Security threats, countermeasures, and challenges of digital supply chains

Badis Hammi, Sherali Zeadally, Jamel Nebhen

▶ **To cite this version:**

Badis Hammi, Sherali Zeadally, Jamel Nebhen. Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys, 2023, 55 (14s), pp.1-40. 10.1145/3588999 . hal-04401069

HAL Id: hal-04401069
https://hal.science/hal-04401069

Submitted on 17 Jan 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Security threats, countermeasures, and challenges of digital supply chains

BADIS HAMMI*, EPITA Engineering School, France
SHERALI ZEADALLY, University of Kentucky, USA
JAMEL NEBHEN, Prince Sattam bin Abdulaziz University, KSA

The rapid growth of Information Communication Technologies (ICT) has impacted many fields. In this context, the supply chain has also quickly evolved toward the digital supply chain where digital and electronic technologies have been integrated into every aspect of its end-to-end process. This evolution provides numerous benefits such as profit maximization, loss reduction, and the optimization of supply chain lead times. However, the use of such technologies has also considerably opened up various security threats and risks which have widened the attack surface on the entire end-to-end supply chain. We present a holistic survey on supply chain security. We discuss the different security issues and attacks that target the different supply chain technologies. Then, we discuss various countermeasures and security solutions proposed by academic and industry researchers to mitigate the identified threats. Finally, we provide some recommendations and best practices that can be adopted to achieve a secure supply chain.

Additional Key Words and Phrases: Blockchain, CPS, Countermeasures, Cyberattacks, IIoT, issues, Supply chain cybersecurity

ACM Reference Format:
Badis Hammi, Sherali Zeadally, and Jamel Nebhen. 2023. Security threats, countermeasures, and challenges of digital supply chains. 1, 1 (March 2023), 38 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Supply Chain (SC) is a global network which delivers raw materials, products, and services to end customers through an engineered flow of information, physical distribution, and money. Figure 1.a illustrates a very basic supply chain with three entities: a supplier with one producer and one customer. Four basic flows connect these entities together: (1) a flow of physical materials and services (materials, components, supplies, services and finished products), from the supplier to the end customer, (2) a flow of cash, from the end customer to the raw material supplier, (3) a flow of information (invoices, sales literature, specifications, receipts, orders and rules and regulations), back and forth along the chain, and (4) a reverse flow of products returned (returns for repair, replacements, recycling and disposals.

The Internet has revolutionized the lives of people and is now pervasive in almost all fields of life. In this context, the supply chain is not an exception. Indeed, the Digital Supply Chain (DSC) is the result of the application of information, digital, and electronic technologies to every aspect of the end-to-end supply chain. According to *Xue et al.* [1], digital supply chain systems are inter-organizational systems that firms implement to digitize the processes of transaction and collaboration with their supply chain partners (i.e., upstream suppliers and downstream customers)[2] [2]. These technologies are radically transforming supply chain structures in different sectors, which result in multiple benefits such as (1) profit maximization and loss minimization, (2) the optimization

[1]https://aims.education/study-online/what-is-supply-chain-management-definition/
[2]In the rest of this paper, we use the terms Supply Chain and Digital Supply Chain interchangeably to refer to a Digital Supply Chain

Authors' addresses: Badis Hammi, badis.hammi@epita.fr, EPITA Engineering School, France; Sherali Zeadally, University of Kentucky, USA, szeadally@uky.edu; Jamel Nebhen, j.nebhen@psau.edu.sa, Prince Sattam bin Abdulaziz University, KSA.

© 2023 Association for Computing Machinery.
XXXX-XXXX/2023/3-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

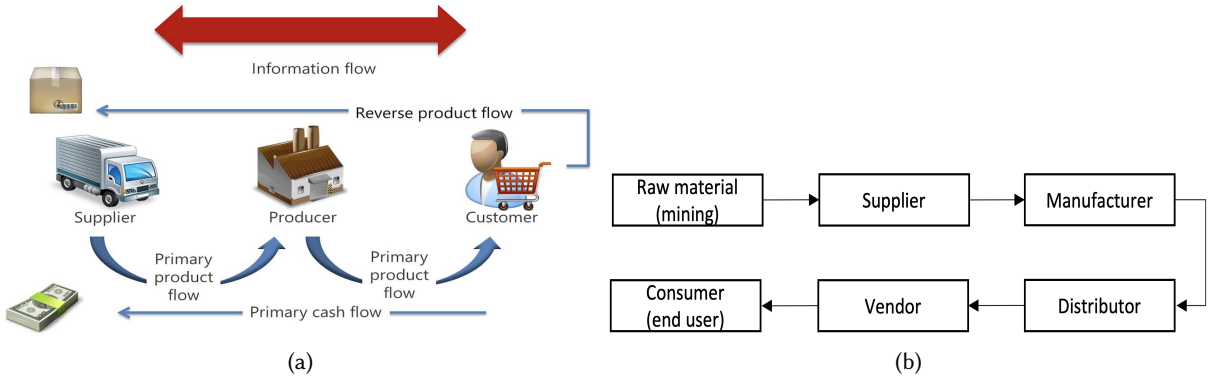


Fig. 1. (a) Basic example of a supply chain [1]; (b) Basic model for supply chain

of supply chain lead times, (3) the enabling of a demand-driven supply chain, (4) the reduction of markdowns and stockouts, (5) improved collaboration among different stakeholders, (6) the connection of data sources and outlets, (7) the utilization of Just-In-Time (JIT) techniques[3], (8) the enabling of a holistic integration of supply chain solutions, and (9) improved cash flows and cost management. However, DSC is vulnerable to a large set of cyberattacks that can range from a simple information theft to complete stoppage of a factory's activities. Indeed, DSC is not a technology, but a collaboration of different technologies and techniques such as the Internet of Things (IoT), cloud computing, networks and telecommunications, and many others. Thus, DSC is vulnerable to the different cyber risks of the underlying technologies.

The discipline which addresses cybersecurity risks that are related to the extended supply chains and supply ecosystems is known as Cyber Supply Chain Risk Management (C-SCRM) [4]. It represents an encompassing function that comprises concepts such as third-party risk management and external dependency management [4]. According to *Boyson et al.* [5], C-SCRM is an overarching discipline which combines cybersecurity, enterprise risk management and supply chain management into a new and powerful concept to provide strategic control over the end-to-end processes of an organization and its extended partners. More precisely, C-SCRM is an interdisciplinary topic that sits at the intersection of: security, cryptography, insurance, telecommunications, computer science, e-commerce, information systems, risk analysis, supply chain management, and operations management [6][7][8].

Research contributions of this work

Table 1 summarizes recently published surveys that have discussed DSC security. We note that the majority of the existing surveys treats the subject from a managerial point of view ignoring the technical part that is of great importance. Furthermore, to the best of our knowledge, all the existing works have considered the supply chain as a single block. However, the supply chain is a set of different techniques and technologies that may change according to the context. Several surveys [9][10] [11][12] have discussed different security issues and countermeasures related to these techniques and technologies such as Industrial Internet of Things or SCADA systems. However, they did not cover all the aspects of the end-to-end supply chain. Thus, there is a need for

[3]JIT or Just-in-Time concept is a manufacturing workflow methodology which aims at reducing costs and flow times within production systems and the distribution of materials. It represents management under which the production is made as per the demand at that particular moment. Therefore, there is no prior production for any anticipated demand which ensures limited wastage, high quality control, adherence to schedules and a seamless continuous throughput [3].

a thorough, in-depth analysis that goes into all details of every part of the supply chain along with a global consideration of the end-to-end process. Finally, there are two aspects of supply chain security, (1) the security of the supply chain processes and infrastructures and (2) the security of the product throughout the supply chain. Most recent studies and surveys have primarily considered only the security of the final products as Table 1 shows. Therefore, there is a need for a study on the security of the supply chain processes, infrastructures, technologies, and links along with their impact on the security of the product.

Survey	Year	Focus on a specific type of DSC?	Considers DSC as a whole (✗) or analyzes all its links (✓)?	Discusses security from a technical or managerial perspective?	Analyzes security solutions designed for DSC?	Limitations
Hintsa *et al.* [13]	2009	No	✗	Managerial	No	- A short paper for the topic - only considers the managerial point of view - Does not cover all the recent works published in the past 12 years
Lu et al. [14]	2013	Yes	✗	Managerial	No	- Focuses on the product and not on the SC - Focuses only on ICT SC - Does not cover all the recent works published in the past 8 years
Bartol et al. [15]	2014	No	✗	Managerial	No	- Only describes the existing standards for SC security
Boyson et al. [5]	2014	No	✗	Technical and managerial	Partially	- Does not cover all the recent works published in the past 7 years
Lu et al. [16]	2017	No	✗	Managerial	No	- Considers only the managerial point of view - Presents only a qualitative study
Iddris et al. [2]	2018	No	✗	Managerial	No	- Considers only the managerial point of view - Presents only a qualitative study
Colicchia et al. [17]	2019	Yes	✗	Managerial	No	- Considers only the managerial point of view - Presents only a qualitative study
Boiko et al. [18]	2019	No	✗	Managerial	No	- 6 pages long, does not cover the majority of security issues
Juma et al. [19]	2019	Yes	✗	Technical	Yes	- Focuses only on blockchain based solutions for SC - Focuses only on trade SC
Ghadge et al. [20]	2019	No	✗	Managerial	No	- Considers only the managerial point of view - Presents only a qualitative study
Hassija et al. [21]	2020	No	✗	Technical and managerial	Yes	- Focuses on the product and not on the SC
Gonczol et al. [22]	2020	No	✗	Technical	Yes	- Focuses only on blockchain based solutions for SC
Zhang et al. [23]	2020	No	✗	Technical	Partially	- Focuses only on blockchain based solutions for SC - Paper is short and does not discuss all relevant existing security issues and solutions
Pandey et al. [24]	2020	No	✗	Technical and managerial	Partially	- Focuses more on the managerial point of view - Does not analyze security solutions from academia or industry
Our survey (this work)	2021	No	✓	Technical and managerial	Yes	We explain below how this work addresses the above weaknesses in these past surveys above

Table 1. Comparison of existing works on supply chain security

Our paper is carefully positioned to avoid overlap with existing surveys by covering areas not considered previously and by considering the entire end-to-end supply chain process from a technical perspective as well as focusing on every aspect of this process.

In this work, we have reviewed various sources of information to identify vulnerabilities, threats, and other relevant security issues pertaining to supply chains. The sources used included many scholarly articles/papers, surveys, books, and case studies all of which were published within the past 15 years. Moreover, given the lack of technical details in this area, we included many technical reports provided by industry in order to provide an in-depth and comprehensive survey that covers, to the best of our knowledge, almost all the works on supply chain security issues as well as the most recent proposed solutions. We summarize the main contributions of this work as follows:

- We present an overview of the supply chain and we analyze its related security threats and issues from two perspectives: (1) at the level of each of the supply chain links, and (2) from a global end-to-end perspective.
- We discuss the security requirements and challenges associated with the supply chain.
- We analyze the different security approaches that have been applied to the supply chain.
- Finally, we outline some recommendations to mitigate the threats we have identified.

2 SUPPLY CHAIN SECURITY ISSUES

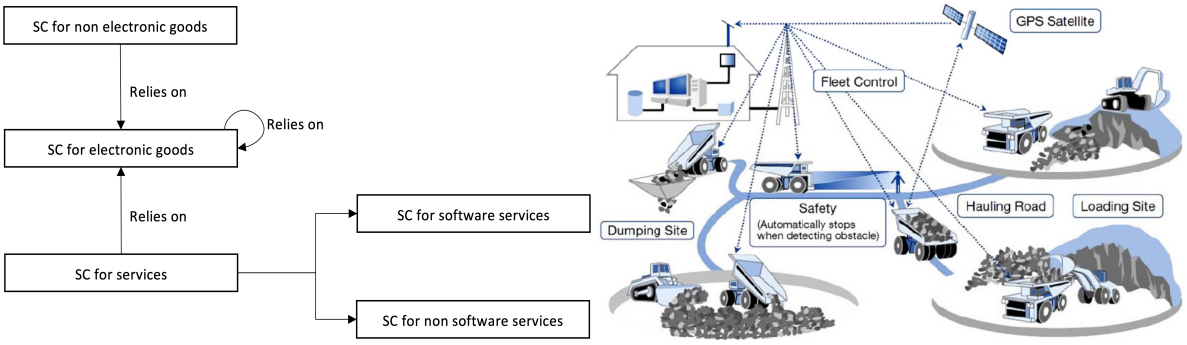
Cyber crime costs organizations $2.9 million every minute according to *RiskIQ research*[4]. According to [25] cybercrime will cost companies worldwide an estimated $10.5 trillion annually by 2025. In this context, supply chain attacks are increasingly popular with attackers because they can access the information of larger organizations or multiple organizations through a single, third-party vendor. According to *Symantec* [26] supply chain attacks were up 78% in 2018. Also, according to [27], supply chain attacks rose by 42% in the first quarter (Q1) of 2021 in the United States (US), compared to the fourth quarter (Q4) of 2020.

This rise in the supply chain cyberattacks is due to the complexity of the digital supply chain. More precisely, the digital supply chain does not comprise of a single technology but rather a set of technologies, techniques, procedures, and policies that are combined to achieve the management of the supply chain. These technologies include, but not limited to, the Internet of Things (IoT), the Industrial Internet of Things (IIoT), Industry 4.0, Cyber Physical Systems (CPS), Supervisory Control And Data Acquisition (SCADA), Industrial Control Systems (ICS), sensor networks, Operational Technology (OT), Information and Communication Technology (ICT), end to end digital connectivity, cloud computing, robotics, machine learning, and so on. Such a wide range of technologies increase the attack surface for the DSC cyberattacks because the DSC is vulnerable to security threats associated with each of them.

For a better understanding of the DSC security issues, we propose the basic model of a supply chain shown in Figure 1.b[5]. In the proposed model we show one actor per supply chain link. However, this does not prevent the consideration of multiple actors (e.g., multiple suppliers, multiple distributors, and so on). Moreover, each link of the supply chain can represent other nested supply chains or parts of it. For example, if we consider the supply chain for the production of computers: at a first level, the manufacturing link describes the computer assembly. However, to reach this step, we need different electronic parts of the computer such as Central Processing Unit (CPU), Random Access Memory (RAM), hard drive, and so on, and each of which follows a similar supply chain. Indeed, if we take the example of the CPU, semi-conductors make up different parts of it. Thus, we need a supply chain for CPU production. Semiconductors in turn are made of raw materials such as *Silicon*. Thus, we need another nested supply chain. The model proposed in Figure 1.b can represent each of these nested supply chains.

The impact, severity, and possibility of cyberattacks differ according to the targeted supply chain and the targeted link in the latter. In other words, a Denial of Service (DoS) attack is possible against the last link of a software supply chain (the end user). However, it is not possible to realize against the last link (the final client) of a milk production supply chain. Similarly, a ransomware attack against a production factory has different consequences from a data theft from one final end user to the complete stoppage of the factory. Figure 2.a shows our proposed taxonomy for supply chains. Thus, we consider four types of supply chains: (1) supply chain for electronic goods (e.g., sensor production, Radio Frequency IDentification (RFID) tag production, computer production); (2) supply chain for non-electronic goods (e.g., food production, real estate); (3) supply chain for software services (e.g., cloud computing services, smartphone applications); (4) supply chain for non-software services (e.g., electricity provision, public administration services). We note that each of the presented types,

[4]https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics
[5]In the rest of this paper, we refer to each step of this model as a supply chain link.
[6]The SC for electronic goods include the ICT supply chain. According to [14], the ICT SC is the foundation of all SC today.



