Deliverable 2.1

Project Requirements

Document version	:	1.0
Submission Date	:	31/12/2020
Dissemination Level	:	Public
Contribution to	:	WP2
Document Owner	:	I-FEVS
File Name	:	BIECO_D2.1
Revision	:	2.0

Project Acronym	:	BIECO
Project Title	:	Building Trust in Ecosystem and Ecosystem Components
Grant Agreement n.	:	952702
Call	:	H2020-SU-ICT-2018-2020
Project Duration	:	36 months, from 01/09/2020 to 31/08/2023
Website	:	https://www.bieco.org

Revision History

REVISION	DATE	INVOLVED PARTNERS	DESCRIPTION
0.1	05/11/2020	I-FEVS	Draft Revised
0.2	15/11/2020	UMU	Contributed paragraphs, 3.11-13
0.3	17/11/2020	I-FEVS	Improved content
1.0	18/11/2020	I-FEVS	Improved content
1.0	20/11/2020	IESE	Contribution to Section 5, Bullet points in Section 6
1.0	26.11.2020	IESE	More Contribution to section 5, and contribution on section 6.
1.1	7/12/2020	CNR	Section 3.14 Preventing Access Control Attacks added
1.2	15/12/2020	CNR	More contributions in section 2.8.
1.2	17/12/2020	UMU	More contributions to section 3, 8 and minor comments and inputs in other sections.
1.2	18/12/2020	GRAD	Review and comments in all the sections of the sections, proposal of restructure.
1.2	18/12/2020	IESE	Improved content on the introduction, Listed KPIs for the research activities in section 8, contribution to the table of acronyms.
1.2	19/12/2020	IESE	Improved content on 2, 2.1, 2.2, added description to scenario 2.5.1,
1.2	19/12/2020	UMU	Improved content on acronyms table, section 2, 5, 6
1.2	20/12/2020	UNINOVA	Improved content for section 4. Review and comments for sections 4, 7, 8.
1.2	21/12/2020	IESE	Introduction to Subsection 4.4. Contribution to the tables of acronyms. Removed section 8.
2.0	24/12/2020	UNINOVA	Contribution to Section 4. Revision and formatting.
2.1	31/12/2020	UNINOVA	Revision and formatting.

List of Contributors:

Riccardo Introzzi (IFEVS), Emilia Cioroaica (Fraunhofer IESE), Francesca Lonetti (CNR), Eda Marchetti (CNR), Sara Matheu (UMU), Ricardo Peres (UNINOVA), Sanaz Nikghadam Hojjati (UNINOVA), Sara Araújo (UNINOVA), José Barata (UNINOVA).

Disclaimer: The information in this document is subject to change without notice. Company or product names mentioned in this document may be trademarks or registered trademarks of their respective companies.

This document reflects only the authors' view. The European Community is not liable for any use that may be made of the information contained herein.

BIECO project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No **952702**.

Executive Summary

The aim of the document is detailing the requirements of the project together with its Key Performance Indicators to set the bases of the next development steps and allow the assessment of the results.

The first chapter of this document provides an introduction to the overall contextualisation of the topics within the project BIECO.

The second chapter starts with the definition of the software supply chain and describes the main aspects relevant for trust development.

In the third chapter, the major classes of cyber security risks and threats are described, with a special focus on the most significant scenarios which can be found in the framework of the software supply chain.

Project goals and requirements are then identified in chapter four to respond to the previously mentioned issues in the use cases under the focus of BIECO. Preliminary work to define KPIs for each of the use-cases is considered as well. On the basis of the results presented here, a detailed description of the three use-cases will be presented in Deliverable 2.2 to pave the way to the final definition of specific goals of the project as will be described in Deliverable 2.2.

Chapter five presents the beyond state of the art activities to be developed within BIECO.

In Chapter six problems and gaps are identified. This is to support and set a starting point for Deliverable 2.2 "Use-Case Definition", in further defining the next development steps to be taken within the scope of BIECO.

The whole document is mainly related to Objective 1 and Task 2.1 which are reported here for convenience.

Objective 1 (WP2)

CHALLENGE: ICT supply chains are complex ecosystems in which many actors (systems, components, users, developers and organizations) are involved, pursuing higher productivity and competitiveness. In most of the cases these actors have no control or access to the rest of the components provided by the other parties, so they have to assume that these elements are following the best security practices and their behaviour adheres to the expected. However, vulnerabilities exist and a cybersecurity issue in one of the ICT components can affect the integrity of the whole supply chain. Even though there are some individual tools that address different security aspects, there is a need of providing a complete solution that addresses all of them and reinforces trust within the complete supply chain.

PROPOSITION: In BIECO, a holistic security framework for ensuring trust within ICT supply chains will be provided. The framework will comprise a set of tools and methodologies for vulnerability assessment, auditing, risk analysis, determining the best mitigation strategies, ensuring resilience and certifying the security and privacy properties of the ICT components and the complete supply chain. The tools will be deployed on a cloud platform that will follow the guidelines of the designed reference architecture.

TASK 2.1

The partners will contribute with their unique insights, providing detailed descriptions of relevant scenarios and the cybersecurity risks and threats encountered in a software supply chain, along with a list of expected improvements.

This task is not aimed at finding solutions, serving only as a means to clearly identify problems and gaps and better define the set of goals to be reached. Even if initial discussions already started and list of requirements were defined as necessary for the definition of the proposal, a further and deepest analysis needs to be performed.

With these requirements acting as the foundation, a list of Key Performance Indicators (KPIs) related to software supply chain cybersecurity will be defined, supporting the development of the remaining tasks during the remainder of the project. Following this line of work, a list of adequate indicators will be elaborated for the evaluation of each of the use cases together with T2.2. With this approach, a precise and well-defined foundation can be built guaranteeing that the BIECO's development is appropriately planned and implemented.

Table of Contents

List of Figures

List of Tables

Glossary of Acronyms and Terms

Acronym	Term
Predictive Simulation	Simulation based on a set of well-defined situations that evaluate DT behaviour in a virtual environment
DT	Digital Twin. This is a simulation model fed with real time or predicted data.
Framework	Composition of tools that communicate over well specified interfaces. It enables implementation of methods.
Vulnerability	A weakness an adversary could take advantage of to compromise the confidentiality, availability, or integrity of a resource.
Weakness	Implementation flaws or security implications due to design choices
ICT	Information and Communication Technology - it indicates the domain of telematics, computer science, multimedia and internet.
Software Smart Agent	An intelligent software component involved in the automation of processes within a system, system component or ecosystem.
Verification	A set of activities that checks whether a system or a system component meets its specifications.
Validation	A set of activities intended to ensure that a system or system component meets the operational needs of the user. The user in this sense can be an actor within the ecosystem, or another system or system components that receives its services.
Risk assessment	The process of identifying, prioritizing, and estimating risks
Security Testing	The process to determine that an information system protects data and maintains functionality as intended
Security Certification	Comprehensive evaluation of an information system component that establishes the extent to which a particular design and implementation meets a set of specified security requirements
Digital Ecosystem	A structural and behavioural construct that forms around digital products, which dynamically interact. These products can be software components or cyber physical systems.
Actor	An Actor represents a non-cyber-physical party of the ecosystem, such as a specific person, company, or some other legal entity that interacts with systems and digital assets, such as software components.

1. Introduction

Formation of digital ecosystems enables a multitude of actors like organisations, users and developers to achieve different goals in cooperation. The achievement of operational, tactical and strategic goals of involved actors relies on trustworthy cooperation of systems within an ICT supply chain.

Traditionally, within modern ICT frameworks, integration and cooperation of large number of components developed by third parties is performed in order to keep a solution ready within a competitive environment.

In this sense, in BIECO we develop a framework that enforces trust into systems, system components as well as actors (such as users, developers, organizations) that interact with these systems and system components within a digital ecosystem.

Software supply chains can often reach high levels of complexity, leading high security risks. Particularly, because these components are shipped as black boxes, making hard the detection of possible malicious behaviour. On top of this, various vulnerabilities can be introduced along the way during the development of a component. Finally, the actor within the ecosystem (for example an organization providing an end system) which relies on the execution of the black box may not be aware if the best security methodologies have been applied during the development of the component. For example, emergent evidence shows that attempts of attacks on system assets is performed malicious intended members of an organization capable to insert a malicious code within a software component.

The only way to deal with such a situation is to assume the worst case - “untrusted by default”. Recent surveys[1] revealed that only 29% of IT business companies are aware of security compliancy and resilience of their own ecosystem.

Despite of the high economic impact of cyber-attacks, due to an exponential growth of available digital assets it is becoming increasingly difficult to manage ICT systems and components. Parts of the problem is due to the fact that many asset providers raise barriers to verify their security and privacy. This situation is worsened by the large heterogeneity of systems and components, as well as of security and privacy standards, which make it difficult to correctly apply adequate security and privacy measures. Furthermore, security and privacy are very dynamic concepts. While the system may be secure today, tomorrow a new vulnerability may emerge, so management must be dynamic to deal with these changes throughout the life cycle.

