turner, Y.; Kang, J.M.; Akella, A.; Banerjee, S.; Clark, C.; Ma, Y.; Sharma, P.; Zhang, Y. Pga: Using graphs to express and automatically reconcile network policies. In Proceedings of the 2015 ACM Conference on Speci al Interest Group on Data Communication, New York, NY, USA, 17 August 2015; pp. 29–42.
47. Trakadas, P.; Simoens, P.; Gkonis, P.; Sarakis, L.; Angelopoulos, A.; Ramallo-González, A.P.; Skarmeta, A.; Trochoutso s, C.; Calvo, D.; Pariente, T.; et al. An Artificial Intelligence-Based Collaboration Approach in Industrial IoT Manufacturin g: Key Concepts, Architectural Extensions and Potential Applications Sensors. Sensors 2020, 20, 5480.
48. Kephart, J.O.; Chess, D.M. The Vision of Autonomic Computing. 2013. Available online: http://ieeexplore.ieee.org/docu ment/1160055/ (accessed on 16 April 2021).
49. A White Paper by 5GPPP Network Management & Quality of Service Working Group. Cognitive Network Management for 5G. Available online: https://5g-ppp.eu/wp-content/uploads/2017/03/NetworkManagement_WhitePaper_1.pdf (acces sed on 16 April 2021).
50. Abdelkhalek, O.; Krichen, S.; Guitouni, A.; Mitrovic-Minic, S. A genetic algorithm for a multi-objective nodes placement problem in heterogeneous network infrastructure for surveillance applications. In Proceedings of the 2011 4th Joint IFIP Wireless and Mobile Networking Conference (WMNC 2011), Toulouse, France, 26–28 October 2011; pp. 1–9.
51. Microsoft Language Understanding (LUIS). Available online: https://www.luis.ai/home (accessed on 16 April 2021).
52. Facebook Wit.ai. Available online: https://wit.ai/ (accessed on 16 April 2021).
53. Google Api.ai. Available online: https://dialogflow.com (accessed on 16 April 2021).
54. IBM Watson. Available online: https://www.ibm.com/watson (accessed on 16 April 2021).
55. López, D.; López, E.; Dunbar, L.; Strassner, J.; Kumar, R. Framework for Interface to Network Security Functions, RFC 8329. 2018. Available online: https://www.rfc-editor.org/rfc/rfc8329.html (accessed on 16 April 2021).
56. W3AF. Open Source Web Application Security Scanner. Available online: https://w3af.org/ (accessed on 16 April 2021).
57. Wazuh. The Open Source Security Platform. Available online: https://wazuh.com/ (accessed on 16 April 2021).
58. Atos Research and Innovation. XL-SIEM. Available online: https://booklet.atosresearch.eu/xl-siem (accessed on 16 Apri l 2021).
59. Atos Research and Innovation. Smart Security: Cybersecurity, Identity and Privacy. Available online: https://booklet.atos research.eu/sites/booklet.atosresearch.eu/files/public/content-files/page/2020/2020_ARI_Smart_Security_thematic%20 offering_v1.0.pdf (accessed on 16 April 2021).
60. Miquel, M.; Marín-Tordera, E.; Masip-Bruin, X.; Sánchez-López, S.; García, J. Implementing a Blockchain-Based Securi ty System Applied to IoT; Springer Nature: Cham, Switzerland, 2021; pp. 1–11.