(a) (b)

Fig. 2. (a) Proposed taxonomy for supply chains[6]. SC: Supply Chain; (b) Autonomous haulage system [28]

relies on multiple digital technologies such as IoT, Information Communication Technology (ICT), and so on. Thus, all the supply chain types rely on the supply chain for electronic goods.

In the current strongly connected world, the majority of organizations depend on other organizations for products and services. Nonetheless, while providing many benefits, globalization has resulted in a world where organizations no longer fully control, and often do not have full visibility into the supply ecosystems of the products that they make or the services that they deliver. Therefore, organizations can no longer protect themselves by simply securing their own infrastructures because their electronic perimeter is no longer meaningful [4]. *Hudnurkar et al.* [29] classified supply chain risks into management processes' risks, infrastructure's risks, external environment risks, human resources' risks, and product characteristics' risks. *Singhal et al.* [30] classifies supply chain risks into operational risks, market risks, business risks, and product risks. In the same context, *Shahbaz et al.* [31] classified supply chain issues into process risks, demand risks, logistic risks, collaboration risks, financial risks, and environment risks. Finally, the European Union Agency for Cybersecurity (ENISA) [32] considers supplier side risks and customer side risks. The aforementioned classifications consider supply chain issues from an organizational and managerial perspective. In this work we propose a classification of supply chain issues from a technical perspective. As the supply chain issues are very broad, our classification needs to be comprehensive enough to consider and include all the existing security issues. Therefore, we classify the main supply chain security problems into: (1) counterfeit products issues, (2) cyberattacks, and (3) insider threats. Each of these classes may have several different issues.

Counterfeit products issues and insider threats have been extensively studied by other works [33][34][35]. Hence, in this work we only briefly describe them and focus on the cyberattacks specific to the end-to-end supply chain and we propose a novel taxonomy of supply chain cyberattacks that considers all the links of the supply chain.

2.1 Counterfeit products

As described earlier, a supply chain is a system of systems. The majority of these systems rely on Commercial Off-The-Shelf (COTS) components, which brings numerous advantages such as the reduction of cost and time to market. Moreover, the use of common components increases the interoperability between the different systems and enhances the adoption of the different related standards, if compared to the use of its own proprietary hardware and software [36]. However, the use of COTS in supply chain can lead to severe security issues. One of the main issues is the use of counterfeit components/products. According to the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) the counterfeit trademark goods are those with similar trademarks as the valid ones which makes it difficult to differentiate them from the genuine products

[33]. Indeed, COTS components/devices that are supplied via an un-authorized channel, are not authentic, and would fail a sufficiently rigorous validation. Because of financial gain motivations, counterfeiters buy counterfeit components/devices and supply them as genuine products [36]. Therefore, their negative impacts on each of the supply chain links are often an unintended consequence (e.g., system failure). However, attackers can also use them as an entry point to their target. Indeed, by inserting counterfeit components (hardware or software) during system design and development and across the supply chain, adversaries can gain various advantages such as system control for later remote exploitation or the deployment of malware that will degrade or alter the system's performance, either through presetting or event-triggering [37][38].

According to the European Organization for Economic Cooperation and Development (OECD) [34], the risk of a consumer purchasing counterfeit goods in the United States or the EU is roughly one in 20 and it gets bigger each year. Indeed, according to [39] the amount of total counterfeiting globally reached $1.2 Trillion in 2017 and is expected to double in coming years. To put that in perspective, it represents almost 2% of everything sold worldwide [34].

When counterfeit goods are unknowingly added to supply chains, parts, sub-assemblies and products can be compromised which endanger future systems and consumers that use them. The counterfeit problem concerns all the supply chains and industries. However, the consequences or impact can vary according to the use case. Indeed, using counterfeit components in aerospace, pharmaceutical or defense sectors can lead to more disastrous consequences than the use of counterfeit products in watches or game consoles. For example, in Panama in 2006, because a pharmaceutical supply chain was not properly controlled, the use of a counterfeit component of a medicine caused the death of more than 78 persons [40].

In this paper, because all the digital supply chains depend on digital technologies, and therefore mainly rely on the supply chain for electronic devices as Figure 2.a shows, we focus on counterfeit problem for COTS and electronic devices. Moreover, the scope of this problem is much broader with regard to inner electronic components (e.g., semiconductors, integrated circuits and so on). Next, we discuss some examples.

The US Department of Justice (DoJ) closed a counterfeiting operation of producing, importing, and selling counterfeit *Cisco* computer networking equipments consisting mainly of routers, switches, network cards, and secure communication devices [41]. These routers power government and companies' networks all over the world [5]. Therefore, if these equipments contain backdoors or are vulnerable to security issues, all the traffic that go through them can be easily accessed.

Similarly, in 2005 *X-bit* labs reported that forged hard disk drives similar to *Maxtor Corps MaXline II HDDs* were being sold on the Japanese market [42].

In January 2005, *Advanced Micro Devices (AMD)*, working in cooperation with Taiwanese authorities, seized a total of 60,000 counterfeit *AMD* microprocessors worth $9.46 million during a raid on an electronics company in Tainan [42]. The latter were intended to be sold and implemented in computers.

All domains can be a victim of some counterfeit parts in the large supply chain process, including the rigorous military sector, which can lead to more disastrous consequences. For example, a U.S. naval submarine base in Connecticut, used more than 33 counterfeit semiconductors in repair works that was intended for active-duty nuclear submarines. These counterfeit circuits were used for radio transmissions, alarm panel, submarines' secondary propulsion systems and many other repair works [43][5]. The consequences of the failure of such components could be disastrous.

In October 2006, the Government-Industry Data Exchange Program (GIDEP) issued an alert about a counterfeit silicon-controlled rectifier of *General Electric (GE)* that caused a high failure rate on the Lockheed Martin Missiles and Fire Control [44].

In 2010, *VisionTech Components*, a Florida-based company, sold 60,000 counterfeit integrated circuits from Asia that went into U.S. Department of Defense (DoD) missile programs, U.S. Department of Homeland Security (DHS) radiation detectors, and U.S. Department of Transportation (DoT) high-speed trains [45]. Failures of the

Information Technology (IT) systems that deploy these components in such sectors could lead to catastrophic consequences.

2.2 Cyberattacks

As we have explained above, the supply chain comprises different technologies and it is therefore vulnerable to cyberattacks that target these underlying technologies. Numerous studies such as [46][47][48][49][10][50][11][51][52][53][54][55] discussed these cyberattacks when considered separately by technology (e.g., attacks on Industry 4.0 or attacks on SCADA systems). However, in this work we propose a different taxonomy (as Figure 3 shows) and describe the attacks from a supply chain perspective in order to highlight their impact on each of the DSC links of the model proposed in Figure 1.b. Indeed, because of these attacks, the entire supply chain of the targeted organization (materials and final products, supply chain links, used tools and so on) is at risk. A cyberattack on any of the supply chain's links can easily produce important damages of different types (monetary, asset, capacity and so on) to the targeted organization [28].

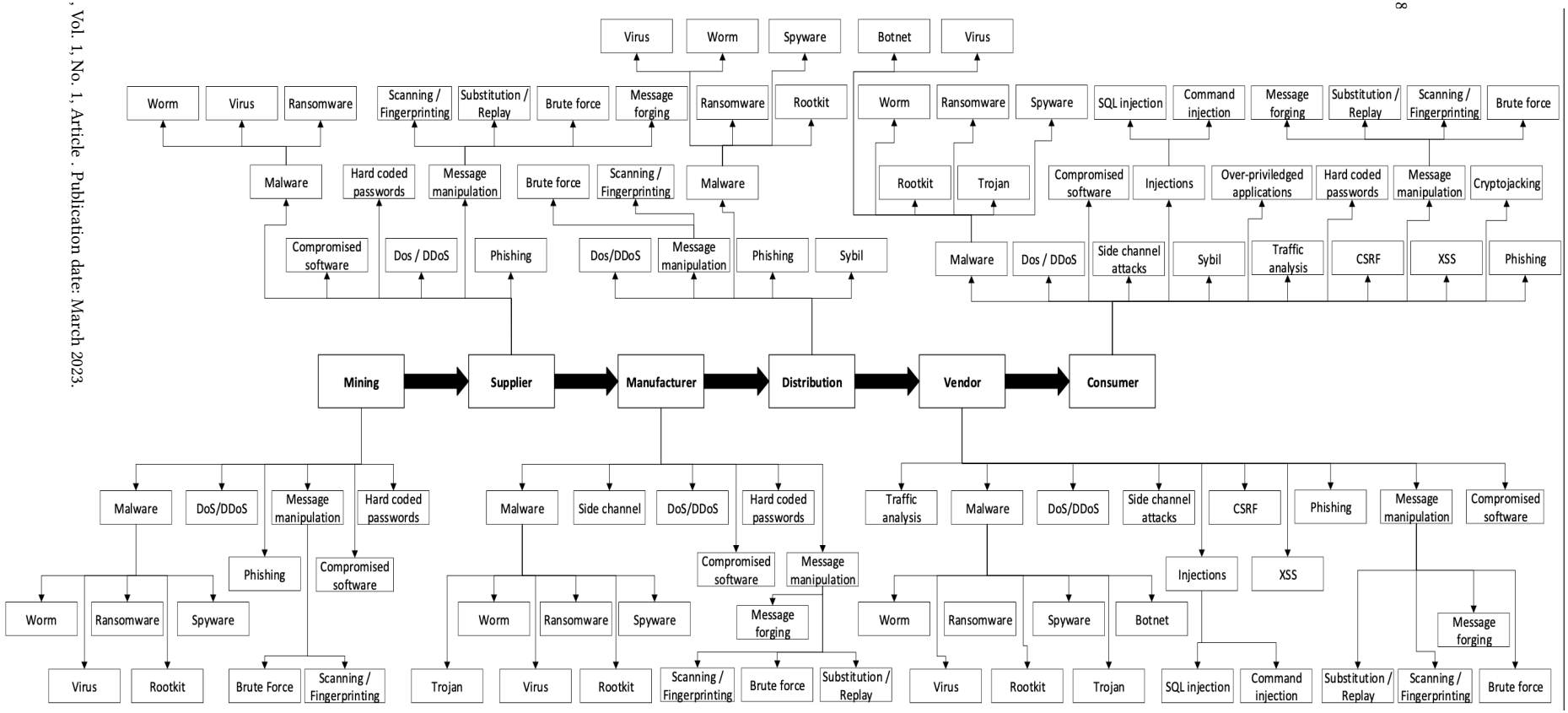


Fig. 3. Taxonomy of cyberattacks for supply chain links (XSS: Cross Site Scripting; CSRF: Cross Site Request Forgery)

2.2.1 Distributed Denial of Service: A Distributed Denial of Service (DDoS) is an attack where an overwhelming number of packets are sent from multiple attack sites to a victim's site. These packets arrive in such a high number that some key resource at the victim (bandwidth, buffers, CPU) quickly becomes exhausted [56][57]. Thus, a DoS/DDoS attack is characterized by the explicit attempt of the attacker to prevent the legitimate use of a service. There are two methods to conduct a DoS/DDoS attack: (1) by exploiting a protocol flaw and (2) by flooding the target. DDoS and especially flooding attacks are among the most dangerous cyberattacks [57][58] and their popularity is due to their high effectiveness against any type of service because they do not require identification and exploitation of protocols' or services' flaws, but only need to flood the target with requests.

In the context of supply chain, two scenarios are possible: (1) the devices that are part of the supply chain can be compromised and be part of a botnet that launches DDoS attacks against targets over the Internet. In this case, the botnet machines (machines of the supply chain) cannot use all their performance capacities to execute their tasks especially for the constrained devices. Moreover, being recognized as the source of attacks can damage the reputation of the company. (2) A service of the supply chain can receive a DDoS attack. The consequences of this case scenario are more disastrous than the first. Indeed, if a service or a step of the supply chain receives a DDoS attack that causes its outage, it will have a domino effect on all the subsequent supply chain steps, which will disrupt the end-to-end supply chain.

Next, we describe the impact of DDoS attacks on the different supply chain links.

Impact on the mining link: Modern mining companies do more than digging the ground to extract metals and minerals after rocks excavation and processing. The modern mining corporation is a complex multinational company that supervises strongly coordinated production tasks running on multiple locations, that are geographically and geopolitically different, all while replying to the supply and demand needs of a market-driven global economy [28]. The mining profession is perilous. Indeed, since the beginning of the mining profession, thousands of accidents such as mine explosions, poisonous gas leaks, structural collapse inside mines, earthquakes, flooding and many others occurred. Fortunately, today, with technological advances, the automation of dangerous tasks have improved safety in the mining sector. Thus, a cyberattack that targets a mine's infrastructure and automated tasks and devices threatens the safety and lives of the working personnel [28]. More precisely, mining[7] equipments rely on a Mining Communications System (MCS) which is a network of devices that receive, collect, or transmit data. The MCS comprise three types of components: (1) transmitters which represent the information source, (2) a network which represent the communication pathway, and (3) the data receivers [28][59]. Numerous mining systems such as autonomous haulage systems, autonomous grinding mills, ball mill drives, mine hoists, dragline excavators, crushers, shovels, bucket wheel and many others rely on these communication technologies (Figure 2.b). Consequently, a denial of service that causes an outage of these systems can be carried out through a direct IT network attack or through a cyberattack that targets the electricity outage. Indeed, a regular and stable electricity supply is vital to the mining sector today. However, electricity is not the sole resource needed. Production mining operations use four major resources to operate: electricity, diesel, water, and compressed air [28]. Thus, an attack against any of these major utilities could cause major disruptions in mining activities thereby affecting the rest of the supply chain, resulting in huge financial losses.

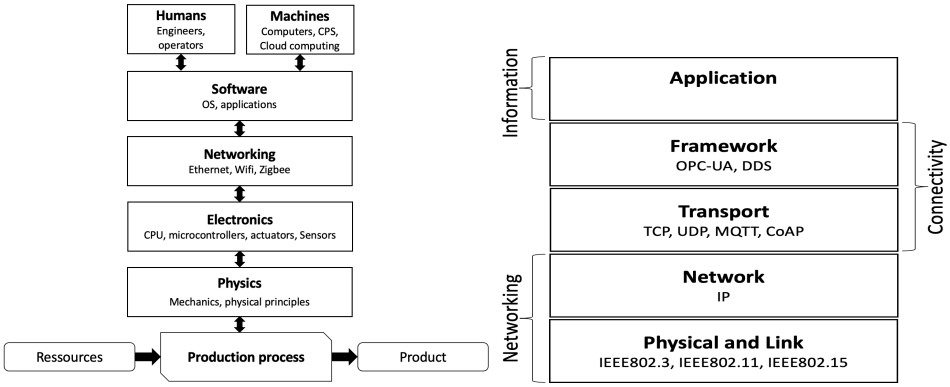
Critical infrastructures such as electrical grid management centers or oil and gas production infrastructures are also part of the mining link and face the same denial of service issues described earlier.

Impact on the supplier link: Suppliers are vital to manufacturers and therefore to the entire supply chain. Indeed, each manufacturer needs different products from numerous suppliers. Generally, the suppliers are small companies with limited resources. Therefore, they are way less protected against cyberattacks than the large major corporations. Numerous studies [60][4] agree that the small suppliers represent the weakest link in the

[7]Mining overlaps with the more complex oil and gas industry. However, from the supply chain perspective, they are part of the same link. Therefore, in this paper, when we discuss mines and mining we also refer to the oil and gas production infrastructures.

supply chain. Thus, if the goal of an attacker is to target an important company via a DDoS attack in order to cause an outage in its production, it can launch the attack by targeting one or more of its suppliers that are less protected. The problem is the same for software supply chains. Indeed, numerous service and software providers use the services of subcontractors. Generally, the subcontractors do not apply the same stringent security policies than their employers, which increases the risk of security breaches.