The need to accurately and promptly detect vulnerabilities and foresee their impact propagation is of paramount importance. A vulnerability assessment process should be continuously active in order to spot hidden weak points of an asset or new surfaces, potentially exposed to attacks. For example, this need is enforced by the emergence of new technologies that aim to improve functionality of systems. Such vulnerability detection can support resilience as involves the identification and deployment of mitigation strategies at any cyber-attack occurrence. However, for undetected vulnerabilities that opened the way to a malicious attack, mechanisms capable to ensure the ultimate trust during runtime need to be developed.

For addressing the problems of current and future emerging technologies, dynamic risk assessment and auditing should be made more general, objective and broadly applicable to future environments as well.

The holistic framework provided by BIECO has been conceived to integrate these methods to support companies in managing cybersecurity risks and threats to which they are exposed along the whole ICT supply chain as a complex system, both during design time and runtime.

[1] https://www.techrepublic.com/article/only-29-of-eu-organizations-are-gdpr-compliant/

2. Software supply chain

Supplying software to customers consist in providing an executable that supports the implementation of a given activity. In some cases, the software represents the end-product that enables execution of (advanced) system functions. In order to enable a fast adaptation of systems, software products are increasingly being shipped during runtime. Given the multiple vulnerabilities of software development and competitive goals within an ecosystem, the main actors interacting with each other in supply chain scenarios can be derived from the Open Trusted Technology Provider Standard (O-TTPS) v1.1 and other standards like the ISO 28000 series that focus more on physical supply chains. The main categories are Customers (end users, acquirers), (Re)sellers (retailers, wholesalers), Vendors / Providers (including system integrators), Suppliers, and Supporting actors (logistic providers, standards bodies, certification / accreditation bodies). Of course, one actor can fit in more than one category (e.g., a supplier could be also a provider). The software digital nature of controlled systems makes the software supply chain more difficult than expected at first, since it faces many peculiar challenges.

2.1. The traditional supply chain

It is convenient to consider first the traditional supply chain model: a chain of processes needed to supply the good, including all steps in its production from conception to delivery and maintenance at the customer’s side. The chain involves three main links: raw material supply, manufacturing and distribution, together with maintenance.

The supply chain can be very complex, nonetheless it can be though as made of rings which are modelled at a high level in the same way. At any point along the chain, resources are flowing from upstream into the business, to downstream up to the finished product. Basically, one can think of each step along the chain as represented by an input, a production operation and an output.

Within a supply chain, multiple actors such as organizations, users and governments interact within digital assets, forming in this way complex digital ecosystems. The flow of assets within such digital ecosystems drives the trust building process on three different levels: from the operational level, where the digital products implement functionalities in the real world, to the tactical level where digital assets and systems form cooperation for enabling achievement of higher-level strategic goals with monetary rewards for the involved actors. Dynamic trust evaluation within digital ecosystems enables fast reconfiguration: at the operational level through triggering of fail-over behaviour in case of detected failures, potentially caused by malicious attacks, to the tactical level where systems form different cooperation in order to guarantee the achievement of business goals. Undiscovered malicious attacks within this dynamicity can seriously hinder achievement of business gains within an ecosystem, directly affecting in this way the health of an ecosystem intended as a measure of how well the business advances within the ecosystem.

2.2. The software supply chain

A similar sequence applies to the software supply chain, as well.

At the operational level, planning is the first step which makes sure the right code is being developed for the required features of a digital asset. In an enterprise framework, this usually covers a huge number of connected artefacts: functional and non-functional attributes of the digital asset, interconnected elements, applications, and developers who take part in the development process. Figure 1 shows a high-level scheme of a software supply chain.

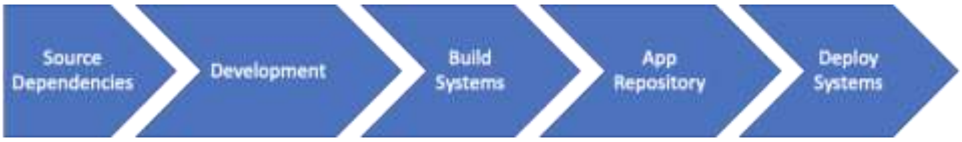

Figure 1: General scheme of a software supply chain.

At the tactical level, the process of forming relationships amongst the actors of the supply chain is major critical aspect. However, because within a cooperation, there might be not only collaborative goals, but competitive goals as well, the danger of malicious hidden behaviours can destroy tactical relationship, with negative impact for businesses. For the sake of the example, software providers use open-source software as a base for their customised products. Such sources need to be managed, analysing the quality and security of each chosen component and actor (such as developers) involved in the development of the product. Under this point of view, relevant aspects include documentation, certification, support, licensing, standards compliance and security implications.

The distribution of a software, through application of a supply chain model, interplays multiple and various steps that can leave open various vulnerabilities until the end product is delivered to the customer. One of these needs is the identification and description of specifications: developers build the code following a line of requirements for verification and validation; then marketing, sales processes and retailers come into play. Further aspects of the production arise downstream (e.g. software presentation to potential customer, integration with other applications on different hardware and operative system environments, choice of direct sale or reseller channels, distribution on cloud data centres, translations for international markets).

Despite the simplicity of the described model, security challenges are linked to all stages of a software component evolution within a software supply chain. The complexity of security challenges may grow with increasing number of sub-steps and parallel branches of product development. Within dynamic ecosystems, agile and trusted configurations and reconfigurations are the key to business success. This process involves agreements, partnerships, resources and efforts to meet customer satisfaction at all levels of trust evaluations: operational, tactical and strategic.

2.3. Securing the Supply Chain

Cyber security falls under the more general practice of protecting information and managing the risks to which it is exposed by preventing or minimising unauthorized and unlawful access, alteration/deletion, use or disruption of information (ISO/IEC 27000:2009[2], CNSS 2010[3]). In a business environment this practice must be integrated with an effective policy implementation and without losing organization productivity in terms of time and cost. This is especially important in SMEs, in which the effort and money expended in protecting each asset could be prohibitive.

There are several standards and initiatives (e.g., NIST cybersecurity framework, ISO 27000, ETSI EG 203 251...) that address security management in general. All of them share common processes that should be performed to efficiently protect, manage and assess the security:

- Establish the context and identify the risks:
  The first step of the assessment of security and privacy risks is performed through the identification of relevant information and its associated assets, together with the potential threats, vulnerabilities and the impact propagation of a hypothetical or real attack. Here, it is also important to take into account the current regulation and standards, as well as

[2] ISO/IEC 27000:2009 (E). (2009). Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO/IEC.

[3] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

context in which the system is going to operate. Fro instance, security requirements in eHealth are completely different from the ones required in a home automation context. Policies and industry standards provide help to manage passwords, antivirus software, firewalls, encryption software, legal liability, security awareness and training.

- Security assessment:
  A risk evaluation is then carried out on the basis of the previous results, providing ranking with respect to occurrence probability and impact. In this case a test-based risk assessment approach can provide the needed objectivity and repeatability needed to facilitate further comparisons with other similar systems. Security testing represents a powerful tool that allow to determine in an empirical way if a system is secure or not.
- Treatment:
  Based on the security assessment performed before, we can take treatment decisions. There are different treatment options proposed by the ISO 3100: avoiding, reducing or retaining the risk, removing the source of risk, modifying the consequences or the likelihood, sharing the risk with others, or even increasing the risk to pursue an objective. Based on the decision, proper controls must be selected and implemented.
- Monitor and communicate:
  Security can vary for many reasons. Among them, the discovery of a new vulnerability that reduces the security of the system or the application of an update or patch that increases it. Therefore, one important part of the security management is to continuously apply this procedure throughout the lifecycle of the product, as adjustments are often necessary to deal with new issues and implement new improvements.

2.3.1. CIA triad and its extension

Hereafter we report from literature the definition of information security that best describes the topic of interest within BIECO:

"*Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats. Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include confidentiality, integrity, availability, privacy, authenticity and trustworthiness, non-repudiation, accountability and auditability*." (Cherdantseva and Hilton, 2013[4]).

At the core of ICT security is information assurance, as stated by the above-mentioned security goals, ensuring that information is not compromised in case of critical problems, both physical (e.g. theft, system malfunctions, natural disasters) or cyber-digital. In the latter case cyber-systems can range from standalone devices to networked and mobile devices.

ICT security acts against malicious cyber-attacks aiming at acquiring private information or gaining control of the system for malicious purposes. It includes securing networks and allied infrastructure, applications and databases as well as security, safety and privacy testing, information systems auditing, business continuity planning, data duplication discovery and digital forensics among the most frequent operations.