Impact on the manufacturer link: The manufacturer link is the phase where the products are created, and it is the most important phase. Therefore, a DDoS attack on the manufacturer, completely paralyses the entire supply chain. Unfortunately, DDoS is a recurrent issue for ICS, IIoT and SCADA [49][10][61][62][63][64].



(a) (b)

Fig. 4. (a) Cyberphysical Production System (CPPS) architecture; (b) Network stack for IIoT.

Indeed, the number of computation components integrated into industrial control systems, production systems, and factories is continuously increasing and currently, millions of embedded devices are used in safety and security critical applications in such environments. In theory, such devices must communicate over closed industrial communication networks. However, many of them are increasingly being connected to the Internet [61] which makes them suitable targets for network attacks and thus to DDoS attacks. Figure 4.a depicts a Cyber-physical Production System (CPPS) architecture [61]. The networking layer defines how the different components communicate in order to achieve manufacturing tasks and is composed of multiple sublayers according to the context and technology (e.g., IIoT, SCADA) [65][66][67]. For example, Figure 4.b shows the network stack for IIoT [65]. The latter implements multiple protocols such as Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), Open Platform Communications Unified Architecture (OPC UA), Data Distribution Service (DDS) and many others. All these protocols increase the DDoS attack vector on the underlying infrastructures either through flooding or protocol flaws as we stated above.

Impact on the distribution link: In a supply chain, the distribution task is provided by one or more companies. These companies are organizations that have their own employees, infrastructures, policies, and so on. Like any other organization, a distribution company relies on some computing/networking infrastructure. The latter could be the target of any possible DDoS attack. As a result, the distribution activity could stop which can lead to a shortage for the vendor side although the manufacturers are providing products.

Software and network services are often provided through the Internet. Therefore, their distribution is ensured by network infrastructures connected to the Internet. A DDoS attack against these infrastructures or some of their components such as the routers or some critical servers (e.g., Domain Name System (DNS) servers) can disrupt or

[7]The SC for electronic goods include the ICT supply chain. According to [14], the ICT SC is the foundation of all SC today.

stop the offered services. According to the F5 Security Incident Response Team (F5 SIRT) [68] the most common attack for service providers is DDoS, at 77% of reported incidents in 2019. For example, the Internet Service Provider (ISP) *Cool Ideas* has been the target of a DDoS attack in 2019 that has severely degraded performance on its network, even causing an hours-long outage[8]. In the same context, in 2019, the ISP *Atomic Access* was also the target of two large-scale DDoS attacks in two months.

Even worse, the distribution network services can be disturbed as a side effect of a huge DDoS attack. More precisely, large-scale DDoS attacks use routers and network services of legitimate ISPs and Autonomous Systems (AS) which directly affect their users. These DDoS attacks can saturate the network used and cause significant outages of legitimate services' distribution over these infrastructures like it was the case for the attack against *Spamhaus* [69] or the *Dyn Mirai* DDoS attack that slowed down the Internet across the world[9][10]. Finally, some services such as DNS or Network Time Protocol (NTP) can be involved in amplification/reflection of DDoS attacks, which also leads to the exhaustion of network bandwidth used for the distribution of legitimate services and their disruption.

Impact on the vendor link: Online services are currently a fact of life and pertinent to nearly all aspects of our daily lives and the covid 19 pandemic has merely accentuated this fact. Online services are target to different kinds of cyberattacks. But, the DDoS attacks are among the most common attacks as confirmed continuously by the numerous quarterly and annual reports issued by security companies such as *Kaspersky, Netscout, Cloudflare and Akamai*. In this context, supply chain vendors such as e-commerce companies or service providers are among the first choice targets for attackers. For example, in 2020 we witnessed the largest DDoS attack in history which targeted *Amazon* with 2.3 Tbps [70]. Another massive attack that took place in 2020 targeted *Neustar* with 1.17 Tbps [70]. Also according to *koddos*[11], DDoS attacks on e-commerce rose by more than 400% in Europe during the pandemic. Worldwide, compared to the first quarter in 2019, DDoS attacks rose by over 278% in the first quarter 2020. However, the increase between the third quarter 2019 and the first quarter in 2020 skyrocketed to 542% according to *Nexusguard* [71]. During the covid 19 pandemic, as consumers and workers became more dependent on online services to meet their various obligations, we witnessed a sharp increase in DDoS attacks. *Netscout Threat Intelligence* saw 4.83 million DDoS attacks in the first half of 2020. This is roughly 26,000 attacks a day or 18 attacks per minute [72]. *Bulletproof* [73] stated that a DoS or DDoS attack could cost up to $120,000 for a small company or more than $2 million for a large enterprise. According to [74], the total cost of DDoS attacks in the United Kingdom alone was around $1.3 billion in 2019. According to *Netscout* [75] a DDoS victim company loses $218,339 on average in the United States, which amounts to an excess of $10 billion lost in the United States annually. These numbers do not vary a lot according to the numerous other DDoS surveys/studies [76][77][70][78][79]. Moreover, all these studies, surveys and technical reports agree that the majority of online vendors have already experienced multiple DDoS attacks and continue to suffer from them, which makes DDoS attacks one of the major cyberattacks on the vendor link of a supply chain.

Cloud Service Providers (CSP) and vendors are also main targets to a great variety of DDoS attacks as *Masdari et al.* [80] has highlighted. Indeed, cloud computing services are used by most IT services consumers (companies or simple end users). Cloud statistics show increased adoption rates but also growing security concerns [81]. For example, according to [82] 35.14% of all attacks on cloud were DDoS attacks in 2015, which makes DDoS one of the top nine threats to cloud computing according to [74]. This is because the attack surface on the cloud is very wide. In fact, in addition to the network layer, transport layer, and application layer DDoS attacks, numerous other attacks are possible on the cloud components as [80] discussed.

[8]https://mybroadband.co.za/news/internet/320911-ddos-attacks-can-wipe-south-african-isps-off-the-internet.html
[9]https://krypsys.com/news/ddos-attack-on-spamhaus-biggest-network-security-attack-in-history-slows-down-internet-access-across-the
[10]https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet
[11]https://blog.koddos.net/ddos-attacks-on-e-commerce-in-europe-rose-by-400-during-the-pandemic/statstat

DDoS attacks are cyberwarfare tools. Since the supply chain vendors directly interact with end-users, a DDoS attack that targets some key vendors can lead to disastrous consequences such as what occurred in Estonia in 2007, on Georgia in 2008 and on Kyrgyzstan in 2009 [83][84][85]. For example, in Estonia, online services of key vendors such as banks, media outlets, and government bodies were taken down by a DDoS attack using unprecedented levels of Internet traffic. The result, for Estonians citizens, was that cash machines and online banking services were sporadically out of service; government employees were unable to communicate with each other, and newspapers and broadcasters suddenly found they could not deliver the news. All these disruptions led the country into an unprecedented crisis [86].

Impact on the consumer link: DDoS attacks on the consumers have less serious effects on the supply chain process than the attacks on other links because they do not stop the whole chain. However, in some cases, it could have disastrous consequences on the end users. For example, if we consider the smart homes use case, numerous DoS/DDoS scenarios are possible on the home devices to prevent them from performing their tasks such as sensing, monitoring or processing. A DoS attack that targets a motion sensor has a different consequence from a DoS attack that targets a smart fridge leading to food waste, which in turn has different consequences from a DoS/DDoS attack that targets a healthcare system, that can have disastrous consequences on the patient's life [87]. In some cases, the DoS/DDoS attack can paralyze the whole smart home system. Such cases include: (1) a DoS/DDoS on the Command and Control (C&C) unit (in the case of a centralized smart home architecture), (2) a DoS/DDoS attack that targets the Internet router access will affect all services (such as cloud-based applications) that rely on the Internet, and (3) a DoS/DDoS attack that targets the grid's smart meter will disrupt the electricity supply to the house which in turn disables all the services provided by the majority of devices. There are numerous other case scenarios in addition to smart homes where DDoS attacks can impact consumers. For example, Collaborative Intelligent transportation systems (C-ITS) [88][89], Wireless Sensor Networks (WSN) [90] and many others.

Software also represents an attack vector against consumers. Indeed, software defects are often measured in terms of the number of flaws per one thousand lines of code [36]. These vulnerabilities in the software are inadvertently incorporated into products during design or implementation. They are also called unintended taint and represent vulnerabilities that can be exploited by hackers to realize numerous attacks, and DoS attacks are one of them. Open source software represents a steal for hackers because they have the source code and they can find vulnerabilities which can be used to execute DoS attacks as it was the case for the ping of death attack, the land attack, Shellshock and many others. Indeed, according to *Sonatype*, supply chain attacks on open-source software surged by 430% over the last year [91].

2.2.2 Malware. Malware is an important threat against supply chain security according to [26]. Malware types such as ransomware and viruses can have disastrous consequences. The best example is how *Wannacry* crippled the world wide economy by spreading into key infrastructures of more than 150 countries and causing economic losses that could reach up to $4 billion according to [92]. Ransomware threats will continue to increase in the future. Indeed, according to the security research firm *Cybersecurity Ventures* [93], a business falls victim to a ransomware attack every 11 seconds and global annual ransomware damage costs reach $20 billion.

Impact on the mining link: Malware developers are showing increasing interests in supply chain. In this context, the mining link is not an exception, but quite the contrary. Indeed, numerous types of malware targeted mines and energy infrastructures. Their goals vary from espionage (spyware and backdoors) to sabotage (viruses and worms). For example, *BlackEnergy*, originally created only for industrial espionage, has been reused to inflict physical damage on industrial important infrastructures. *BlackEnergy* and another Advanced Persistent Threat (APT) namely, *Sandworm*, were identified as the potential cause of disruption at two power generation installations in Ukraine in December 2015 [94], making hundreds of thousands of Ukrainian homes temporarily in the dark in the first confirmed cyberattack against an electric grid [95]. Moreover, *BlackEnergy* and *KillDisk*

were identified in comparable cyberattacks attempts that targeted a mining corporation and a large railway operator also in Ukraine [96]. Which demonstrates that *BlackEnergy* has evolved from being a malware that attacks only facilities in the energy sector to be a threat against the facilities in other fields (e.g., mining) [28].

The mining industry is often targeted through its own infrastructure and therefore through its supply chain. Indeed, SCADA, MCS and ICS systems are often the entry points for attackers. The best example is *Stuxnet* which is the first publicly known worm to target industrial control systems. More precisely, it was designed to attack industrial Programmable Logic Controllers (PLC), which allows for automation of processes in machinery and specifically aimed at those developed by *Siemens*. Over fifteen Iranian facilities were attacked and infiltrated by the *Stuxnet* worm [97]. It also included a zero-day vulnerability to spread via Universal Serial Bus (USB) sticks, a Windows rootkit to hide its binary components, and it signed its files with certificates stolen from other unrelated third-party companies [98]. *Stuxnet* mainly targeted the uranium enrichment infrastructure in Iran. It targeted the uranium centrifuges causing their destruction [99]. It is currently estimated that the *Stuxnet* worm destroyed 984 uranium enriching centrifuges constituted a 30% decrease in enrichment efficiency [97][100].

Duqu is another worm related to *Stuxnet*. According to *Symantec* [101], the worm is nearly identical to *Stuxnet*, but with a completely different purpose, that is to capture information such as keystrokes and system information [102]. The exfiltrated data may be used to enable a future Stuxnet-like attack [103].

In 2014, researchers [104][36] identified an attack campaign that targeted energy sector institutions through the dissemination of a malware called *Havex* via various supply chain channels. Hackers infected the website of a law company specialized in the energy sector, which allowed the dissemination of the malware to numerous site visitors, mainly several energy companies. The attackers also embedded *Havex* into software updates that were managed by a supply chain vendor, leading its clients to install *Havex* directly on ICS systems. Which permitted the attackers the grant of important access to various energy operators' Information Technology (IT) and Operational Technology (OT) environments, with payloads that can allow the full exploitation of such infrastructures with high privileges. Moreover, this type of malware can be easily modified to cause havoc such as data destruction or denial of service [36].

In the same context, in August 2017, a malware dubbed *Triton* attacked petrochemical facilities in what is the first-ever example of malware targeting the safety instrumented system designed to prevent a disaster at an industrial facility [105]. This caused the plants to shut down for more than a week [106]. It is worth noting that in 2012 the wiper malware Shamoon was used in attacks that performed data wiping tasks. Other variants such as Shamoon 2 and Shamoon 3 appeared in 2016 and 2018[12] [107].

Impact on the supplier link: As described earlier, suppliers are generally smaller/mid-sized businesses and represent the weakest link in the supply chain when big companies are targeted. According to [108], there is a higher probability for small businesses to be targeted by cyberattacks compared to big companies. For example, over 50% of all breaches in 2020 concerned small companies, which represent nearly 100% rise from 2019, when small businesses were the target 28% of the time. To illustrate this point, we cite the example of the aeronautical equipment manufacturer *Asco*. In 2019, the latter was paralyzed by a cyberattack that forced the company to put a thousand of its employees on technical unemployment, out of a total of 1,500 in what was considered as the third incident of this type recorded in the aeronautical sector since the beginning of the year. *Asco* manufactures high precision components for airplanes such as the mechanism allowing the retraction and extension of wing flaps for example, it supplies *Airbus, Boeing, Bombardier* and *Lockheed Martin*. During this attack, several sites were affected by a ransomware; in the United States, Canada, Germany and Belgium, the shutdown of the Zaventem plant caused enormous delays in the whole production supply chain[13]. According to an investigation of *Agence*

[12]https://attack.mitre.org/software/S0140/

[13]https://www.lesechos.fr/industrie-services/air-defense/aeronautique-un-sous-traitant-dairbus-et-boeing-paralyse-par-une-cyberattaque-1029704

France-Presse (AFP), Airbus has always been the target of several cyberattacks perpetrated through subcontractors and suppliers of the manufacturer, mainly for espionage purposes[14]. According to the same investigation, other cyberattacks have targeted the French technology consultancy group *Expleo* (formerly known as *Assystem*), the British engine manufacturer *Rolls-Royce*, and two other *Airbus* suppliers. The attack on *Expleo* was discovered at the end of 2018, but the infection was much older. Very sophisticated, it targeted the Virtual Private Network (VPN) that connected the company to Airbus. Successfully penetrating a VPN theoretically opens the doors to all parts of the network. The other attacks followed a similar pattern: attacking the supplier, then entering the aeronautics giant, taking advantage of the subcontractor's access to the *Airbus* system. According to AFP, the first of the infections was detected at the British subsidiary of *Assystem* and at *Rolls Royce*, allowing further attacks at *Assystem* France and *Airbus* to come to light.

Impact on the manufacturer link: Industrial control systems are highly distributed information systems used to control and monitor critical infrastructures such as plants and facilities. The main architectural design characteristics of ICS are real time response, high availability, and reliability. To achieve these goals, several protocols [109] have been designed (described in Section 2.2.1). With increasing connectivity to the Internet for various reasons, ICS adopted Internet based technologies and most of communication protocols have been redesigned to work over IP [51]. This openness increases the attack surface of ICS components as well as communication protocols with a higher risk than attacks on traditional IT systems [51], especially that most of the world's critical ICS infrastructures still use legacy technologies that are vulnerable to simple cyberattacks [110]. In this context, a key issue is that ICS and, especially SCADA communication protocols (e.g., Modbus, Process Field Bus (Profibus) and Distributed Network Protocol 3 (DNP3)) are different from their ICT counterparts; this is largely due to the fact that they were designed at a time when industrial control systems were completely isolated from public networks and ICT-based intrusion scenarios were considered to be very unlikely [111].

In recent years, cyberattacks targeting ICS belonging to different critical infrastructures have been identified and malware attacks are among top threats and security issues for such infrastructures [112][10][110][50]. Furthermore, numerous IoT-based devices are integrated into these ICS infrastructures for effective communication and modernization purposes, which increases the malware attack surface [110][50].

There are various types of malware such as *Stuxnet , Havex, BlackEnergy3, Industroyer* and *Wannacry* described earlier that have been used to launch attacks against ICS systems. In the same context, *Fovino et al.* [111] presented a Modbus worm that exploits the lack of authentication and integrity vulnerabilities in the Modbus protocol. The worm performs two attacks: DoS, by identifying sensors or actuators and sending them DoS-inducing messages, and command injection, by sending unauthorized commands to the sensors or actuators.

ICSs are the target of different types of malware; virus, worm, spyware, and so on. However, in recent years, we have witnessed an increasing trend related to ransomware attacks [113]. According to *Mehrfeld et al.* [113] malware and ransomware can affect ICS in different ways: (1) it infects only the system's upper layers (e.g., Human Machine Interface (HMI), application layer. and so on). Thus, data and systems relevant for production are still available. However, impairments in IT systems such as invoicing and the processing of orders, production orders, production planning or warehousing are affected. If problems persist, it can also affect production because no new orders or planning can be received. Moreover, often production systems have to be shut down to protect them from infection. (2) the complete ICS is affected by the ransomware at all the layers. Hence, the interruption of the production process will be necessary for the removal of the ransomware and the restoring of the system. Depending on the production environment, certifications or other documentation must be updated and validated before ramping up the production. This is the case for sensitive and critical industries such as pharmaceutical, nuclear or military [113]. One such example is the *Locker Goga* ransomware attack on the Norwegian company *Norsk Hydro* in March 2019 [114][115]. To prevent further spread of the ransomware, all central services were shut

[14]https://www.frenchweb.fr/comment-des-hackers-attaquent-airbus-en-passant-par-ses-sous-traitants/377231

down and employees were not allowed to start their office workstations [113]. In particular, the use of automated processes was no longer possible and the employees had to switch to manual mode and paper processes again. The most severe and for the longest time damage hit the Building Systems division, responsible for the manufacturing of customer-specific products[15]. In the same context, a massive ransomware attack (with a ransomware dubbed *Petrwrap*) paralyzed the French industry giant *Saint Gobain*. In both of these attacks the financial losses were very high.

Impact on the distribution link: Malware can seriously affect the supply chain's distribution link and past malware attacks against distributors demonstrate this. For example, the distribution giant *FedEx* was hit by *Wannacry*[16] and by *NotPetya*[17] which heavily affected its delivery capacity, costing the company losses reaching $670 million[18]. *NotPetya* has also hit the Copenhagen-based shipping giant *A.P. Moller-Maersk*, which moves about one-fifth of the world's freight. Operations at *Maersk* terminals in four different countries were impacted, causing delays and disruption that lasted weeks which caused losses which amounted to $ 300 million.

The distribution link in the energy sector is also heavily suffering from malware. Indeed, whether it is a grid power distribution network or a gas/oil pipeline, they are targets of malwares and cyberattacks. In this context, in May 2021 a ransomware[19] shut one of the USA's largest oil pipelines, the 8850 Km *Colonial Pipeline*, which carries 100 million gallons a day of refined fuels between Houston, Texas, and New York Harbor, or 45 percent of all fuel needed on the USA's East Coast, leading the nation's Federal Motor Carrier Safety Administration to issue a regional emergency declaration permitting the transport of fuel by road[20].

The network infrastructure used for the distribution of software and network services is also prone to malware attacks that can have numerous consequences such as passive traffic eavesdropping for espionage, tampering with the offered services or causing damages on network components. In this context, there are numerous malware attacks against routers. *SYNful Knock* allows a stealthy modification of the router's firmware image that can be used to execute various functional modules and maintain persistence within a victim's network while gaining total access through the use of a backdoor password. Those modules are enabled via the HyperText Transfer Protocol (HTTP) protocol using Transmission Control Packets (TCP) packets sent to the interface of the router [116]. This particular process consists of a three-way handshake to be initiated and then completed. A uniquely crafted TCP SYN packet is sent to the targeted device, then the malware responds with a TCP SYN-ACK acknowledgement message of its own, which is answered by a third message to complete the counterfeit three-way handshake process[21] [116]. Once in, attackers can monitor both outgoing and incoming traffic, as well as load additional malicious modules. As the infection is done at the firmware level, resetting or powering down the router does not remove the threat. The only solution is to re-image the hardware with the original Internetwork Operating System (IOS)[22].

Another example is *VPNFilter* which is considered as one of the most notorious router malwares [117]. It has infected more than half a million routers and network-attached storage drives in more than 50 countries since 2016. This virus exploited known system vulnerabilities to install malware on affected devices and even steal users' sensitive information (e.g., passwords and credit card details). The malware is persistent even after a system reboot, making it difficult to eradicate [118].

[15]https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/
[16]https://www.wate.com/news/national-world/fedex-hit-by-wannacry-ransomware/
[17]https://www.securityweek.com/fedex-may-have-permanently-lost-data-encrypted-notpetya
[18]https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906
[19]https://www.energyclimatecounsel.com/2021/05/13/colonial-pipeline-cyberattack-highlights-vulnerability-of-nations-energy-sector/
[20]https://www.theregister.com/2021/05/10/colonial_pipeline_ransomware/?td=keepreading-top
[21]https://sensorstechforum.com/200-cisco-routers-infected-with-synful-knock-malware/
[22]https://esj.com/articles/2015/09/18/cisco-router-malware.aspx

Impact on the vendor and consumer links: The vendors and consumers are frequently the first target of malware attacks especially those that use automated propagation mechanisms. Knowing that vendor infrastructures as well as consumer systems are mostly managed by humans, it makes them more vulnerable to such attacks. However, their impact on the supply chain is very different. Indeed, attacking a vendor direct consequences on the supply chain because it represents a very important link. However, even if the impact of malware attacks on consumers is not disastrous for the supply chain continuity, it has severe consequences and losses on consumers.

According to [108], 86% of cyberattacks are financially motivated. Malwares do not deviate from this trend and ransomware are by far the most used in such attacks. Indeed, 304 million ransomware attacks occurred in 2020 representing a 62% increase compared to 2019 according to [119]. This number rose by 11% at the mid-year of 2022 compared to 2021 [120]. According to [121] the combined cost of 2022's ransomware incidents will reach $20 billion. Indeed, malware attacks and more specifically ransomware attacks are often present in the news. IT businesses/enterprises and all other sectors are often victims of such attacks. Some of the latest attacks include: a ransomware attack in 2020 on New Orleans cost the city around $7 million[23]. All servers were taken offline due to the attack, except the servers of the essential services. In May 2019 the servers of the city of Baltimore were largely compromised by the ransomware variant called *Robinhood*. This dangerous attack caused financial damage of up to $18.2 million. In February 2020, a ransomware infection cost the Danish corporation *ISS* around $50 million of damages [122].

In the case of most malware attacks, there are some of them that stand out the most. *Emotet* is one of these examples which is considered by the US Department of Justice as one of the top cyber threats in the world which caused hundreds of millions of losses worldwide[123]. *Emotet* is a variant of the online banking trojan *Cridex* (also known as *Bugat* or *Feodo*). *Emotet* actually consists of a series of several malware programs that together cause different damages. More precisely, it has a modular structure. An infection initially installs a core component of the malicious program, which could then reload modules for various malicious functions or other malware programs such as *Trickbot* or the ransomware *Ryuk*. This included modules for attacks on online banking, spying on access data from e-mail clients and web browsers, reading out Outlook address books, sending spam and carrying out DDoS attacks. The banking module now (like some other banking Trojan families) used the so-called web injects [124]. During online banking, they dynamically insert additional input fields in the user's web browser to query Transaction Authentication Numbers (TANs) in order to carry out transfers in the background. They also suppressed security warnings from the bank.

Another security issue which is a major concern of consumers is the mobile application malware attack. Over 24,000 malicious mobile apps are blocked daily [125], a volume that guarantees at least a few malicious apps are getting through. According to [77][126] more than 45,000 malicious apps were identified in 2020 with 23% available on *GooglePlay*. In 2020, *Kaspersky* mobile products and technologies [127] detected 5,683,694 malicious installation packages, 156,710 new mobile banking Trojans, 20,708 new mobile ransomware Trojans. For example, recently in 2020/2021, a new trend of tracking COVID-19 cases began using mobile apps which have opened up opportunities for cybercriminals to launch cyberattacks. One such application was infected with a ransomware called *CovidLock*; once the user installs the application, *CovidLock* encrypts key data on its android device. It denies all access to the victim until he/she pays the requested ransom[24]. Indeed, people rely heavily on their mobile phones and many other IoT devices for daily tasks. However, the latter are known to be vulnerable systems to cyberattacks, which increase the impact of cyberattacks on the consumer link .

Another domain where attacks on the vendor and consumer links could be disastrous is electronic health (e-health). The latter relies heavily on IoT, Wireless Area Body Networks (WBANs) and cloud services, which provide a large attack surface. Unfortunately, malware attacks often target e-health systems. A recent report

[23]https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[24]https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware

[128] predicts that cyberattacks will cost the health sector $347 billion between 2019 and 2023. According to [129] healthcare cyberattacks doubled in 2020, with 28% tied to ransomware. In the same context, French hospitals have been the target by 192 cyberattacks in 2020 (versus 54 in 2019) mainly DDoS and ransomware attacks (mainly *Ryuk* and *Egregor*). Among these cyberattacks, 27 of them have completely paralyzed health services. Attacks on e-health represent 11% of cyberattacks recorded in France in 2020. A similar trend was noted at the start of 2021 because according to the minister of digital transition, there is at least one per week since the start of 2021. Another example occurred in 2019 when the U.S. was hit by an unprecedented number of ransomware attacks. The attacks impacted no less than 966 government agencies, educational establishments and healthcare providers. The costs of the attacks amount to more than $7.5 billion [130]. The affected organizations included 113 state and municipal governments and agencies, 764 healthcare providers, and 89 universities, colleges, and school districts. Regarding hospitals and health infrastructures, the problems caused by the attacks were not limited to the financial loss but they also caused disruptions that threatened peoples' health, safety and lives. Emergency patients had to be redirected to other hospitals. The attacks also caused the inaccessibility to medical records, and, in some cases, their permanent loss. They also caused the cancellation of surgical procedures, the postponing of medical tests, the cessation of admissions, and the interruption of 911 services. Dispatch centers had to rely on printed maps and paper logs to keep track of emergency responders in the field. Police services lost the access to background check. Therefore, they were not able to obtain details about criminal histories or active warrants. The attacks also caused the deactivation of surveillance systems, the deactivation of badge scanners and building access systems, and the deactivation of remote control of jail doors. Schools could not access data about students' medications or allergies. There are many other disruptions and effects that have been observed which are common to almost all ransomware attacks such as websites going offline. The inaccessibility of online payment portals. The cessation of email and phone systems. The delay of payments to vendors. The closing of schools. The stoppage of property transactions. The loss of students' grades. The incapacity of issuance of utility bills. The delays by months of grants to nonprofits. The non renewal or issuance of driver's licenses. And the extension of tax payment deadlines.

2.2.3 Default/hardcoded credentials . Hardcoded credentials represent one of the main security issues in different systems like IIoT, IoT and ICS [36][10][131] which can lead to security issues at the different links of the supply chain. As the CTO of *VMware, Ray O'Farrell* attested before Congress, *"a hardcoded password effectively means you have no password."*[25]

Hardcoded passwords fall into a vulnerability class known as unintended taint[26]. *Woods et al.* [36] consider the majority of ICS systems as "insecure by design" mainly because of the unintended taint problem. In fact, organisations often need the remote management of their systems. Manufacturers realize it through hardcoded credentials which ensure an easy access to the system, without a complex procedure, especially in the case of an emergency. Unfortunately, what can facilitate the tasks for operators, can be misused to cause harm if used by attackers or unskilled users. In order to ensure access control, the used credentials must remain secret. Paradoxically, they must be provided to a large number of legitimate users, and even worse, they are often published in operating manuals.

If we look at the consumer link or the devices that are used in the other supply chain links, when consumers buy IoT devices, they are often set up with hardcoded credentials, generally in the form of a username and a password. These credentials are often available on the vendor's website and are frequently easily guessable, which facilitate unauthorized access to them via different cyberattacks such as data identity theft, social engineering,

[25]Cybersecurity of the Internet of Things, Subcommittee on Information Technology Hearing, October 3, 2017, (testimony of Ray O'Farrell) https://oversight.house.gov/legislation/hearings/subcommittee-on-the-information-technology-hearing-cybersecurity-of-the

[26]Authentic components which have been previously validated but have some software flaws or vulnerabilities that are unintentionally inserted into them (the designer can be aware or unaware of them) [36].

access to IoT cshell service (reverse shell), insecure web services and more [131]. It also allows malware such as *Mirai* [132] to compromise IoT devices and exploit them for data exfiltration or to execute various attacks such as buffer overflows, Structured Query Language (SQL) injection, Remote Code Execution (RCE), remote code injection, Distributed Denial of Service (DDoS), and so on [133]. Indeed, by leveraging IoT devices, hackers built a large botnet using *Mirai* malware in 2016. The *Mirai* botnet has been used in some of the largest and most disruptive DDoS attacks against numerous actors of the supply chain vendor link. More precisely, the *Mirai* botnet targeted the servers of *Dyn*, a company that controls much of the Internet's DNS infrastructure. It was hit on October 21^{st}, 2016 and was flooded by 1.7 Tbps of traffic [134][135][136][137], and remained under sustained attack for most of the day, bringing down sites such as *Twitter, the Guardian, The New York Times, Netflix, HBO, Spotify, Reddit, PlayStation Network, GitHub, CNN* and many others in Europe and the US. *Mirai* employed a dictionary attack that uses a dictionary of only 62 possible username/password pairs that are common to IoT devices. The high success of Mirai is due to the default and hard coded passwords which are often easily guessable ones. For example, the password management company *SplashData* evaluated more than five million passwords leaked on the Internet during the previous years and compiled the top 100 worst passwords for 2018. Surprisingly, for the fifth straight year, the top spots (#1 and #2) in the annual worst-of-the-worst list remain unchanged: "123456" and "password" respectively [138][139].

2.2.4 Scanning attack. Each cyberattack requires different phases. One of the most important phases is the identification of the potential victims which is achieved through scanning. Unfortunately, it is easy for the hackers to find vulnerable devices and services, especially ICS and IoT devices using existing scanning tools such as *Zmap* or *Censys*, and other online tools such as *Thingful* which serve for data collection from connected machines and IoT devices. However, *Shodan* is considered to be the best because of its intuitive web interface and easy to use Application Programming Interface (API) [140][141].