[4] Cherdantseva Y. and Hilton J.: "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals". In: Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013)

The CIA triad of confidentiality, integrity, and availability, as first mentioned by NIST in 1977[5], constitutes the axioms of information security. Nonetheless, debate still questions whether it is sufficient to handle rapidly changing technology and business requirements. Many experts usually add other principles (see Cherdantseva and Hilton definition above).

Nine items have been proposed in 1922 by the OECD in their Guidelines for the Security of Information Systems and Networks. Developing upon those, NIST proposed thirty-three items in 2004[6]. Three Tenets of Cybersecurity[7] have been identified by DoD Software Protection Initiative starting from 2009, indicating System Susceptibility, Access to the Flaw, and Capability to Exploit the Flaw while Open Group proposed in 2011 the operational definition of security objectives in its security management standard O-ISM3[8], assessing information control and availability, data quality and compliance. Hereafter the most relevant concepts are described.

2.3.1.1. Authenticity

Authentication (from Greek: αὐθεντικός authentikos, "real, genuine", from αὐθέντης authentes, "author") aims at proving an assertion, such as the identity of a system or a user. Authentication is the process of verifying that identity[9]. This goes beyond identification itself – as indicating a specific entity – because it encompasses the identity validation through a certification process.

In ICT the term digital authentication is often used and refers to all procedures used to ensure party identities via electronic methods in a given digital framework including a networked one.

NIST described a general scheme for digital authentication:

- Enrolment, the application of a party to a credential service provider (CSP); the CSP makes the applicant a subscriber after it successfully provides its identity; the subscriber receives an authenticator – consisting in a token and the associated credentials.
- Authentication, the subscribed party can then start authenticated sessions (using its token and credentials) and perform transactions with another relying party.
- Life-cycle maintenance, CSP maintains subscribers' credentials for the due time while the subscribed parties are responsible for their authenticators.

Here, a relevant vulnerability is represented by man-in-the-middle attacks, in which a third malicious party split the communication stream in two and sets in the middle, pretending to be each of the two authorised parties in order to gather information from each side. To contrast this type of attacks, extra identification factors are implemented exploiting also different communication channels; a first example is given by 2-factor authentication (2FA).

2.3.1.2. Integrity

Data integrity is the state of assuring information accuracy and completeness over its lifecycle[10]. It ensures internal consistency or lack of corruption in information: data cannot be modified in an unauthorized or undetected way. It falls under the cases of consistency as understood in the standard ACID model (atomicity, consistency, isolation, durability) of transaction processing.

[5] A. J. Neumann, N. Statland and R. D. Webb (1977). "Post-processing audit tools and techniques". US Department of Commerce, National Bureau of Standards. pp. 11-3 – 11-4.

[6] "Engineering Principles for Information Technology Security", csrc.nist.gov.

[7] Hughes, Jeff; Cybenko, George (21 June 2018). "Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity". Technology Innovation Management Review. 3 (8).

[8] Aceituno, Vicente. "Open Information Security Maturity Model". Retrieved 12 February 2017.

[9] "What is Authentication? Definition of Authentication, Authentication Meaning". The Economic Times. Retrieved 2020-11-15.

[10] Boritz, J. Efrim (2005). "IS Practitioners' Views on Core Concepts of Information Integrity". International Journal of Accounting Information Systems. Elsevier. 6 (4): 260–279. doi:10.1016/j.accinf.2005.07.001.

2.3.1.3. Non-repudiation

As derived from law definition, non-repudiation refers to the case where a party cannot dispute the authorship or the validity of a contract, implying the obligation to fulfil its clauses.

In ICT it refers to assuring the impossibility of a party to deny the transmission or the receipt of a transaction[11]. Noteworthy cryptographic systems and similar technologies can support non-repudiation efforts.

The concept goes beyond proofing authenticity (i.e., a transaction matches a digital signature by a party's private key) and integrity (the transaction has not been altered meanwhile the transmission and delivery), by preventing a party from challenging the signature (e.g., by demonstrating the digital-signature algorithm is vulnerable or the private key has been compromised). Thus, authenticity and integrity are pre-requisites for non-repudiation.

2.3.1.4. Confidentiality

Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes" as stated by Anderson[12]. Its significance is related to privacy as it is a component aiming at protecting information from unauthorized access.

2.3.1.5. Availability

Availability is commonly viewed as one of the most important aspects of an effective information security solution: the information must be made available when it is needed.

Actually, the systems dedicated to store and process the information, the associated security controls and the access communication channels must be effectively operational at any time preventing service disruptions due to power outages, hardware failures and system upgrades as well as to denial-of-service attacks (e.g., flood of incoming messages forcing the target system to discontinue its operations). Ultimately end-point nodes need to be able to perform their activities through the system services, this is possible by ensuring availability.

2.3.1.6. Authorisation

Authorisation comprises the function of specifying access privileges to resources within a system[13]. This applies also to ICT frameworks, where access policies need to be defined[14].

In facts the system grants access to a resource by a given party based on a set of rules: once an authenticated party submits a request the system shall grant or reject it according to precise policies (e.g., role-based access control or RBAC, implemented on most multi-user systems, relies on Authorisation).

The access control consists of two steps: the policy definition and policy enforcement. Authorisation refers to the initial definition step, preceding the enforcement one which relates to granting or rejecting access requests. In the case of distributed systems, access is often granted without strict identity proof but on the basis of tokens.

Usually, limited access and restricted authorisations are granted to parties to allow them to fulfil their tasks and minimise the exposure surface to potential attacks (e.g., when a party cannot be completely trusted).

[11] McCarthy, C. (2006). "Digital Libraries: Security and Preservation Considerations". In Bidgoli, H. (ed.). Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management. 3. John Wiley & Sons. pp. 49–76. ISBN 9780470051214.

[12] Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. p. 240. ISBN 9780128008126.

[13] Fraser, B. (1997), RFC 2196 – Site Security Handbook, IETF

[14] Jøsang, Audun (2017), A Consistent Definition of Authorization, Proceedings of the 13th International Workshop on Security and Trust Management (STM 2017)

Maintaining authorization data is not trivial, as managing authentication credentials (e.g., it is often necessary to modify or remove users' authorizations, by changing or deleting the associated access rules).

2.4. Scenario overview for the supply chain

A wide number of critical scenarios has been recently reported by ENISA[15] for the most complex case of the Internet of Things field: a concise document describes the analysis of several security scenarios starting from the identification of high-level categories of security. Here, we take this official document as a reference as the most comprehensive also for other fields in the framework of the software supply chain.

2.4.1. Physical Attacks

2.4.1.1. Sabotage

Assembly pipelines can provide malicious actors with the opportunity to interfere and inject defects both to HW and SW components, which may be exploited at a later time causing problems (including the total shutdown of the production line or malfunctions of the product).

This case is impacting component assembly and embedded SW implementation.

2.4.1.2. Grey Markets

Defective, discarded or lost products may be offered in grey markets outside proper distribution networks. Such systems may lead to the release of untested and unreliable final products.

The two stages where the problem may occur are technical support and maintenance or device retiring and disposal.

2.4.1.3. Exploitation of Inadequate Physical Enclosures

This situation is referred to HW devices which should feature physical tamper-proof. This aspect involves the proper design and choice of material to avoid illegal malicious access to core elements. A significant example is given by the maintenance ports which should be disabled or removed prior to field installation to avoid their usage by attackers.

The lack of tamper-proof solutions can be exploited in Service provision and end-user operation phases as well as in technical support and maintenance.

2.4.2. Intellectual Property Loss

2.4.2.1. IP Theft

The illegal acquisition, exploitation, storage or distribution of intellectual property and sensitive information (e.g., design documents, source-code, credentials etc.) represent a previous asset for attackers. This threat is usually handled in a security-by-obscurity approach – which is subject to much criticism by experts.

Mainly, product design and component manufacturing can be affected by IP theft.

2.4.2.2. Reverse Engineering

While reverse engineering is not a threat for itself, it should be considered similarly to IP theft in the sense that both ways lead to the discovery and release into public domain of design details, vulnerabilities or backdoors, which can be exploited by attackers.

[15] ENISA, Guidelines For Securing the Inernet of Things, November 2020, DOI: 10.2824/314452

Usually, reverse engineering takes place during component assembly and SW embedding, device programming as well as technical support and maintenance or device retiring and disposal.

2.4.2.3. Overproduction and Cloning

This practice relates to fabricating a product, whose design specifications have been provided under a limited agreement by the rightful owner, outside of the bounds of the legal contract. Malicious parties can clone physical characteristics, FW and SW or the security configuration of a given device. Clones may include modifications and backdoors (for later reverse engineering or access) and then be sold on the market at cheaper prices. Alternatively, a genuine device can be substituted with a modified clone during transportation or commissioning.

The affected phases are component manufacturing and assembly or SW embedding.

2.4.3. Abuse and Manipulation

2.4.3.1. Electric and Magnetic Field Attacks

Interfering with a given device at an electromagnetic level is the basis of this attack aiming at corrupting or reading system memory and thus deploy Denial-of-Service attacks or the extraction of sensitive information – including, for instance, private keys during the generation process.

Such attacks can be deployed throughout component assembly and SW embedding as well as in Service provision and end-user operations.

2.4.3.2. Malware Insertion

Inserting malicious software can provides illicit access and other unauthorised functionalities to attackers. The operation can be carried out in the frame of insecure update mechanisms and poisoned software providers. This is a major concern in the area of IoT gateways which can be turned in a source of threats – these nodes, originally conceived to support security, can represent a main way to get access into trusted networks once compromised.

Many stages can be affected, ranging from component manufacturing and assembly to SW embedding and device programming, from IoT platform development to Service provision and end-user operation.

2.4.3.3. Debug Interface Exploitation

Debugging of IoT devices is a hard task especially when it comes to ensure confidentiality, integrity and availability. Standards do not specify how to implement debugging interfaces (e.g., JTAG) which are intended for internal use; if improperly disabled they may end-up in the final design and be available in production and assembly stages. Included with malicious intent or just for oversight, they enable access in the system of the final product at a dangerous level.

Their exploitation can be deployed in service provision and end-user operations, mainly.

2.4.3.4. Tampering and Counterfeits

Unauthorised supplier may distribute counterfeit products (specially chips) featuring malicious and modified modules (e.g., HW trojans) or non-validated parts that may increase the entity of vulnerabilities in the final product, which is referred to as tampered product. Such unauthorised chips and, more in general, HW components may come from similar parts with lower tolerances and capabilities and from reused, defective and disposed-of parts,

Opportunities for tampering can be found in many stages: semiconductor fabrication, component manufacturing and assembly.

2.4.4. Legal

2.4.4.1. Implications due to standard and Regulation non-compliance

Conceiving and designing privacy (encryption) processes is a challenge constrained by laws and regulations. Besides, actors have their own different interpretation of security issues. Service-Level-Agreements (SLAs) are meant to ensure common contractual view of the whole platform to be implemented: they specify security-guidelines which all components have to comply with. Furthermore, General Data Protection Regulation (GDPR) and local regulation must be applied as well. The result is that many existing and available components should not be included in the final product, leading to cost increase and production slow-down.

As initially mentioned, product design, service provision and end-user operation as well as technical support and maintenance may be heavily affected by these issues.

2.4.4.2. Performing a Data Protection

Performing a Data Protection Impact Assessment should be done in accordance with the General Data Protection Regulation to promote/achieve Privacy by Design. For many organizations, fulfilling the GDPR requirements is an integrated part of their business. Unfortunately, the requirements are often vague or too open and therefore subject to interpretation. One of the most challenging aspects of achieving the GDPR compliance is the creation of a Data Protection Impact Assessment (DPIA). This is a significant problem, especially for small and medium organizations, with cost and personnel restrictions. This is a privacy related challenge because DPIA is one of the cornerstones for achieving Privacy by Design as set by the GDPR.

2.4.4.3. GDPR-based development life cycle

The available development life cycles do not completely incorporate the privacy-by-design principles, and proposals targeting the GDPR demands are needed. Therefore, a reference GDPR-based development life cycle for the specification, implementation and testing of software systems and applications which takes into account (European) legal requirements is needed

2.4.4.4. Enforcing and demonstrating the privacy principles compliance

The peculiarities and the complexity of the currently available systems and applications call for specific automatic approaches, facilities and tools for enforcing and demonstrating the privacy principles compliance. This is a crucial aspect for the successful and lawful privacy-by-design process development.

2.4.4.5. Modeling the law

Considering in particular the access controls aspects, a challenge can be using Access Control elements and extensions to address concepts related to a given law requires formal translations in order to avoid misinterpretation or errors. Thin includes:

- the necessity of automatically enforceable matching of actual attributes gathered from legal use cases and the resulting policies in order to comply with GDPR’s principle of “data protection by design and by default”.
- a reference access control architecture to support context-aware security policies should be defined so as to assure the enforcement of the privacy policies throughout different kind of systems and environment. Additionally, methods for leveraging the integration of the Access Control and business processes as well as to mechanisms to enforce GDPR compliance during business activities of data management and analysis should be conceived.
- Verification & Validation approaches. the GDPR is changing how Personal Data should be processed. Part of the scientific and industrial worlds are replying to these exigencies by modifying the Access Control Mechanisms (ACMs) and the way of managing and

writing their policies. Consequently, specific testing strategies or validation approaches should be defined so as to assure that the generated data protection policies are aligned with the GDPR. Failing this task can lead in developing ACP that allows an unauthorized user to access protected personal data (security perspective) and consequently resulting in an unlawful processing (legal perspective). Therefore, the need of developing facilities for verifying the compliance of the derived policy with respect to the requirements expressed in the GDPR.

2.4.5. Unintentional Damage or Loss of Information

2.4.5.1. Compromise of Network

Lack of Quality of Services (QoS) and firewall policies may easily lead to compromised nodes in a network. The situation can be weaponised to organise large-scale attacks, such as Denial of Service (DoS), or degrade the supply-chain operations. Nodes with direct access to the Internet are the most exposed.

This kind of actions can be implemented at different levels: product design, device programming, service provision and end-user operations.

2.4.5.2. Use of default Authentication Settings

Authentication credentials of devices should never be fixed or derived from easily accessible information – for instance Media Access Control (MAC) address. This is of particular concerns for updates, which represent a critical point in security. Devices should be assigned unique random credentials during manufacturing.

These aspects involve product design, components assembly, SW embedding, device programming, together with service provision and end-user operations, technical support and maintenance.

2.4.5.3. Undetected SW or HW Disruptions of Devices

Extensive monitoring of all supply chain systems should be ideally implemented for early detection of HW and SW issues. The more proactive is the approach, the lower the number of disruptions and down-times in the supply chain in comparison to reactive measures only.

This kind of issue is affecting all stages of the supply chain and of the product life cycle.

2.4.5.4. User Errors

Informing and training users is a good approach to raise awareness of system functionality and secure risks. Human errors represent one of the most direct approaches to attackers aiming at breaking through a system security, be the case of internal members acting on critical systems or of end users improperly setting or using their own devices even when adequate protection measures are available. The topic also relates to other aspects of security since communication interception, among stakeholders in the supply chain for instance, and other social engineering attacks may open the way to more serious vulnerabilities.

Thus, all the above may concerns service provision and end-user operations, technical support and maintenance, device recovery and repurpose.

2.4.5.5. Technological Evolution during Device Lifecycle

Unexpected vulnerabilities may appear along a device life cycle due to technology improvements beyond the state of the art at design and implementation stages. This is particularly impactful in the case of long life-cycle products, as is the case of vehicles. An example is represented by the inability to enhance encryption strength after a flaw has been discovered in the previous scheme or the SW vendor disrupt support to its product.

Involved stages are service provision and end-user operation, technical support and maintenance.

2.4.5.6. Use of unpatched devices and systems

While new vulnerabilities may be commonly found during a device life cycle, as expected, a SW update mechanism needs to be implemented to avoid lacking the possibility to react to a new security risk. Noteworthy this tool should implement all measures to avoid code tampering and ensure genuine FW upload.

2.4.5.7. Cloud Service Disruption

Cloud-service based systems which are critical to the supply chain should be designed to run core operations even when off-line for extended time periods. A common example is given by the availability of some form of backup service when the service vendor goes out of business. Another frequent situation comes from the malicious takeover of domain names seriously impacting cloud services for which security measures need to be implemented.

Starting from device programming and IoT platform development, through service provision up to end-user operation, this issue must be taken into account.

2.4.5.8. Recovery Procedures Failure

A system may be unable to recover as a consequence of an attack; furthermore, FW, settings and credential might need to be updated along the device lifecycle. Also here comes into play the chain of trust with different implementation approaches, depending on the situation: the whole recovery procedure must be planned for the different potential situations that might cause security issues and stop or worsen device services. Criticality levels must be considered to select the appropriate solution.

Service provision and end-user operation are most affected by the problem in addition to technical support and maintenance.

2.4.5.9. Attack to Registration Procedures

Insecure registration procedures offer to attackers the opportunity to register malicious devices or prevent the proper registration of regular ones. Authentication platforms are dedicated to this purpose after device initialisation in manufacturing line and prior to final user provisioning in order to grant them proper access to services.

This aspect is covering device provisioning, IoT platform development, Service provision and end-user operation, technical support and maintenance.

2.4.5.10. Use of Recovered or Repurposed Components

Reuse of components regularly applied in a supply chain may seem a valid option for cost optimisation and timesaving. If not properly validated for reinsertion, they could contaminate an otherwise secure batch of devices.

This threat holds in device recovery and repurpose.

2.4.5.11. Attack to Manufacturing Processes

Within a supply chain the manufacturing pipelines are among the most sensitive zones. The lack of proper measures to regulate and monitor personnel access can rise security issues and create vulnerabilities. In the simplest scenario such a situation can lead to further threats as the already described sabotage or malware injection.