Shodan [142] is one of the most popular search engines available today, designed to crawl the Internet and to index discovered services [141]. Thus, it includes information about systems and devices connected to the Internet. By using different types and categories of search queries, users can extract information about those systems/devices. In many cases, users of those systems may not be aware of the amount of information that is publicly exposed about their systems. These systems are usually installed according to the manufacturers' installation manuals, and in many cases, users may keep default settings designed by manufacturers [143][142]. For example, researchers from *Bitdefender* used *Shodan* to detect more than 100,000 Internet-connected security cameras that contain a security vulnerability which allows them to be accessed via the open web and used for surveillance, roped into a malicious botnet, or even exploited to hijack other devices on the same network [144][145]. Two cameras manufactured by *Shenzhen Neo Electronics*, China, were found to permit attacks without even logging into the system to gain unauthorized access [144]. ICS systems that are increasingly connected to the Internet are facing the same challenge. For example, *Huq et al.* [28] conducted searches through *Shodan* to identify Human-Machine Interfaces (HMI) used to control ICS systems that are exposed to the Internet and are vulnerable to compromise. They got access to different HMIs such as those which control carbon dioxide (CO2) sensors, water pumps, milling machines, water treatment facility, conveyor belts and many other. *Shodan* represents a publicly available search engine and any user can use it to obtain information about exposed ICS systems and get access to them. Therefore, a malicious user can without a difficulty misuse the obtained information and access to attack the vulnerable systems.

2.2.5 Software supply chain attacks. Supply chain links rely on different systems in order to execute different tasks. These systems contain thousands of software components, supplied by various provisioners, each with a different degree of integrity and safety. The defect rate of a software is quantified according to the number of taints per one thousand lines of code [36]. Systems have generally tens of millions of code lines. Therefore, they represent thousands of possible vulnerabilities.

Software vulnerabilities that are unawarely embedded into products during their design or implementation are named unintended taints. Such vulnerabilities are continually discovered, made public, and remediated using patches. However, some systems are not updated/patched quickly or not patched at all. In both cases, they are highly vulnerable. According to *Executive Order 13800*[27], known but unmitigated vulnerabilities are among the highest cybersecurity risks. One of the well-known incidents related to such security issues is the Heartbleed vulnerability [146][147] *CVE-2014-0160* which was a security vulnerability in the *OpenSSL* cryptography library that allowed attackers to get access to confidential data such as unencrypted exchanges between Transport Layer Security (TLS) parties, authentication secrets like session credentials, private keys, cookies, and so on, which would enable attackers to decrypt communications of compromised parties. After an attacker has gained authentication credentials, the attacker can impersonate the victim, and that even after a security patch of Heartbleed is applied. In other words, the attacker can impersonate the victim as long as the victim's credentials are still valid (e.g., before credentials changing or the revocation of the private key). When the Heartbleed Secure Socket Layer (SSL)/TLS vulnerability was announced more than 80,000 SSL certificates were revoked in the week following the publication [148][149]. The unintended taint was embedded into the OpenSSL library in 2012 and was publicly revealed in April 2014. However, system administrators are known to be generally slow in patching their systems. For example, in May 20^{th} 2014, 1.5% of the 800,000 most popular websites that use TLS were still vulnerable to *Heartbleed*[28]. In January 23^{rd} 2017, according to *Shodan*[29], nearly 199,594 devices connected to the Internet were still vulnerable. Another vulnerability of the same caliber is *Shellshock CVE-2014-6271* which is a security vulnerability in the *Unix Bash* shell that enables an attacker to cause *Bash* to execute arbitrary commands and gain unauthorized access to Internet-facing services (e.g., web servers) that use *Bash* to process requests [150]. Following few days of the *Shellshock* publication, various related vulnerabilities were discovered[30] (*CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186* and *CVE-2014-7187*). Following few hours of initial disclosure of *Shellshock*, adversaries exploited it to create botnets to perform DDoS attacks and vulnerability scanning[31][32]. Also, in the few days after the initial disclosure, there have been millions of scans and cyberattacks related to *Shellshock* [33].

Another type of taint is the malicious taint, which occurs when authentic components which have been previously validated have some functionality intentionally inserted into them by some adversary which affects their safety, reliability, and security [36]. The best example to highlight the danger behind malicious taint is the *Solarwinds* supply chain attack [151][152][153]. In the Solarwinds attack, hackers gained access through trojanized updates to *SolarWinds' Orion* computer monitoring and management software. Basically, a software update was exploited to install *Sunburst* malware in *Orion*, which was then installed by almost 18,000 customers. Once installed, the malware provided hackers with a backdoor to *SolarWinds* customers' systems and networks. This attack illustrates a good example of software supply chain vulnerabilities and consequences, because instead of directly attacking the federal government or a private organization's network, hackers target a third-party vendor, which provides them with software. In this case, the target was the computer management software *Orion*, supplied by the Texas company *SolarWinds*. More than 33,000 companies are said to use Orion. *SolarWinds* says 18,000 of its customers have been affected, including 425 companies of the *Fortune 500*[34]. The very first attack would have targeted *FireEye* systems. FireEye is a company that assists in the security management of several large private companies and federal government agencies.

[27]https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure
[28]https://www.theregister.com/2014/05/20/heartbleed_still_prevalent/
[29]https://www.shodan.io/report/DCPO7BkV
[30]https://www.itnews.com.au/news/further-flaws-render-shellshock-patch-ineffective-396256
[31]https://www.itnews.com.au/news/first-shellshock-botnet-attacks-akamai-us-dod-networks-396197
[32]https://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/
[33]https://bits.blogs.nytimes.com/2014/09/26/companies-rush-to-fix-shellshock-software-bug-as-hackers-launch-thousands-of-attacks/
[34]https://fortune.com/fortune500/

2.3 Insider threat

According to the Cybersecurity and Infrastructure Security Agency (CISA) [154] insider threat is the potential for an insider[35] to use his/her authorized access or understanding of an organization to cause harm to that organization. This harm can be malicious or unintentional acts that negatively affect the integrity, confidentiality, and availability of the resources (e.g., data, personnel) of the organization [155].

According to a recent report [35], the number of cybersecurity incidents caused by insiders increased by 47% since 2018. The average annual cost of insider threats has also skyrocketed in only two years, rising 31% to $11.45 million. Also, according to the European Union Agency for Cybersecurity (ENISA) [156], 88% of organizations admit insider threats to be a source of preoccupation. Therefore, a security problem caused by an insider could have repercussions on all the supply chain links, especially when insider attacks are considered as a serious challenge for organizations [157]. For example, a former software engineer for *Amazon Web Services (AWS)* took advantage of a misconfigured web application firewall and accessed more than 100 million customers' accounts and credit card records[36] [156]. In this case, it is worth noting that a security threat occurred at the vendor link which affected both the vendor and the consumer links. Another example is what happened to *Tesla*[37], where an insider used his insider access to make direct code changes to the Tesla Manufacturing Operating System under false usernames and exporting large amounts of highly sensitive Tesla data to unknown third parties.

2.4 Discussion

It is undeniable that cyberattacks represent a real danger on supply chain and they are a real threat to the latter. According to [157] in 2020 86% of organizations suffered from a successful cyberattack.

A supply chain can be attacked via its different links. The impact of an attack varies depending on the targeted link. However, because of the strong interconnectedness of all the links in the supply chain, the attacks can have serious consequences on the continuity of the latter. There is an exception for the consumer link. That is, an attack against this link will not disturb the continuity of the other supply chain links because it represents the last link. However, it could have disastrous consequences according to the environment and to the context.

There are numerous reasons behind launching attacks on the supply chain. Some of the supply chain links such as the mining link or the manufacturing link are both a geopolitical target as well as an economic target. The motivations for attacking them and the supply chain in general, therefore go beyond any direct financial gain alone. We summarize the main motivations as: (1) cyber espionage for competitive advantage through the acquisition of the latest technical expertise, knowledge and intelligence. (2) Financial gain which includes the classic data theft like Personally Identifiable Information (PII), credentials, and financial data. (3) Cyber/economic war, where cyberattacks are perpetrated with the aim to weaken the economy of a nation. (4) Hacktivism, because of the perception of mines, transportation companies, and manufacturers as environmental polluters.

Malware and DDoS are the top security threats to the supply chain because of their consequences that severely disrupt the latter. Moreover, the number of such attacks is continuously increasing. For example, according to *AV-Test*[38], there is a total of 1,24161 billion of malware types detected in 2021 before its end compared with 1,13924 billion of malware types detected in 2020. In 2019, 93.6% of malware types detected were polymorphic (having the capacity of changing their code to bypass detection) [158]. In recent years, there is a clear trend of ransomware attacks because they are the source of direct financial gain to the attackers. According to [157], in 2021 around 69% of organizations were compromised by ransomware.

[35] An insider is any person who has or had authorized access to or knowledge of an organization's resources such as personnel, networks, systems, and so on.
[36] https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/
[37] https://www.tesla.com/
[38] https://www.av-test.org/en/statistics/malware/

As we have mentioned previously, one of the major security issues is the default and hardcoded configuration/credentials that are not modified by users after the devices have been deployed or simply cannot be modified because they are hardcoded. This can open the door to multiple kinds of attacks. The most virulent one remains the malware infection. As we have discussed before, numerous malware programs such as *Mirai*, *Bashlite*, *Mukashi* and many others rely on default and hard coded credentials to get access to devices [131].

Many technical infrastructures often rely on the same software (operating systems, libraries, platforms and so on), hardware (computing chips, sensors and so on), firmware components, and other common components. More precisely, we can find lot of common components deployed in different oil facilities, mining companies or other manufacturing industries. This enables unintended taint that impacts one infrastructure (manufacturer/operator) to affect others.

Alrawi et al. [159] conclude that there are three main attack vectors in relation to IoT devices which are also similar for ICS systems: vulnerable services, weak authentication, and default configurations. Unfortunately, it is fairly easy to find vulnerable devices and services using tools such as *Shodan*, *Thingful* or others which find devices and services at all the supply chain links with weak security controls. *Shodan* can be used for vulnerability and penetration testing assessments alongside with *Google Hacking Database (GHDB)*[39] [160][141].

As Figure 3 shows, numerous attacks such as message forging, substitution or replay attack, sybil attack, spoofing attack, eavesdropping and many others, can be launched on the supply chain. However, social engineering attacks are among the most used ones. Social engineering techniques can provide access when targets are difficult to breach through technical means. They attempt to gain the trust of a gatekeeper with appropriate access or other useful information before manipulating him/her in order to get access to it or leave with it [161]. Social engineering can be achieved over the phone (vishing), in person (impersonation), over short messages (smishing) or through a combination of them. However, the most common form is the phishing (and spear phishing) that is executed electronically through the Internet. Indeed, in 2020 phishing was the top crime type reported to the Internet Crime Complaint Center (IC3). The number of complaints has increased by more than 100% compared to 2019 [162]. This trend represents a real danger for the supply chain because these phishing attacks are mainly used for cyber espionage, to disseminate malware and for financial data theft. According to [163], financial institutions are currently the first targets of phishing attacks. Indeed, according to [164], phishing is ranked first out of the top 10 biggest threats to organizations. Furthermore, phishing is the second most common attack used in data breaches, after denial-of-service following a hack [108]. According to *Verizon*, in the U.S. 30% of the victims open the phishing emails received. Among the victims, 12% click on the infected links or attachments, which demonstrates the danger that such attacks represent[77].

3 SECURITY REQUIREMENTS AND CHALLENGES

NIST SP 800-161 [165] considers integrity, security, resilience and quality as the four goals and challenges to consider for the cyber supply chain systems. *Bryant et al.* [166] considers safety, reliability, availability, resilience and security as the key objectives that a cyber supply chain system must attain, while, *Windelberg et al.* [166] focuses on security, safety, reliability, and quality.

We believe that the supply chain ecosystem must fulfill several security requirements and it faces multiple challenges in order to ensure its sustainability and resiliency. These challenges and requirements are different according to the supply chain domain and products related to it. For example, a military product requires confidentiality of information among other requirements whereas a milk supply chain requires transparency for all transactions. However, there are some requirements that are common and mandatory to all the use cases (that we discuss in this section). Figure 5 depicts a detailed taxonomy of the security requirements and challenges of cyber supply chain systems.

[39] https://www.exploit-db.com/google-hacking-database

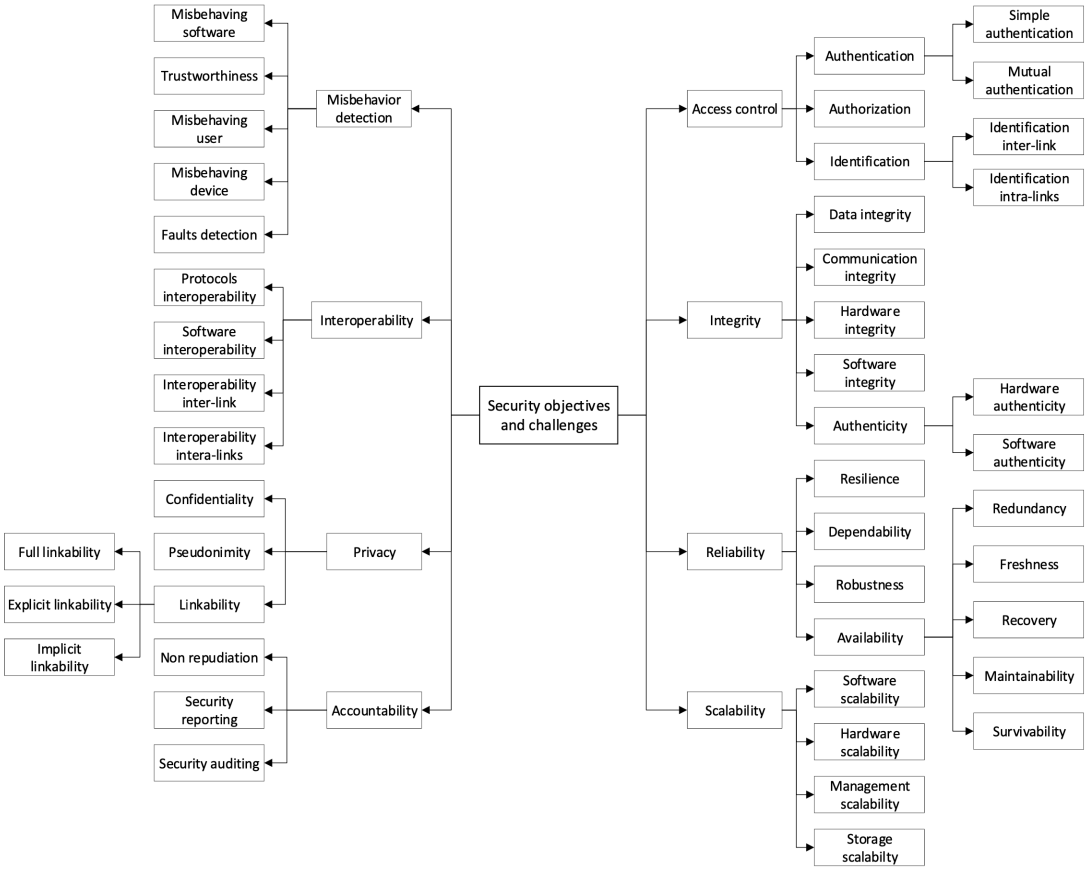


Fig. 5. Taxonomy of security challenges and goals for supply chain links

Integrity: Integrity is a crucial requirement that must be ensured at each link and be part of the supply chain. In the supply chain context we define three types of integrity: (1) *Data integrity*: implies maintaining the consistency and trustworthiness of data (storage data, transactions' data or network messages) over its entire life cycle. Therefore, it can be modified only by authorized users. (2) *Software integrity*: implies the guarantee to use consistent and trustworthy software. Indeed, tampering with software code can cause the system's disruption and have severe consequences such as system crashes. (3) *Physical integrity of devices*: ensures that the physical material (e.g., sensors, machines) was not tampered with. The lack of integrity of materials can lead to disastrous consequences that can range from adding surveillance/espionage devices to existing material to sabotage that causes accidents.