Among the most sensitive stages, along the supply chain, are semiconductor fabrication, component manufacturing and assembly, together with SW embedding.

2.5. BIECO Scenarios

Given the extension of the field of ICT security, project BIECO will focus on three specific scenarios among those which are identified as relevant by experts.

2.5.1. Scenario 1

Insertion of intended faults within software smart agents that are deployed at runtime. These intended faults can manifest into malicious behaviour in key situations. Until recently, the software architectures of platforms focused solely on the static deployment of software functions. These functions were deployed and integrated by engineers of organizations. During system operation, only minor changes were performed. Emerging platforms, however, will support dynamic deployment of software smart agents. This will be an enabler for smart ecosystems, which comprise a changing number of participants pursuing different goals and interacting with each other to achieve these goals in the best possible manner. The resulting dynamic architectures will yield new challenges for the software engineering of ecosystems. For example, the admission of smart agents into existing systems will become a matter of trust evaluation. The admission of a smart agent into an ecosystem will enable a system to join an ecosystem, and for example permit a smart agent to supervise specific control functions of a system, such as ensuring silent operation at night. Ecosystem admission should be based on functional correctness and on trust evaluation of the third-party component entering the ecosystem. Building trust in ecosystem components requires a new approach to testing, one that predicts the trustworthiness of a component to handle situations properly, instead of testing its correct implementation. This is necessary because a software component can contain a hidden malicious attack that shows up in situations when a foreseeable hazardous situation can be reached.

Until now, admission to a digital ecosystem has been based on the actors' commitment to published roadmaps organized and provided by an ecosystem orchestrator for the long term. Dynamic ecosystems, however, are particularly faced with the challenge of intended malicious behaviour which may be hidden in the smart agents. As a consequence, besides being functionally correct, a dynamic ecosystem also needs to assess the participants' trustworthiness before granting them admission. Assessing the trustworthiness of ecosystem participants requires new platforms that enable behaviour evaluation at runtime.

2.5.2. Scenario 2

Exploitation of architecture vulnerabilities though physical attacks.

As mentioned above, physical attacks may exploit undervaluation of potential risks, simple insufficient care in design (inadequate physical case) and implementation (e.g. supply from grey-market) or intentional sabotage e.g. malware injection), leading to serious potential threats.

The impacted areas can range from component assembly to embedded SW implementation, from technical support and maintenance to device retiring and disposal, from service provision to end-user operations.

Architectural design, implementation and maintenance have to be protected and monitored to avoid any kind of vulnerabilities against current and conceivable future attack methods based on new technologies.

An example worth to note is given by the frequent hardware attack deployed to vehicle architecture via the CAN bus through the gateway board for remote communications. Such a board represent the most exposed node in the remote network for Over-the-Air (OtA) services, moreover a malicious party could install its own components and open a breach in the implemented security countermeasures.

2.5.3. Scenario 3

Exploitation of "morally degraded" technologies for attacks (attackers become smarter than the current technology in use).

Security is a very dynamic concept. Today, one thing may be secure, but tomorrow this situation may change dramatically, involving high costs for the user, not only in terms of money, but also in terms of time and data leakage.

This situation makes it necessary to use agile tools that allow managing and ensuring the security of a product throughout its life cycle. Not only is it completely impossible to ensure that a system is 100% secure due to time and cost constraints, but also, the intelligence of the attackers, as well as the resources available to carry out such attacks, also evolve over time. Even the most accepted protocols in the digital society and considered as secure can be affected over time by new attacks. This is the case for example of the Transport Layer Protocol (TLS)[16] widely used for protecting our internet communications, or the Bluetooth technology[17], which was the main technology used for COVID-19 tracing and tracking for being considered more privacy preserving.

Other examples that we are more used to is the obsolescence of cryptographic algorithms or the increase in key lengths in line with the advances on the computational power of our computers. It is a reality that when quantum technology is more developed, many of the security algorithms currently considered as secure will cease to be so.

Managing these security changes is crucial to guarantee the security of the system and for this, it is necessary to develop methodologies and dynamic tools that allow us, not only to detect these changes, but to evaluate the impact and take the appropriate actions to protect the assets.

[16] https://www.zdnet.com/article/raccoon-attack-allows-hackers-to-break-tls-encryption-under-certain-conditions/

[17] https://techxplore.com/news/2020-05-bluetooth-flaw-impersonation-devices.html

3. Cybersecurity risks and threats

Nowadays, most relevant risks on cyber security are commonly related to networked systems relying on classic cryptography:

- Phishing
- Remote Work Endpoint Security
- Cloud Jacking
- IoT Devices
- Sophisticated and Targeted Ransomware Attacks
- Deep fakes
- Mobile Malware
- 5G-to-Wi-Fi Security Vulnerabilities
- Insider Threats
- Application Programming Interface (API) Vulnerabilities and Breaches
- Dependencies between components and vulnerabilities
- Software maintenance
- Default configuration
- Preventing Access Control Attacks

BIECO will address several items among the above-mentioned ones – such as Remote Work Endpoint Security, IoT Devices, Dependencies between Components, Vulnerabilities, Software Maintenance and Preventing Access Control Attacks.

3.1. Phishing

Exploits social engineering to steal private information, such as user identity and credentials, with both on-premises and cloud services attacks with an incidence of 77 % on espionage incidents in 2019 and a rising trend in 2020. Attacks performed through cloud applications turn out to be more effective than those carried out with traditional emails, given the common trust most people have in workplace cloud environments.

3.2. Remote Work Endpoint Security

Agile work is promoting more and more remote activity of workers, in many of these cases, inadequate or low network security is implemented at remote endpoints – for instance, mobile devices often conceal indications of potential phishing attacks and other cybersecurity threats.

One fourth of data breaches involve off-premises assets, mobile devices and telecommuters, according to WatchGuard[18].

In the context of software development, a remote endpoint used for development can become the target attack for inserting malicious codes into software that is then deployed on systems.

3.3. Cloud Jacking

is expected to become the dominant threat in the next future due to the increase of cloud computing of many businesses. Most incidents will exploit device misconfigurations according to Sophos 2020 Threat Report[19]. Direct code injection or through third party libraries will provide

[18] https://www.watchguard.com/wgrd-resource-center/predictions-2020

[19] https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf

vulnerabilities to most attacks, against cloud platforms, aiming at eavesdropping, taking control of and modifying sensitive information.

As an alternative, attackers inject malicious code into third-party libraries that users may download and execute unintentionally.

Forcepoint's 2020 Cybersecurity Predictions and Trends blog[20] reports that a lot of the security responsibility rests on the customers' side: shared responsibility models of typical public cloud vendors state that cloud service providers are responsible for protecting their infrastructure and customers are responsible for protecting their data, monitoring access, managing configurations, detecting anomalous user behaviours, monitoring system vulnerabilities and patching.

3.4. IoT Devices

Internet of Things (IoT) market is showing a strong grow and is expected to reach $1.1 trillion by 2026. One of the main features of these devices is the low computing capability to increase the battery life that allows the continuous operation of the device. However, this computing capability, together with the low costs, have made that essential aspects, such as security and privacy, are not considered properly, leading to a situation in which an attacker is able to harm a lot of unprotected and interconnected devices. The introduction of such an enormous number of IoT devices bears a proportional number of complex cyber-security threats in many sectors, some of which could be critical, e.g., Medical, Defence, Finance.

Noteworthy, IoT sector is undergoing an exceptional expansion while IoT supplier, designers and providers race to offer their solutions at very high swiftness, this leads to the expansion of potential attack surfaces to cybercrime. In addition, these rapidly evolving and complex systems are hard to be managed consistently, implementing effective security strategies at the emergence of new conditions.

3.5. Sophisticated and Targeted Ransomware Attacks

Among malware from crypto virology, a major concern comes from ransomware (i.e., a malicious software used to blackmail into paying a ransom threatening to publish victim's data or perpetually block access to it) with an increasing trend for all business sectors.

This kind of attack can be launched with kits readily available on the dark web, allowing to achieve devasting effects. In the last years highly sophisticated and targeted attacks have been deployed. McAfee head of cyber-investigation foresees a consolidation of this type of attacks up to powerful malware-as-a-service tools which are designed to cooperate among each other. Furthermore, likely the most powerful ransomwares will increasingly be deployed from affiliate structures to maximise their effect rising a major issue especially to SMEs, which would have to deal with heavy costs due to downtime and recovery.

3.6. Deepfakes

Digitally alter images and videos is becoming easily possible with the help of artificial intelligence (AI) and machine learning. Deepfakes exploit these tools to maliciously spread false information to portray activity that did not actually happen. Experts agree that deepfake may emerge among the most serious cybersecurity threats.

Despite this has been used to manipulate people's opinion till now – mainly for political, economic or social reasons – it is also prone to fraud usage allowing to generate synthetic identities or events. In 2020 the emergence of deepfake-as-a-service organisations has been

[20] https://www.forcepoint.com/blog/x-labs/2020-forcepoint-cybersecurity-predictions

observed, this is considered a potential serious threat especially if exploited to render scams more convincing, leading to billion-dollar costs to businesses.