Availability: Availability implies that resources and services must be accessible to legitimate users and services on demand. Hence, a system must be resilient against attacks that target such a service. There are different ways to ensure availability according to the context. These include redundancy, distribution, and decentralization. *Gartner*[40] defines availability as the assurance that an organization's IT infrastructure has suitable recoverability and protection from system failures, natural disasters or malicious attacks. Therefore, recovery is an important aspect of the availability.

Reliability: System reliability is the combination of hardware and software reliability [167]. Hardware reliability is defined as the ability of a hardware to correctly execute a required function under certain conditions in a specified operational environment for some specific period of time [168][167] while software reliability is

[40]https://www.gartner.com/en/information-technology/glossary/availability

defined as the ability of a software to produces accurate and consistent results that are repeatable, under low, normal, and peak loads, in a specified operational environment [169][167]. Errors and unintended faults that are internal to a system create reliability problems. This differentiates reliability from robustness, where for the latter the causes are external to the system [170]. Generally, reliability means sound continuous performance whereas integrity is associated with sound condition [170].

Integrity, availability, and reliability are essential features and are often interdependent. Integrity problems impact negatively the reliability and availability and vice versa [166].

Authentication/mutual authentication: Authentication is the mechanism of proving an identity. Mutual authentication requires both communicating parties to authenticate each other. This requirement is necessary to protect the supply chain system at all the links' levels, against spoofing the roles of entities, against the data theft and many other security attacks and issues.

Identification: Identification is a major requirement in the supply chain ecosystem. In contrast to identification, anonymity ensures that any entity can make use of the system all while remaining anonymous to all system's entities. In the supply chain context, identification has two components: (1) the identification inter-link: this represents the identification within a supply chain link such as the mining or manufacturing link. Different techniques and technologies can be used according to the use case scenario, e.g., Industrial Internet of Things (IIoT), cloud computing, and so on. (2) the identification intra-link: this identifies the transactions, services, and users between the different links of the supply chain. For example, the manufacturer must be able to identify all transactions from its suppliers.

Authenticity: Ensuring authenticity means relying on genuine and not counterfeit hardware or software. As we have described earlier, products, processes, and information can be counterfeit. If a non authentic (counterfeit) component or a component which integrity is compromised (prone to tampering) is used or installed, it may cause security and safety failures [166]. Examples of counterfeit products include (1) the presentation of cloned items as being from the original manufacturer, (2) the selling of used or recycled components as new, or (3) the production of unauthorized copies of software. Counterfeit processes can comprise different steps like design, production, and testing [166]. Forging documentation is also considered as a production of counterfeit [171].

Interoperability/ traceability and data sharing: Interoperability is considered among the biggest challenges for supply chain. As for the identification, we define two types of interoperability;
(I) interoperability inter-link concerns the different technologies, processes, and procedures used within the different links of the supply chain. For example, the mining link (e.g., a mine) relies on a mining communications system which can be composed of different technologies such as autonomous haulage devices, seismic sensors, and so on. A manufacturer (manufacture link) that uses an IIoT system also relies on a network composed of heterogeneous technologies and devices. Generally, these systems cannot fully cooperate and understand each other because of two main reasons: (1) technical non-interoperability of respective protocols. There exist some solutions to address this issue. For example, there are numerous products that ensure a communication gateway between the different networking protocols[41]. However, relying on a gateway could add communication delays, which can have consequences on real-time systems. Moreover, these technical problems do not only concern networking technologies but many others such as software and services. (2) Industrial/commercial competition in order to be the leader in some area, leading the products' developers to intentionally encourage non-interoperability between their devices and competitive products from other vendors.
(II) interoperability intra-links which concern the different processes and procedures that are used between the different links of a supply chain. One of the best examples is the traceability (and data sharing) of products. Currently, it is very hard for a link's user (e.g., a manufacturer) to verify the origin of all the products that the other link user (e.g., supplier) provides. This is not limited to products or data origin, but to everything related to

[41] https://www.silabs.com/products/development-tools/wireless/mesh-networking/z-wave/z-ip-gateway

the supply chain such as transactions, industrial information, and others. This is even more true if we consider the end consumer who has no choice but to believe the vendor. The main reason lies in the absence of a global tool/service that allows such traceability and data sharing because of the interoperability of the different supply chain actors. Currently, blockchain technology offers the means to provide such a service. The traceability can be coupled with the confidentiality for sensitive data and access to the latter can be provided through authentication and authorization services.

4 COUNTERMEASURES AND RECOMMENDATIONS

4.1 Governments' countermeasures

Recent globalization trends along with the strong dependence on ICT systems, according to president *Obama*, the cyber infrastructure is gradually treated as a "strategic national asset", and the security issue of this infrastructure is turning into a "national security priority" [172][173]. Indeed, numerous governments are expressing worry about the threat to the supply chain that relates to a nation's cyber infrastructure. For example, in 2012, more than 50 nations defined and published cyber strategies to define what security means to their future national and economic security initiatives [174].

Unfortunately, government strategies focus more on the ICT supply chain (especially for governmental and military agencies) to the detriment of the other areas. The supply chains that ensure the production and distribution of information and communications services and products encompass a highly dynamic and widely distributed collections of people, processes, and technologies. The latter comprise various components (software and hardware). Thus, it is difficult to know if a part of this chain (e.g., process, a hardware or one of its components, a software or a part of it) was maliciously manipulated or modified, because the curent verification methods are not able to reply satisfactorily to this problem [175].

In the US, the Comprehensive National Cybersecurity Initiative (CNCI) #11 [176] focuses on developing a multi-pronged approach for global supply chain risk management of national security systems. National Institute of Standards and Technology (NIST) initiated in 2008 a program for Cyber Supply Chain Risk Management (C-SCRM) to develop key practices and recommendations for non-national security systems. Since then, NIST kept a steady research and publication effort on industry best practices for C-SCRM e.g., the Draft NISTIR 8276 [4] NIST SP 800-53 [177] NIST SP 800-161 [165] and NISTIR 7622 [178]. Consistent with these best practices, the National Defense Authorization Act authorizes the Secretary of Defense or the Secretaries of the Army, Navy, and Air Force to exclude vendors or their products if they pose an unacceptable supply chain risk [179][175].

While the US and Europe focus on excluding products and vendors that represent important threats, other countries such as China, India and Russia rely upon policies promoting "indigenous innovation" to reduce cyber supply chain risk, even if they state similar concerns. The indigenous innovation encourages the national and local development, sourcing[42], and manufacturing of ICT, equipments, and services [175][180][181]. For example, China has launched an aggressive indigenous innovation program. The latter prioritize the investment in local research and development and includes all sectors of the ICT field (chips, hardware and software) [175][181]. Furthermore, the use of an indigenous product catalog is required for its government tender. Finally, China defined a security scheme called Multi-Level Protection Scheme (MLPS) for most information systems. The MLPS describes a set of rules such as: the research, development and manufacturing of products, must receive investments or be controlled by Chinese citizens, legal persons or the state, and have independent legal representation in China. The designed technology and the product's key parts must have independent Chinese or indigenous intellectual property rights [175][181]. Moreover, a certification authority called China Information Security Certification Center (ISCCC) has been set up in order to certify products [181][182]. Russia also implemented a certification policy that concentrate on non-disclosed functions and processes [183], but focuses more on addressing concerns

[42]Searching for a supplier that would help the company's objectives in terms of cost, quality and deadlines.

	Approach	Year	Security goal									Protection of the product or protection of the SC
			Integrity	Authentication	Authorization	Identification	Availability	Scalability	Traceability	Data sharing	Authenticity	
Threat models and frameworks for supply chainsecurity	*Al Sabbagh et al.* [184]	2015	✓	✓	✗	✗	/	✗	✗	✗	✓	Supply chain and product
	Yeboah-Ofori et al. [185]	2019	✗	✗	✗	✗	✗	✗	✗	✗	✗	Supply chain and product
	Wu et al. [186]	2019	/	/	/	✓	✗	✗	✓	/	/	Supply chain
Security solutions for software supply chain	*SAFECode* [187]	2010	✓	✓	/	✗	✗	✗	/	/	✓	Product
	Alberts et al. [188]	2011	✗	✗	✗	✗	✗	✗	✗	✗	✓	Supply chain and Product
	Microsoft [189]	2012	✓	✓	✗	/	/	✗	✗	✗	✓	Supply chain and product
Security solutions for product supply chain	*Bhargava et al.* [190]	2013	✗	✗	✗	✗	✗	✗	✗	/	/	Supply chain
	Huang et al. [191]	2015	✗	✓	/	✓	✗	✗	✗	✗	/	Product
	Sk Subidh et al. [192]	2016	✓	✓	✗	✗	✗	✗	✗	✗	✓	Product
	Skudlarek et al. [193]	2016	✓	✓	/	✗	✗	✗	✓	✗	✓	Product
	Zhang et al. [194]	2018	✓	/	/	/	✗	✗	✗	✗	✓	Product
	Esfahani et al. [195]	2019	✓	✓	✗	✗	✗	✗	✗	✗	/	Supply chain
Blockchain based solutions for supply chain	*Bocek et al.* [196]	2017	/	/	/	✓	/	✓	✓	✓	/	Product
	Wu et al. [197]	2017	✓	✓	/	/	✓	✓	✓	✓	/	Supply chain
	Bellavista et al. [198]	2017	✓	✓	/	✓	/	✗	✓	✓	/	Supply chain
	Xu et al. [199]	2018	/	✓	✓	✓	/	/	/	/	/	Supply chain and products
	Mediledger [200]	2018	✓	/	/	✓	✗	/	✓	✓	✓	Product
	TradeLens [201]	2018	✓	/	/	✓	✗	/	✓	✓	✓	Product
	Figorilli et al. [202]	2018	✓	/	/	✓	✗	/	✓	✓	✓	Product
	Toyoda et al. [203]	2018	✓	/	/	✓	✗	/	✓	✓	✓	Product
	Caro et al. [204]	2018	✓	/	/	✓	✗	/	✓	✓	✓	Product
	Waltonchain [205]	2018	✓	✓	✓	✓	✓	/	✓	✓	✓	Product
	Walmart [206]	2019	✓	/	/	✓	✗	/	✓	✓	✓	Product
	Malik et al. [207]	2019	✓	/	/	/	✓	✓	✓	✓	/	Product

Table 2. Comparison of the major existing works that provide security solutions for supply chain (✓: Yes; ✗: No; /: Unknown)

about backdoors and other functions that might not be disclosed to users. Russia also created a National Software Platform to help reduce dependence on foreign products and, arguably, to support domestic innovation [175].

The indigenous innovation strategy has some benefits especially considering the worldwide various competitions at different levels: economically, politically and militarily, where each country tries as much as possible to rely on goods and services that may not be maliciously manipulated by an adversary. However, it cannot be adopted by the majority of countries because of various types of resource constraints. Moreover, because of globalization, most organizations no longer have a full control -and generally do not have full visibility into- the supply chain ecosystems of the goods or services that it provides and ensures [4]. Finally, the indigenous innovation strategy is a double edged sword, because it limits trade, compromise foreign investment, and abstain the local industry from the advantages of foreign technological innovations [175].

4.2 Security solutions

Table 2 summarizes and compares the different security solutions for the C-SCRM.

4.2.1 Threat models and frameworks for supply chain security. Yeboah-Ofori et al. [185] modeled and analyzed cyber supply chain threats and attacks identified by supply chain actors. They considered concepts such as goal, actor, attack, and threat actor relevant to the supply chain, threat model, and requirements domain, and modeled the attack using the Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX) threat model [208]. Finally, to determine the propagation of the attack and its cascading effects, they used a method of discrete probability to calculate the conditional probabilities. However, they only proposed a threat model and did not provide a detection/protection method that meets the needed

requirements that Table 2 shows. *Al Sabbagh et al.* [184] proposed a threat-modeling framework specific to the software supply chain. This framework appears to provide a holistic approach in identifying software supply chain security problems. However, it focuses more on the security problems caused by the poor coordination between suppliers and customers and unaligned security measures taken at different levels in different systems than common security concerns of software supply chain systems aspects [184]. Moreover, the authors only rely on a qualitative study (through interviews) while a more rigorous technical approach (e.g., with technical data) is very important in such area. *Wu et al.* [186] proposed the idea of Supply Chain of Things (SCoT) to bind the different components (layers/entities) related to the supply chain, such it is the case for IoT. The approach proposed by Wu *et al.* 's work [186] is supposed to have an important impact on different fields like intelligent decision making, end-to-end traceability, and smart transportation.

4.2.2 Security solutions for software supply chain. Microsoft proposes a framework that incorporates best practices of software integrity risk-management into (1) the process of software product development, and (2) the operations of online services [189]. The framework is expected to enhance the security and trustworthiness of software among the different involved parties (people, processes, and technologies) that make up a modern ICT supply chain. It follows six phases: planning, discovery, assessment, development, validation, and implementation. However, this approach can only be applied to a software supply chain.

Alberts et al. [188][209] describe the Carnegie Mellon Software Engineering Institute (SEI) risk assessment approach for software supply chain. The approach relies on few factors, called drivers, that has a strong influence on the eventual output or result. The experimentations realized on to validate the approach show that the establishment of a comprehensive profile of systemic risks to mission success requires around 15-25 drivers. Each driver is represented as a yes-no question, where an answer of yes means that the driver is in its success state. In other words, it contributes as a minimal risk to the software SC mission. An answer of no means that the driver is in its failure state. That is, it represents a severe degree of risk to the software SC mission [188].

In the same context, *SAFECode* [187] builds sound assurance practices within each phase of the software development, which can have an important contribution in the reduction of the risks related to the supply chain. It does not design a framework or an approach like the one proposed earlier in this section. But, it provides a set of best practices, verifications and controls, mainly integrity controls at (1) the software sourcing phase; (2) the software development and testing phase; and (3) the software delivery and sustainment phase.