3.7. Mobile Malware

Mobile devices are rapidly taking over fixed computers for most users, widely spreading in all business and private sectors; the amount of business information stored on mobile systems is considerably growing. Mobile malware is malicious software originally designed for mobile phone operative systems (OS) to target any critical and sensitive task – it is worth to note that technological evolution has implemented the same OSs on various devices other than phones, ranging from entertainment to automotive, from domotics to healthcare making mobile malware an emerging cyber-threat.

3.8. 5G-to-Wi-Fi Security Vulnerabilities

Handovers for 5G-to-Wi-Fi and other wireless communication channels, which are spreading out in nowadays networked systems, represent a spot with potential cybersecurity vulnerabilities due to skill and knowledge gaps, among the different communication technologies, in designing and manufacturing. The increasing sophistication of cyberattacks could exploit any breach in new systems to gain advantage. Software and Hardware weaknesses in the handover process represent opportunities for hackers to compromise security; this holds particularly for 5G networks for which carriers are routing traffic to Wi-Fi networks to balance bandwidth. With 5G, being introduced to cover wide public areas, voice and data information is handed over from enabled mobile devices to Wi-Fi spots – a number of vulnerabilities have already been found thus making it a serious threat.

3.9. Insider Threats

More than 34% of successful cyber-attacks involve internal actors – insider attacks rely on malware as well as negligence in system and data use by organisations and their employees.

Hence thorough investigation, timely detection and rapid response to indicators of insider attacks are key countermeasures. Specialised tools help by monitoring anomalies and variations which can be signs of such attacks (e.g. unauthorised logins, new app installation on isolated systems, unusual activity by users with newly granted privileges, operations of new devices on restricted networks). Machine learning and intelligent tagging of suspicious events turns out to be effective to identify threats such as misconfigurations and risky behaviours.

3.10. Application Programming Interface (API) Breaches

Security readiness of most APIs hinges on web application security. Moreover, two thirds of organisations publish their APIs to provide developers and their partners with solutions ready to use their app ecosystems and platforms. Hence APIs spread increases as well as the dependence on their use. The necessity to rapidly reach the market rises the probability that a larger number of vulnerabilities is included in APIs, impacting on high-profile applications in financial operations, messaging, peer-to-peer and social media.

Therefore, API security represent the weakest link for such applications leading to cloud-based threats for user data and privacy as well as for business information.

3.11. Dependencies between components and vulnerabilities

A CPS is composed of: (i) a cyber part, mainly based on software and control elements, (ii) an interconnection part composed of interfaces between the software world and the physical world, and (iii) a physical part that interacts with the physical world via sensors and actuators. These different parts communicate via different kinds of wireless and wired networks. Complex cyber-physical systems include several components and establish multiple relationships, which in turn complicates not only the integration of security mechanisms but also the measurement of their effectiveness. Security vulnerabilities in one component could affect other components and trigger cascading effects due to unforeseen threats and dependencies among components, which might compromise the whole system.

Moreover, CPS are mainly integrated into industrial systems, including critical infrastructures, so these systems have to be protected from external and internal threats that come with Internet connectivity. Traditional "physical" devices such as lights, video surveillance, ID cards, biometrics, access control systems and more are now IP-enabled. This creates an entirely new set of vulnerabilities that hackers are already exploiting and will continue to exploit, so as to access a company's network, e.g., to steal business or customer information.

3.12. Software maintenance

Cybersecurity is itself a dynamic concept. Indeed, at the end of the manufacturing process, a product can be certified as secure, but this condition could change during its life cycle if a new vulnerability is discovered. The manufacturer must guarantee continuous updates and patches throughout the life cycle of the product, so that the consumer is protected against new threats. However, the process of developing a patch or an update is often expensive and time consuming, which leaves the product vulnerable for a period of time. In addition, the discovery of a vulnerability, as well as the installation of a patch or an update can alter the level of security provided by the project, needing a security revaluation.

3.13. Default configuration

The default settings in a product can be a double-edged sword. On the one hand, a weak default configuration applied equally on all devices can facilitate the execution of an attack if no pre-configuration is required from the user. On the other hand, helping the user to configure safely and convey the security of their product to you guarantees a reduction in the attack surface and the limitation of the number of attacks it could be subjected to if no configuration is made.

3.14. Preventing Access Control Attacks

Among security mechanisms that guarantee the confidentiality, integrity and availability of data, access and usage control systems represent an important component able to mediate all requests of access to protected data. They ensure that only the intended, i.e., authorized users can access the data, and that these intended users are only given the level of access required to accomplish their tasks.

Designing a secure authentication and access control system is very difficult. Access control vulnerabilities are among the most common vulnerabilities in web applications. They occur when an access check is missing or incorrectly performed into the access control policies or mechanisms implementing these policies, allowing an attacker to execute some operations that might not be authorized. Moreover, authentication and access control bugs are difficult to detect by simple analysis tools, because their logic is application specific. Then, specific methodologies and testing tools are needed to prevent access control attacks.

Access control policies specify the level of confidentiality of data, the procedures for managing data and resources, and the classification of resources into category sets yielding different security requirements.

Access control systems usually rely on the eXtensible Access Control Markup Language (XACML), the de facto standard for specifying, storing and deploying access control policies.

Since access control policies are very complex, assessing their correctness is a very challenging task. Policy testing is very critical and must be performed in an effective way to identify policies inconsistencies that could hide potential security flaws and bugs. Since exhaustive testing is impossible due to budget constraints, efficient testing methodologies and tools need to be provided for guaranteeing reliability and high quality of the access control systems. Mutation analysis and combinatorial approaches are the most suitable approaches for test cases derivation and assessment.

Inside the access control systems, the Policy Decision Point (PDP) is one of the most critical components. It is in charge of implementing the evaluation logic of access control policies, i.e., the rules for accessing data and resources. Then, any error or overlook of the PDP could result either in forbidding due access rights, or worse in authorizing accesses that should be denied, thus jeopardizing the security of the protected data. Testing of the PDP consists of probing the PDP with a set of test cases (i.e., XACML requests) and checking its responses against the expected decisions. Available proposals for generation of test cases leverage the application of the combinatorial approaches to XACML policies values for generating test inputs, or the representation of policy-implied behaviour by means of models.

Another important issue into the context of the access control testing is the automated verdict derivation that represents a key aspect for improving the cost-effectiveness of testing, especially when test suites are large and manual inspection of results is not feasible.

3.15. The DREAD model

Here, we propose to take as a reference the DREAD model (used by Microsoft and currently by OpenStack, among others; although it was abandoned by its authors). It is a mnemonic for risk rating using five categories:

1. Damage – what would be the amount of damages caused by a given attack?
2. Reproducibility – how easy is it to reproduce the attack?
3. Exploitability – how many efforts are required to launch the attack?
4. Affected parties – what would be the impacted parties?
5. Discoverability – how hard is it to detect the hazard of such an attack?

The calculation always produces a number between 0 and 10; the higher the number, the more serious the risk. However, there is not a consensus on how the actual risk point scale should be, since it all depends on the individuals performing the thread modelling. DREAD requires scoring each of the five categories on a scale from zero to ten, which leads to discussions on the fine differences between consecutive numbers, e.g., five and six. Therefore, the approach is not fully consistent and it is still subject of debate. One solution to this problem could be using scores of High, Medium, or Low, that are easy to agree, instead of the eleven numerical values.

Despite it provides a more qualitative than quantitative method to classify cyber-security threats it turns out to be effective and of immediate application to determine risks and prioritise among them.

3.16. The STRIDE model

Starting from the above considerations on risks and threats a good line of thoughts appears to be to refer to the STRIDE model, the counterpart of which has been considered when describing the main aspects of cyber-security.

STRIDE is a mnemonic acronym to indicate the main types of threats to ICT security. It entails six items as listed in

Table 1.

Table 1: Security properties and corresponding threats as indicated by the STRIDE model.

Security Property	Threat	Description
Authenticity	Spoofing	Pretending another identity to gain control
Integrity	Tampering	Information alteration, deletion or injection
Non-repudiability	Repudiation	Repudiating or refuting a statement or contract validity
Confidentiality	Information disclosure	Unauthorized data access (also off-line)
Availability	Denial of Service	Disrupting normal communication
Authorization	Elevation of Privilege	Gaining elevated access to resources

In the following a brief description of the main cyber-attack types, although not exhaustive, limiting the discussion to the above-mentioned STRIDE model, being the actual matter very vast, fluid and continuously evolving.

3.16.1.1. Spoofing

In ICT security, a spoofing attack is implemented when a party successfully identifies as another by falsifying data, to gain unauthorised advantage. It includes TCP/IP Spoofing, Caller ID spoofing, E-mail address spoofing, Geolocation spoofing and GPS spoofing.