4.2.3 Security solutions for product supply chain. Bhargava et al. [190] proposed an approach for end-to-end security auditing of business processes that comprise supply chains. The approach enables tracking the information flows of shared data and detecting compromised business processes of partners and it addresses information leakage and unauthorized data disclosure in supply chains. However, this work lacks numerous technical details that explain how these objectives can be fulfilled. *Huang et al.* [191] proposed a clone detecting approach called Double-Track Detection (DTD). Since reading RFID tags generates events, the proposed approach relies on storing a verification sequence value v in a tag memory; after a reader detects the tag, this verification sequence value v is updated to $v + 1$, and a local database stores the related tag event data (updated v). The initial v-value should be randomized. In cases when an attacker modifies the value of v, the scheme can still detect clones because it may cause duplicated v-values. However, the approach does not rely on any cryptographic security solution such as the digital signature. Therefore, if an attacker forges a new v it cannot be detected. *Sk Subidh et al.* [192] addressed security in the supply chain of Digital Microfluidic Biochips (DMFBs). The main goal of the proposal was the prevention of attackers from the exploitation of the vulnerabilities related to the supply chain and then the modification of DMFBs' proprietary protocols. Alike tampering can lead to disastrous consequences on biotechnology innovation, healthcare, and laboratory analysis. However, they did not design a structured security approach. They only discussed the impact of existing techniques such as digital signature and code obfuscation on supply chain security. *Skudlarek et al.* [193] proposed the deployment of unique chip IDs as a mean to ensure

the authentication, tracking, provision, and analysis of all the products during the whole lifecycle of the chip and for all the supply chain's related parties. A key feature of the platform is the use of a Physically Unclonable Function (PUF) to provide each chip with its own unique ID and a unique key to protect data in transit to the chip. However, the approach mainly relies on PUF which are known to not being always scalable solutions especially for a supply chain [210][211][212]. Indeed, using PUF requires a registration phase. Before a new entity is registered, a trusted party gathers the unique Challenge-Response Data (CRD) from the entity's PUF. Then, the trusted party stores it in a database along with the ID of the entity itself. *Zhang et al.* [194][213] proposed a solution to protect the ownership of both intellectual property and integrated circuit owners' designers. In this solution, a dynamically obfuscated wrapper for split test along with a secure split test methodology aim at preventing intellectual property overusing[43] at multiple abstraction levels and enable integrated circuit designers to fully control the production, test, and authentication processes. *Esfahani et al.* [195] proposed a Transport Layer Security (TLS)-based authentication mechanism which is resistant against Man In The Middle (MITM) attacks in web applications that use the TLS protocol to secure Hypertext Transfer Protocol (HTTP) communications. Specifically, the proposed mechanism prevents the attacker from impersonating the legitimate server to the user (i.e., client) thereby comprising user's sensitive information. The TLS-based authentication mechanism is based on the Server Invariance with Strong Client Authentication (SISCA) mechanism [214] and relies on channel ID-based authentication and server invariance. However, this solution is designed for the manufacturer link and not for the whole supply chain. Moreover, it only is effective against one attack which is MITM.

4.2.4 Blockchain based solutions for supply chain security[44]*.* During the last few years, there has been an increasing interest in applying blockchain technology to supply chain [22][19][215]. This strong interest stems from the blockchain data structure and principle which, by default, satisfies many of the supply chain requirements such as traceability, immutability, distribution, data integrity, transparency, and counterfeit prevention.

Gonczol et al. [22] classified blockchain approaches for supply chain into two categories: (1) blockchain-based conceptual systems and (2) blockchain-based implemented systems. Indeed, numerous works [216][217][218][219][220][221][222][223][224][225][226][227] do not provide any technical details about their proposed systems. They also do not consider the features and development issues which arise when blockchains are integrated to other technologies (e.g., IoT configurations, sensors, RFID tags, and so on) in supply chains. These efforts consider blockchains as black boxes although it is an important research issue when we consider the problem of "How can a supply chain implement a blockchain system?" [22].

In this paper we are interested in the second category namely, blockchain-based implemented approaches. According to [22] there is an explicit difference between the implemented applications proposed by academia and the approaches proposed by industry. Indeed, the academic approaches [228][202][197][203] focus first on the clear definition of the problems from which the supply chain suffers, then on the proposal of a blockchain-based solution that handle the identified problems and requirements. However, most of the studies related to industry applications [201][206][229][200][230] focus on sales, or simply announce the incorporation of blockchain technology.

Xu et al. [199] proposed a digital identity management scheme that can be integrated with blockchain maritime supply chain management systems to enforce information accuracy. However, the paper does not provide technical details on how this goal can be fulfilled. In the same shipping/transport context, *Wu et al.* [197] proposed an online shipment tracking framework that aims to achieve near real-time visibility during the physical distribution of the products in the SC. It consists of a set of private distributed ledgers and one public blockchain. The private ledgers serve for the sharing of the information related to the custody events amid the trading partners in a specified

[43]The unauthorized integration of intellectual property without the consent of the original intellectual property owner

[44]The approaches discussed in this section also fall into the other categories (e.g., threat models, frameworks, security solution for software SC or product SC). However, we preferred classifying them as blockchain based approaches due to the novelty of the technique.

shipment. *TradeLens* [201] is another shipment application. It is the result of a collaboration between *IBM* (*IBM Cloud* and *IBM Blockchain*) and *Maersk*. *TradeLens* is presented as an open solution to the limited collaboration between the various parties implicated in the shipment travel. It assumes the provision of a foundation of trust and the tracking of products shipped from the time they are loaded onto a container until they arrive to the final customer, all along the registration of different shipping events from various stakeholders [22].

The transparency of the supply chain in order to prevent food-borne illness outbreaks, as well as proving food quality, sustainability and fair trade are major issues in the food supply chain. To address these issues, *Walmart* created a food traceability system based on the *Hyperledger Fabric* [206] that allows it to trace the origin of over 25 products from 5 different suppliers. *Provenance*[45] is a similar application which is used for food and beauty products traceability. In the same context, *Caro et al.* [204] proposed AgriBlockIoT, a fully decentralized, blockchain-based traceability solution for Agri-Food supply chain management, which integrates IoT devices producing and consuming digital data along the chain.

In the medical area, *Mediledger* [200] is a product verification system which complies with the drug supply chain security Act in the US. The act stipulates that the distributors must verify with the manufacturer, the unique identifier of the medicine that were returned before they resell them [22]. In the same pharmaceutical context, *Bocek et al.* proposed *Modum.io* [196] which is a system that complies with the Good Distribution Practice (GDP) regulation[46] which requires a proof that shipped medicinal products have not been exposed to conditions compromising their safety. More precisely, *Modum.io* combines blockchain and sensors to enforce data immutability and public accessibility of temperature records, all along the reduction of operational costs in the pharmaceutical supply chain. Indeed, in order to guarantee the compliance with regulations and the quality control during the transportation of medical products, the medical industry must ensure the application of various complex and strict environmental control processes (e.g., temperature and humidity). In *Modum.io*, the sensors monitor the temperature of each transported package during the shipment in order to satisfy the strict compliance with GDP regulations. Data is first stored in a mobile device such as a smart phone. Then, all data is transferred to the blockchain where a smart contract evaluates this data against the product attributes. However, no security was implemented for the communication between the sensors and the mobile device which can make an attacker tamper with data before their storage in the blockchain.

Figorilli et al. [202] proposed a mechanism that relied on blockchain and RFID for wood traceability from its tree form in the forest to the end product. Other applications such as *PeerLedger*[47], *Ambrosus* [231], *Guardtime HSX*[48] and *OriginTrail* [229] offer similar traceability and transparency for other application domains. *Everledger* is another application example that was designed for diamonds traceability and then was extended to gemstones, minerals, insurance, luxury, art, and wines. One of the distinguishing characteristics of *Everledger* is that it uses blockchain technology, coupled with the digital twin technique [232][233].

For Industry 4.0, *Bellavista et al.* [198] proposed a relay scheme based on a trusted execution environment that provides higher security guarantees. More precisely, the proposed solution relies on a smart contract that invokes an off-chain secure computation element, to securely communicate with its peer counterpart. However, the system suffers from increased latency due to cross-blockchain interactions and off-chain computations. Moreover, this approach is applied only to the manufacturing phase and not the whole supply chain process.

Toyoda et al. [203] proposed a novel Product Ownership Management System (POMS) of RFID-attached products for anti-counterfeits that can be used in the post supply chain stage. For this purpose, they leveraged the idea of Bitcoin's blockchain that anyone can check the proof of possession of balance. With the proposed POMS, a customer can reject the purchase of counterfeits even with genuine RFID tag information, if the seller

[45]https://www.provenance.org/sector/food-drink
[46]https://www.ema.europa.eu/en/human-regulatory/post-authorisation/compliance/good-distribution-practice
[47]https://www.peerledger.com/
[48]https://guardtime.com/

does not possess his/her ownership. In other words, its primary objective is to use the traceability feature in the blockchain to avoid trading of counterfeit products. *Waltonchain* [205] is another system that uses IoT devices as data senders to the blockchain in a supply chain process. *Waltonchain* uses a secure two-way authentication, and integrated encryption logic. An IoT device (data sender) can upload by itself to the blockchain, allowing IoT monitoring (such as temperature measurements, humidity measurements) much safer.

Malik et al. [207] proposed TrustChain, a three-layered trust management framework, which uses a consortium blockchain to track interactions among supply chain participants and to dynamically assign trust and reputation scores based on these interactions.

4.3 Recommendations

In this section we provide a set of recommendations and best practices, from both : the organizational and the technical perspectives, to enhance the security of the supply chain.

4.3.1 Best practices for supply chain security. Regarding best practices on supply chain security, *Microsoft* [175] recommends: (1) the development of sound threat models to assist in the identification and prioritization of supply chain threats/risks. Indeed, currently, corporations mainly depend on their proprietary threat models. However, considering such an approach (only considering their own threat models) may solely reflect the knowledge of the threats/risks from the vendor's perpective and not the actual existing risks; (2) To ensure audits by independent third parties, which provide an external neutral review. However, this solution can be costly in money and time; (3) governmental supervision, though it suffers from scalability issues because of the huge number of products that must be controlled. *NIST* [4] recommends: (1) the integration of cyber supply chain risk management across the organization; (2) the establishment of a formal program that guarantees the organizational responsibility for the management of the threats/risks related to the cyber supply chain. In fact, mature organizations consider formal programs with established governance, policies and procedures, processes, and tools; (3) the knowledge and management of the critical suppliers; (4) the fully understanding of all the parts of the supply chain; (5) the close collaboration with the key suppliers; (6) the inclusion of the most important suppliers in the resilience and improvement actions; (7) the assessment and monitoring over the supplier relationship.

4.3.2 Technical implementation approaches for supply chain security. Regarding technical implementation, we consider the following technologies.

Cryptography approaches for supply chain security: We believe that some technologies and techniques, can achieve high levels of supply chain security for both the products and the processes, if applied and set up together. According to the works discussed earlier, blockchain technology can satisfy multiple security and performance requirements and goals such as traceability, immutability, data integrity, data sharing, data availability, and scalability. However, blockchain technology alone is not sufficient. Blockchain technology must be coupled with a strong authentication scheme especially for the different devices at the different supply chain links in order to ensure the authentication of the data stored and exchanged. Elliptic Curve Cryptography (ECC) is known to be lightweight and can therefore be adapted to resource-constrained IoT devices [234][235][236]. Even, if encryption is not possible, the IoT devices must at least use signature to enforce secure authentication as well as data integrity. For example, the Elliptic Curve Digital Signature Algorithm (ECDSA) has multiple benefits over traditional signature algorithms such as *Rivest Shamir Adleman (RSA)* especially in terms of key sizes and signature times [237]. Moreover, a timestamp verification can be added to mitigate replay attacks. Furthermore, we need a certification mechanism for the keys to ensure the authorization and identification of devices. For example, in [237], is a proposal of decentralized blockchain-based mechanism that provides lightweight certificates to constrained devices. If such mechanism is not possible, because of the devices constraints (e.g., some RFID tags), Physically Unclonable Function (PUF) represents an alternative [238]. However, PUF technology is not suitable for all the scenarios because of its limited scalability.

Artificial intelligence and big data approaches for supply chain security: We believe that artificial intelligence and big data techniques represent a real asset in the supply chain security. *Hassija et al.* [21] describes how artificial intelligence can enhance the management of supply chain risk by securing them against disruptions through the anticipation of their occurrence and the minimization of their side effects. For example, *Baryannis* [239] proposed a supply chain risk prediction framework using data-driven artificial intelligence. In the same context, *Zage et al.* [240] proposed a method for identifying deceptive practices within the supply chain, specifically for the e-commerce domain. Moreover, *Camossi et al.* [241] proposed the Anomalous Container Itinerary Detection (ACID) framework that analyzes container status messages to discover non conform container shipments.

5 CONCLUSION

It is an undeniable fact that most of the products and services that we use in our daily life today are the result of some supply chain. The Internet and Information Communication Technologies (ICT) are currently pervasive in many application domains. These technological advances have revolutionized and transformed the supply chain to Digital Supply Chain (DSC), which is the result of the application of information, digital, and electronic technologies to every aspect of the end-to-end supply chain. Moreover, over the last few years, we have witnessed the explosive growth of the Internet of Things (IoT), and as the costs of IoT devices continue to decline making them more affordable, they are increasingly being used in the digital supply chain. Unfortunately, the use of such technologies has considerably increased security risks and increased the attack surface on all the supply chain links. In this work we have presented an in-depth analysis of the security issues associated with the supply chain. In contrast to existing surveys on supply chain security, we have considered both the managerial and the technical perspectives. Moreover, we discussed all the supply chain's links and processes rather than considering the supply chain as a single block which we have shown was made by the previously published surveys and reviews.

In this work, we have analyzed and discussed various security issues and challenges related to the different supply chain links and related technologies. We have also discussed the different security approaches that have been applied to the supply chain. Based on our analysis, we found that previously proposed supply chain security solutions have not considered the different security challenges and issues considered above. Therefore, we need a comprehensive and holistic approach that ensures the security of the end-to-end supply chain. Finally, we provided a set of recommendations and best practices, from both the organizational and the technical perspectives, to enhance the security of the supply chain. We believe that some cryptography primitives and techniques (e.g., digital signature, blockchain) and artificial intelligence are among the key solutions that can enhance the security of the supply chain.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for their valuable comments which helped us improve the organization, content, and presentation of this paper.

REFERENCES

[1] Ling Xue, Cheng Zhang, Hong Ling, and Xia Zhao. Risk mitigation in supply chain digitization: System modularity and information technology governance. *Journal of Management Information Systems*, 30(1):325–352, 2013.
[2] Faisal Iddris. Digital supply chain: survey of the literature. *International Journal of Business Research and Management*, 9(1):47–61, 2018.
[3] Jay Heizer, Barry Render, and Chuck Munson. *Principles of Operations Management: Sustainability and Supply Chain Management (Global editon)*. Pearson, 2017.
[4] Jon Boyens, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. Technical report, National Institute of Standards and Technology (NIST), 2021.
[5] Sandor Boyson. Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7):342–353, 2014.