3.16.1.2. Tampering

It refers to the malicious modification or alteration of data. As examples we report the Evil Maid attack and the security services planting of surveillance capability into routers[21].

[21] Gallagher, Sean (14 May 2014). "Photos of an NSA "upgrade" factory show Cisco router getting implant". Ars Technica, https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/

3.16.1.3. Repudiation

Repudiation refers to the case where the author of a statement or a contract, questions its authorship or validity. The meaning is derived from legal setting where the authenticity of a signature is being disputed.

In digital security, repudiation involves challenging the proof of data integrity (such as hash codes) or data origin (digital signature), alleging data alteration or invalid signature by showing that one of the items involved was compromised or the verification method can be broken.

3.16.1.4. Information Disclosure

Information disclosure, also indicated as privacy breach and data leak, is the release of secure, private or confidential information to an untrusted environment. Intentional incidents are often combined attacks by hackers from organized crime, political parties or national governments. Also, unintentional events may occur, caused by careless disposal of used equipment or storage media.

3.16.1.5. Denial of Service

This type of cyber-attack aims at making a resource, either temporarily or indefinitely, unavailable to intended user parties. Usually, the target is a host on the internet.

The attack is accomplished by saturating the target with multiple unnecessary and synthetic requests with the aim of overloading the resource and prevent legitimate requests from being handled.

The most effective attacks of this kind are Distributed Denial of Service (DDoS) – the perpetrators exploit many different sources to flood the target making it hard to stop the attack by blocking all sources.

3.16.1.6. Elevation of Privilege

Gaining elevated access to resources can be accomplished by exploiting bugs, design flaws and configuration oversights in a system – the attack can be undertaken through Operative System (OS) as well as application vulnerabilities, making an application reach higher privileges than those intended by developers or administrators; in such a way that it can perform unauthorised operations.

3.17. An example: the Rowhammer attack

A particular case related to HW Vulnerability Exploitations is reported here to provide an example of how real implementations fall under the previous item categorisation.

In modern times, technology is evolving at a very fast-pace to deliver more performant devices but this leads to the possibility the systems include new hardware components with unknown vulnerabilities.

The so-called Rowhammer attack exploits software crafted in such a way that flips the bits and gets access to memory locations where other application execute. It takes advantage of an unintended effect in dynamic random-access memory (DRAM): close-by memory cells leak their charges interacting each other, thus content leaking or changing can occur from memory rows not intentionally addressed to neighbour ones.

This is one example of HW vulnerability exploitation, successfully deployed in some privilege escalation, information disclosure and tampering attacks in the past.

4. Project Goals and Requirements

4.1. BIECO Goals

The BIECO project aims to develop a framework that enables measurable, risk-based trust while developing, deploying and operating complex interconnected ICT systems. This will be achieved through the handling of reliability and trust aspects of ecosystem participants (ICT systems, ICT system components and actors) within the supply chain.

The general goals of the project can be framed as specific SMART (Specific, Measurable, Achievable, Realistic, Time-bound) objectives, taking into account the challenges of this kind of complex ecosystems. These are listed below:

- **G1** – Providing a framework that will allow the reinforcement of trust in ICT supply chains
- **G2** – Performing advanced vulnerability assessment over ICT supply chains
- **G3** – Achieving resilience in ecosystems formed by unreliable components
- **G4** – Extending auditing process to evaluate interconnected ICT systems
- **G5** – Providing advanced risk analysis and mitigation strategies that support a view of the complete ICT supply-chain
- **G6** – Performing evidence-based security assurance and a harmonized certification for ICT systems
- **G7** – Industrial validation of BIECO's framework within IoT ecosystems

Based on this, Section 4.3 will describe the initial list of both functional and non-functional requirements that can be derived from these goals, followed by Section 4.4 addressing the KPIs for each of them, which can be seen as the overall success criteria for BIECO. Both of these serve as initial specifications to guide the development of the technical WPs during the early stages of the project and will be later on refined in T2.2 following the specific needs and scenarios of the use cases.

4.2. BIECO Requirements

Complementary to the specification of the Functional Requirements, Table 3 provides an initial list of Non-Functional Requirements, pertaining not to the functionalities and services offered by the system, but instead to the way they should be carried out.

Table 3 summarize BIECO's Functional and Non-Functional Requirements, respectively. Along with a brief rationale, each requirement is contextualized in regard to its associated goals (as listed in Section 4.1) and the WPs that directly address it.

Firstly, the Functional Requirements are presented, entailing the specification of the actual functionalities and services to be provided to stakeholders by the BIECO ecosystem.

Table 2 – Functional Requirements of the BIECO Project

Requirement	Rationale	Goals	WPs
FR1 – Real-time Monitoring	BIECO should be capable of performing real-time monitoring/auditing of the underlying systems or devices to detect deviations from the expected behavior.	G1, G3, G4	WP5

Requirement	Rationale	Goals	WPs
FR2 – Adaptation	BIECO should be able to adapt the underlying system/component/device at runtime based on adequate mitigation strategies	G1, G3, G5	WP5, WP6
FR3 – Vulnerability Analysis	BIECO should enable the identification and/or forecasting of vulnerabilities in ICT systems through advance data analytics.	G1, G2, G3	WP3
FR4 – Simulation	BIECO should be capable of simulating the behavior of underlying systems or components to self-check future failures or vulnerabilities.	G1, G2, G3	WP4
FR5 – Security evaluation	BIECO should be able capable to measure the security of a system in an objective way using empirical tools such as testing.	G1, G5, G6	WP6, WP7
FR6 – Security certification	BIECO should be able to generate a visual and dynamic security label as a result of the security certification process,	G1, G5, G6	WP7
FR7 – Security baseline	BIECO should base the security evaluation on standards and best practices, taking into account also the relevant regulation.	G1, G5, G6	WP7
FR8 – Behavioral profiles	BIECO should design a security behavioral profile as a result of the certification process.	G1, G5, G6	WP7, WP6

Complementary to the specification of the Functional Requirements, Table 3 provides an initial list of Non-Functional Requirements, pertaining not to the functionalities and services offered by the system, but instead to the way they should be carried out.

Table 3 - Non-Functional Requirements of the BIECO Project

Requirement	Rationale	Goals	WPs
NFR1 - Interoperability	Heterogeneous components of the BIECO ecosystem should be capable of cooperating and exchanging data using common representations and interfaces	G1	WP3, WP4, WP5, WP7
NFR2 – Scalability	BIECO solutions should be agile and dynamic, being as automated as possible.	G1	WP6, WP7

Requirement	Rationale	Goals	WPs
NFR3 – Modularity	BIECO solutions should be loosely coupled, allowing stakeholders to mix and match functionalities of the framework as needed.	G1	WP2, Wp3, WP4, Wp5, WP7
NFR4 – Privacy-Preserving	Measures should be taken to ensure that BIECO's tools preserve the privacy of sensitive data (e.g. source code) of stakeholders.	G1, G2	WP3
NFR5 – Standardization	BIECO solutions should be based as much as possible on current standards.	G1, G5, G6	WP7

4.3. Key Performance Indicators

For enabling reinforcement of trust into ICT supply chain, BIECO will offer one architectural solution of a framework that enables connection of different tools according to methodologies defined within the project. Generally, the tools and methodologies will address design time as well as runtime aspects of trust linked to security and safety. Concretely, vulnerability assessment, monitoring and risk analysis will enable definition of suitable mitigation strategies in case of detected malicious intrusions of behaviour.

For the ultimate trust assurance, BIECO will provide solutions that improve systems' resilience in case of malicious attacks. In this regard, one solution will be developed for enabling self-checks on the system with the scope of:

1) identifying hazardous situations created by undetected vulnerabilities that made their way through the system operation at runtime.
2) detecting sporadic hardware failures

In order to avoid hazardous situations, BIECO will offer one solution of predicting effects of possible untrusted deviations in a virtual environment. Based on prediction and dynamic risk assessment, methodologies will be developed that enable a system to transition into a safe state, assuring in this way, the ultimate trust.

Detection of malicious behaviour and runtime activation of safe behaviour will be assured by one monitoring tool integrated within the BIECO framework. The monitoring tool will listen to (a) the events provided by one simulation tool that does the prediction and (b) interface to the actual component execution in the real world. Interfaces for communicating between different tools will be developed within the project and will support the overall BIECO architecture creation.

Based on detected untrusted deviations, which may be caused by security attacks, one methodological security assessment approach will be developed.

The following table provides a list of KPIs linked to work packages.

Table 4 – Key Performance Indicators of the BIECO Project

#	**Key Performance Indicator**	**Goals**	**WPs**
1	BIECO’s reference framework ≥ 1	G1	WP2
2	BIECO’s reference architecture ≥ 1	G1	WP2
3	Tools for detecting and forecasting vulnerabilities in ICT components ≥ 1	G2	WP3
4	Tools for analyzing the propagation of vulnerabilities across the ICT supply chain ≥ 1	G2	WP3
5	Solutions to perform self-checks on ICT systems ≥ 1	G3	WP4
6	Tools for simulating failure prediction within ICT supply chains ≥ 1	G3	WP4
7	Methods for recovering the systems back from a security fault ≥ 1	G3	WP4
8	Simulation tools for the runtime auditing of interconnected ICT systems ≥ 1	G4	WP5
9	Abstraction models of interacting ICT components delivered ≥ 2	G4	WP5
10	MUD files generated ≥ 1	G4	WP5
11	Methodology for dynamically estimating risks in ICT supply chains ≥ 1	G5	WP6
12	Visual tools for risk threats and hazard analysis for security and safety ≥ 1	G5	WP6
13	Mitigation strategies provided (with security, privacy and accountability measures) ≥ 5	G5	WP6
14	Security certification methodology, including specific security claims and metrics ≥ 1	G6	WP7
15	Security service framework covering security assessment and testing, prevention, monitoring, detection and mitigation ≥ 1	G6	WP7
16	Technological and methodological assets validated in BIECO ≥ 10	G7	WP8
17	Industry sectors validating BIECO’s assets ≥ 3	G7	WP8

5. Problems and gaps identification

Considerable work has been done in analysing and describing Software Ecosystems (SECOs) formed around software products. Supported by the evolution of network technology, an emerging transition is bringing systems of all types (including safety-critical system) to be part of complex ICT supply chains into what is known as smart ecosystem (SES). SES typically emerge around cyber-physical systems (CPS) that receive software and hardware components from different suppliers, actors within an ecosystem. Within BIECO we use the meta-term "digital ecosystem" to refer to both software ecosystems (formed around software products) and smart ecosystems (formed around cyber physical products.)

Withing a cyber-physical system, where hardware and software components are provided by different actors, their interaction requires additional checks of trust. The key difference between digital ecosystems and system of systems is that digital ecosystems involve actors with goals, which significantly influences the dynamics within. In cooperation, the actors might have not only collaborative goals, but also competitive goals, which may influence the health of the ecosystem. The health on an ecosystem is an indication of how well the business within ecosystem evolves over time. In digital ecosystems, where hardware and software components of cyber-physical systems are provided by different actors, malicious behaviour can be introduced along with software components by actors who join the ecosystem based on declared collaborative goals, but who are actually acting in competition.

Until recently, admission to a digital ecosystem has been based on the actors' commitment to published roadmaps organized and provided by an ecosystem orchestrator for the long term. Ecosystems which comprise safety-critical applications, however, are particularly faced with the challenge of intended malicious behaviour which maybe hidden in the smart software agents. As a consequence, besides being functionally correct, an ecosystem also needs to assess the participants' trustworthiness before granting them admission. Assessing the trustworthiness of ecosystem participants requires new concepts, platforms and methods that enable behaviour evaluation, particularly at runtime where the malicious behaviour may express.

Even though many proof-of-concept attacks and techniques have been observed for years, the according countermeasures have not been always implemented, leaving devices and systems that join an ecosystem vulnerable to malicious attacks.

There is huge research and documentation effort to summarise all existing attacks nonetheless many more are found continuously. Furthermore, there is a difficulty to define a common standard methodology to describe how security evaluation and certification must be done. The wide variety and heterogeneity of methodologies, mechanisms, standards[22] and products derives on a confusing landscape of solutions. Therefore, it is quite unclear which security aspects should be considered to guarantee an adequate security level. In this context, comparability is unfeasible, as different schemes uses their own metrics, especially when products are evaluated under different national schemes or approaches, or when they include some subjective or difficult to calculate metrics (e.g., CWSS uses likelihood). The cybersecurity act presents a pioneer initiative to foster the development of a European Cybersecurity certification framework. This regulation, in addition to the NIS directive and the General Data Protection Regulation (GDPR) form the three main pillar for cybersecurity in Europe.

However, the definition of a security evaluation and certification scheme is not easy, posing several challenges that is necessary to address. The wide variety of schemes and requirements hardens the objective comparability of the security achieved. Also, the context (regulation, domain...) determines the security level required for a particular product and should be considered. This problem is exacerbated by the out-of-date certificates that gives a false sense of security. The dynamism inherent to security makes necessary agile and dynamic approaches to manage the security of a product throughout its lifecycle. As a consequence, it is also necessary

[22] https://ecs-org.eu/working-groups/news/wg1-state-of-the-art-syllabus-updated

dynamic labels that are capable to show in real time, the real security level. However, current schemes and approaches are not aware of this dynamism; Common Criteria (CC), Commercial Product Assurance (CPA) or Certification de Securité de premier niveau (CSPN) requires a complete recertification in case of a security change, involving high money loses and time.

Moreover, classification of the relevant existing attacker models is often incomplete, especially when it comes to many hardware peripherals connected to networked systems. This situation represents a potential weakness that has to be taken into account.

Ongoing discussions and debates on proper approaches to fix the lack of standardised and effective tools capable to manage the security evaluation of complex systems, indicate the importance to rapidly address the problem.

6. Expected improvements

Within BIECO we envision the advancement of the current state of the art in the field of security management addressing the complete lifecycle of an ICT component. In this regard, methods and tools will be developed for vulnerability and malicious behaviour detection and assessment by addressing the specifics of an ICT component life-cycle: from conceptualization to design to deployment and runtime execution in the field.

BIECO will advance the current state of the art and practice by bringing forward the design of systems resilience to malicious attacks relevant for the use cases. Of particular interest is the detection of intended faults that are strategically place within software components and manifest into malicious behaviour during runtime. Within an ecosystem, malicious actors can deliver code with intended failures that manifest into malicious behaviour in specific technical situations when it is most likely to achieve a target destruction impact. The target destruction impact can range in severity from not meeting user expectations to putting the system in hazardous situation through occurrence of serious accidents that endanger the life of people or the environment. For safeguarding systems operation against malicious attacks that made their way into the runtime of the system, we will build on novel methodologies for behaviour prediction based on digital twin execution during runtime. Timely predictive detection enables a system to trigger a fail-over behaviour, in case of predicted hazard.

When considering software smart agents that execute in open environments, the deviation from the specifications can be considered both an increase of intelligent behaviour through an improved capability to adjust to new environmental situations or a malicious deviation. Therefore, any deviation from the expected behaviour needs a careful and holistic evaluation. Particularly, the environment for evaluating trust in a software smart agent needs to comprise connections with connected software and architectural components of the system. That is because within an ecosystem, the inter-related software components can themselves be downloaded at runtime and strategic placed intended faults within multiple components can expose malicious behaviour not in singularity, but through a cooperative instrumentation of functional and timing behaviour.

While the risks associated with maliciously behaving actors within ecosystems have been recognized there is still no satisfactory solution for the issue yet. In BIECO we follow one of the most promising directions in this context, driven by the formation of trust in smart software agents. At the beginnings of development of autonomic computing systems, reputation was a good indicator of the level of trust in a system. State of the art approaches envision the possibility to store information about a system's reputation in order to address the need for trustworthiness in potential partners. However, this approach implies the execution of a system's behaviour in the real world and hence entails the risks associated with executing malicious behaviour that can be introduced along with the software smart agents. A solution for building reputation in a system without executing its behaviour in the real world has become possible by recent advancements in the field of automation. The notion of a Digital Twin (DT) has been introduced by NASA as a realistic digital representation of a flying object used in lab-testing activities. Since then, the notion of DT has also been adopted in the emerging Industry4.0 for representing the status of production devices and to enable forecast of change impacts. While the concept of DT is so far only being employed for simulation and testing detached from object operation, we see great potential in the incorporation of its usage into an object's operation time (the smart software agent in our case), which will be further on investigated within BIECO. In this way, we can create safe conditions for building reputation via multiple observations of a component's behaviour in specific situations. Within an ecosystem, the reputation of a smart software agent can be built based on collected evidence about the decisions that the smart agent makes in these specific situations.

Finally, dealing with some of the associated challenges to security evaluation, and based on current standards, BIECO will also develop a security certification and evaluation methodology combining security testing and security risk assessment, to obtain a trust level based on the evidence provided by the execution of a series of tests. To this end, BIECO will explore different security metrics that could be measured in an objective way, as well as a set of security claims essential to measure the global security of the system. Based on the certification results, the system will obtain a label and a behaviour profile based on the MUD standard, that will be the link between the design and the runtime phases.

7. Conclusion

The present deliverable provides a description of the State of the Art of the relevant aspects of the Security in a software supply chain. The most widely adopted classification methods of the threats and risks is given together with a high-level description of the main types of cyber-attacks.

Project goals and Requirements are assessed to set the way for a more detailed definition in Deliverable 2.2. KPIs are identified as well, at a high-level definition to prepare the next specific activities focused on the three use-cases of BIECO.

In the last part of the document problems and gaps are considered and expected improvements are described as well.