[6] Jonathan D Linton, Sandor Boyson, and John Aje. The challenge of cyber supply chain security to research and practice–An introduction, 2014.
[7] Dmitry Ivanov and Boris Sokolov. The inter-disciplinary modelling of supply chains in the context of collaborative multi-structural cyber-physical networks. *Journal of Manufacturing Technology Management*, 2012.
[8] Don Davidson and Stephanie Shankles. We cannot blindly reap the benefits of a globalized ict supply chain! Technical report, DEPARTMENT OF DEFENSE WASHINGTON DC CHIEF INFORMATION OFFICER, 2013.
[9] Koen Tange, Michele De Donno, Xenofon Fafoutis, and Nicola Dragoni. A systematic survey of industrial Internet of Things security: Requirements and fog computing opportunities. *IEEE Communications Surveys & Tutorials*, 22(4):2489–2520, 2020.
[10] Abhijeet C Panchal, Vijay M Khadse, and Parikshit N Mahalle. Security issues in iiot: A comprehensive survey of attacks on iiot and its countermeasures. In *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*, pages 124–130. IEEE, 2018.
[11] Sagarika Ghosh and Srinivas Sampalli. A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access*, 7:135812–135831, 2019.
[12] Dimitrios Pliatsios, Panagiotis Sarigiannidis, Thomas Lagkas, and Antonios G Sarigiannidis. A survey on SCADA systems: secure protocols, incidents, threats and tactics. *IEEE Communications Surveys & Tutorials*, 22(3):1942–1976, 2020.
[13] Juha Hintsa, Ximena Gutierrez, Philip Wieser, and Ari-Pekka Hameri. Supply chain security management: an overview. *International Journal of Logistics Systems and Management*, 5(3-4):344–355, 2009.
[14] Tianbo Lu, Xiaobo Guo, Bing Xu, Lingling Zhao, Yong Peng, and Hongyu Yang. Next big thing in big data: the security of the ict supply chain. In *2013 International Conference on Social Computing*, pages 1066–1073. IEEE, 2013.
[15] Nadya Bartol. Cyber supply chain security practices dna–filling in the puzzle using a diverse set of disciplines. *Technovation*, 34(7):354–361, 2014.
[16] Guanyi Lu, Xenophon Koufteros, and Lorenzo Lucianetti. Supply chain security: A classification of practices and an empirical study of differential effects and complementarity. *IEEE Transactions on Engineering Management*, 64(2):234–248, 2017.
[17] Claudia Colicchia, Alessandro Creazza, and David A Menachof. Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, 2019.
[18] Andrii Boiko, Vira Shendryk, and Olha Boiko. Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia computer science*, 149:65–70, 2019.
[19] Hussam Juma, Khaled Shaalan, and Ibrahim Kamel. A survey on using blockchain in trade supply chain solutions. *IEEE Access*, 7:184115–184132, 2019.
[20] Abhijeet Ghadge, Maximilian Weiß, Nigel D Caldwell, and Richard Wilding. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 25(2):223–240, 2019.
[21] Vikas Hassija, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, 8(8):6222–6246, 2020.
[22] Peter Gonczol, Panagiota Katsikouli, Lasse Herskind, and Nicola Dragoni. Blockchain implementations and use cases for supply chains-a survey. *Ieee Access*, 8:11856–11871, 2020.
[23] Haibo Zhang and Kouichi Sakurai. Blockchain for iot-based digital supply chain: A survey. In *International Conference on Emerging Internetworking, Data & Web Technologies*, pages 564–573. Springer, 2020.
[24] Shipra Pandey, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, 2020.
[25] 2021 Must-Know Cyber Attack Statistics and Trends. Technical report, Embroker, April 2021.
[26] Cleary Gillian, Corpin Mayee, Cox Orla, Lau Hon, Nahorney Benjamin, O'Brien Dick, O'Gorman Brigid, Power John-Paul, Wallace Scott, Wood Paul, and Wueest Candid. Internet Security Threat Report (ISTR). Technical report, Symantec, 2018.
[27] 2020 in review, Data Breach Report. Are consumers at less risk? Technical report, Identity Theft Resource Center (ITRC), 2021.
[28] Numaan Huq. Cyber Threats to the Mining Industry. Technical report, TREND MICRO, 2016.
[29] Manoj Hudnurkar, Sujeet Deshpande, Urvashi Rathod, and SureshK Jakhar. Supply chain risk classification schemes: A literature review. *Operations and Supply Chain Management: An International Journal*, 10(4):182–199, 2017.
[30] Piyush Singhal, Gopal Agarwal, and Murali Lal Mittal. Supply chain risk management: review, classification and future research directions. *International Journal of Business Science & Applied Management (IJBSAM)*, 6(3):15–42, 2011.
[31] Muhammad Saeed Shahbaz, Raja Zuraidah RM Rasi, and MD Fauzi Bin Ahmad. A novel classification of supply chain risks: Scale development and validation. *Journal of Industrial Engineering and Management (JIEM)*, 12(1):201–218, 2019.
[32] ENISA Threat Landscape For Supply Chain Attacks. Technical report, European Union Agency for Cybersecurity (ENISA), 2021.
[33] J. Michael Martinez de Andino. Counterfeits in the Supply Chain: A Big Problem and it's Getting Worse. Technical report, Hunton & Williams LLP, Februari 2014.
[34] Rosemary Coates. Are there counterfeits in your global supply chain? Technical report, Logistics management, August 2019.
[35] 2020 Cost of Insider Threats Global Report. Technical report, Ponemon Institute, 2021.
[36] Beau Woods and Andy Bochman. Supply chain in the software era. page 12, 2018.

[37] John F Miller. Supply chain attack framework and attack patterns. Technical report, MITRE CORP MCLEAN VA, 2013.
[38] Melinda Reed, John F Miller, and Paul Popick. Supply chain attack patterns: Framework and catalog. *Office of the Deputy Assistant Secretary of Defense for Systems Engineering*, page 88, 2014.
[39] Global Brand Counterfeiting Report, 2018. Technical report, R Strategic Global, December 2017.
[40] E Danielle Rentz, Lauren Lewis, Oscar J Mujica, Dana B Barr, Joshua G Schier, Gayanga Weerasekera, Peter Kuklenyik, Michael McGeehin, John Osterloh, Jacob Wamsley, et al. Outbreak of acute renal failure in panama in 2006: a case-control study. *Bulletin of the World Health Organization*, 86:749–756, 2008.
[41] Virginia Woman Sentenced to 60 Months in Prison for Importing and Selling Counterfeit Cisco Computer Networking Equipment. Technical report, Department of Justice. Office of Public Affairs, September 2011 Updated February 2017.
[42] Michael Pecht et al. The counterfeit electronics problem. *Open Journal of Social Sciences*, 1(07):12, 2013.
[43] Lee Howard. Feds: Counterfeit submarine parts shipped to Groton base. Technical report, July 2013.
[44] GIDEP Alert, Document no. EE-A-06-06B. Technical report, overnment-Industry Data Exchange Program, March 20, 2006.
[45] Robert McMillan. Woman Helped Sell Fake Chips to US Military. Technical report, November 2010.
[46] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, 38:8–27, 2018.
[47] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, 4(5):1250–1258, 2017.
[48] Jyoti Deogirikar and Amarsinh Vidhate. Security attacks in IoT: A survey. In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pages 32–37. IEEE, 2017.
[49] Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 149:102481, 2020.
[50] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.
[51] Zakarya Drias, Ahmed Serhrouchni, and Olivier Vogel. Taxonomy of attacks on industrial control protocols. In *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, pages 1–6. IEEE, 2015.
[52] Ashish Singh and Kakali Chatterjee. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79:88–115, 2017.
[53] Abdullahi Chowdhury, Gour Karmakar, and Joarder Kamruzzaman. Survey of recent cyber security attacks on robotic systems and their mitigation approaches. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, pages 1426–1441. IGI Global, 2019.
[54] M Uma and Ganapathi Padmavathi. A Survey on Various Cyber Attacks and their Classification. *IJ Network Security*, 15(5):390–396, 2013.
[55] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. Sensor network security: a survey. *IEEE Communications surveys & tutorials*, 11(2):52–73, 2009.
[56] Jelena Mirkovic. *D-WARD: source-end defense against distributed denial-of-service attacks*. PhD thesis, University of California, Los Angeles, 2003.
[57] Badis Hammi, Sherali Zeadally, and Rida Khatoun. An empirical investigation of botnet as a service for cyberattacks. *Transactions on emerging telecommunications technologies*, 30(3):e3537, 2019.
[58] Hammi Badis, Guillaume Doyen, and Rida Khatoun. Understanding botclouds from a system perspective: A principal component analysis. In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pages 1–9. IEEE, 2014.
[59] Gareth A Kennedy and Michael D Bedford. Underground wireless networking: A performance evaluation of communication standards for tunnelling and mining. *Tunnelling and underground space technology*, 43:157–170, 2014.
[60] Luca Urciuoli, Toni Männistö, Juha Hintsa, and Tamanna Khan. Supply chain cyber security–potential threats. *Information & Security: An International Journal*, 29(1), 2013.
[61] Ahmad-Reza Sadeghi, Christian Wachsmann, and Michael Waidner. Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, pages 1–6. IEEE, 2015.
[62] Bilal Hussain, Qinghe Du, Bo Sun, and Zhiqiang Han. Deep learning-based ddos-attack detection for cyber–physical system over 5g network. *IEEE Transactions on Industrial Informatics*, 17(2):860–870, 2020.
[63] Cristina Alcaraz and Sherali Zeadally. Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, 8:53–66, 2015.
[64] Muhammad Rizwan Asghar, Qinwen Hu, and Sherali Zeadally. Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, 165:106946, 2019.
[65] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, 14(11):4724–4734, 2018.

[66] André Temprilho, Luís Nóbrega, Paulo Pedreiras, Pedro Gonçalves, and Sérgio Silva. M2M communication stack for intelligent farming. In *2018 Global Internet of Things Summit (GIoTS)*, pages 1–6. IEEE, 2018.
[67] Daniele Antonioli and Nils Ole Tippenhauer. Minicps: A toolkit for security research on cps networks. In *Proceedings of the First ACM workshop on cyber-physical systems-security and/or privacy*, pages 91–100, 2015.
[68] Pompon Raymond and Heath Malcolm. Top Attacks Against Service Providers 2017-2019. Technical report, February 2020.
[69] Spamhaus DDoS attack fails to take down Internet. *Network Security*, 2013(4):1–2, 2013.
[70] Ali Raza. Top 10 DDoS attacks in 2020: Comprehensive Guide. Technical report, NameKoddos, October 2020.
[71] Miu Tony, Yeung Ricky, Cheung Kitson, and Li Dominic. Q1 2020 threat report: Distributed denial of service (ddos). Technical report, Nexusguard, 2020.
[72] Hummel Richard, Hildebrand Carol, Modi Hardik, Conrad Chris, Dobbins Roland, Bjarnson Steinthor, Belanger Jon, Sockrider Gary, Alcoy Philippe, and Bienkowski Tom. Ddos in a time of pandemic. Technical report, NETSCOUT, 2021.
[73] Bulletproof annual cyber security report 2019. Technical report, BULLETPROOF, 2019.
[74] Nick Galov. 39 Jaw-Dropping DDoS Statistics to Keep in Mind for 2021. Technical report, January 2021.
[75] Mark Jones. DDoS attacks cost US businesses $10bn per year. Technical report, March 2019.
[76] McKeay Martin, Ragan Steve, Goedde Amanda, Tuttle Chelsea, Morales Hampe Georgina, and Venukumar Murali. 2020 A Year in Review. Technical report, December 2020.
[77] ANDRA ZAHARIA. 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends (2021 EDITION). Technical report, April 2021.
[78] Q2 2020. The State of DDoS Weapons A Threat Intelligence Report By A10 Networks Security Research. Technical report, A10 Networks, 2020.
[79] Casey Crane. The 15 Top DDoS Statistics You Should Know In 2020. Technical report, November 2019.
[80] Mohammad Masdari and Marzie Jalali. A survey and taxonomy of DoS attacks in cloud computing. *Security and Communication Networks*, 9(16):3724–3751, 2016.
[81] Sandeep Choudhary and Nanhay Singh. Analysis of Security-Based Access Control Models for Cloud Computing. *International Journal of Cloud Applications and Computing (IJCAC)*, 12(1):1–19, 2022.
[82] Rashmi V Deshmukh and Kailas K Devadkar. Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science*, 49:202–210, 2015.
[83] Andrzej Kozlowski. Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal*, 3:237–245, 2014.
[84] Aviram Jenik. Cyberwar in Estonia and the Middle East. *Network Security*, 2009(4):4–6, 2009.
[85] Michael Lesk. The new front line: Estonia under cyberassault. *IEEE Security & Privacy*, 5(4):76–79, 2007.
[86] 2007 cyber attacks on Estonia. Technical report, 2008.
[87] Tamara Denning, Tadayoshi Kohno, and Henry M Levy. Computer security and the modern home. *Communications of the ACM*, 56(1):94–103, 2013.
[88] M Poongodi, Mounir Hamdi, Ashutosh Sharma, Maode Ma, and Pradeep Kumar Singh. DDoS detection mechanism using trust-based evaluation system in VANET. *IEEE Access*, 7:183532–183544, 2019.
[89] Subir Biswas, Jelena Mišić, and Vojislav Mišić. DDoS attack on WAVE-enabled VANET through synchronization. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 1079–1084. IEEE, 2012.
[90] Ademola P Abidoye and Ibidun C Obagbuwa. DDoS attacks in WSNs: detection and countermeasures. *IET Wireless Sensor Systems*, 8(2):52–59, 2018.
[91] IT Revolution Sonatype, Muse Dev. 2020 State of the Software Supply Chain. Technical report, 2020.
[92] JONATHAN BERR. "WannaCry" ransomware attack losses could reach $4 billion. Technical report, May 2017.
[93] Steve Morgan. Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. Technical report, Cybersecurity Ventures, October 2019.
[94] Michael J. Assante. Confirmation of a Coordinated Attack on the Ukrainian Power Grid. Technical report, January 2016.
[95] Kim Zetter. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Technical report, March 2016.
[96] Kyle Wilhoit. KillDisk and BlackEnergy Are Not Just Energy Sector Threats. Technical report, TREND MICRO, February 2016.
[97] Michael Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities. Technical report, July 2015.
[98] Liam O'Murchu. Stuxnet - Infecting Industrial Control Systems. Technical report, September 2010.
[99] David Kushner. The Real Story of Stuxnet. Technical report, February 2013.
[100] William J. Broad, John Markoff, and David E. Sanger. Israeli Test on Worm Called Crucial in Iran Nuclear Delay. Technical report, January 2011.
[101] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. Duqu: A Stuxnet-like malware found in the wild. *CrySyS Lab Technical Report*, 14:1–60, 2011.
[102] Steven Cherry. Sons of Stuxnet. Technical report, December 2011.

[103] Eric Chien, Liam OMurchu, and Nicolas Falliere. W32. Duqu: the precursor to the next stuxnet. In *5th {USENIX} Workshop on Large-Scale Exploits and Emergent Threats ({LEET} 12)*, 2012.
[104] ICS Advisory (ICSA-14-178-01). Technical report, August 2018.
[105] Thomas Roccia. Triton Malware Spearheads Latest Attacks on Industrial Systems. Technical report, McAfee, November 2018.
[106] Blake Sobczak. The inside story of the world's most dangerous malware. Technical report, March 2019.
[107] Robert Falcone. Shamoon 3 Targets Oil and Gas Organization. Technical report, Paloalto Networks, December 2018.
[108] 2020 Data Breach Investigations Report. Technical report, Verizon, 2021.
[109] Cristina Alcaraz and Sherali Zeadally. Critical control system protection in the 21st century. *Computer*, 46(10):74–83, 2013.
[110] Resul Das and Muhammet Zekeriya Gündüz. Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science*, 8(4):122–133, 2020.
[111] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, and Alberto Trombetta. An experimental investigation of malware attacks on SCADA systems. *International Journal of Critical Infrastructure Protection*, 2(4):139–145, 2009.
[112] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ICS) security. *NIST special publication*, 800(82):1–156, 2011.
[113] Jens Mehrfeld. Cyber Security Threats and Incidents in Industrial Control Systems. In *International Conference on Human-Computer Interaction*, pages 599–608. Springer, 2020.
[114] Yassine Mekdad, Giuseppe Bernieri, Mauro Conti, and Abdeslam El Fergougui. A threat model method for ICS malware: the TRISIS case. In *Proceedings of the 18th ACM International Conference on Computing Frontiers*, pages 221–228. ACM, 2021.
[115] Di Pinto Alessandro and MacKenzie Heather. Breaking Research: LockerGoga Ransomware Impacts Norsk Hydro. Technical report, March 2019.
[116] Hau Bill, Lee Tony, and Homan Josh. SYNful Knock - A Cisco router implant - Part I. Technical report, September 2015.
[117] Jose Costa Sapalo Sicato, Pradip Kumar Sharma, Vincenzo Loia, and Jong Hyuk Park. Vpnfilter malware analysis on cyber threat in smart home network. *Applied Sciences*, 9(13):2763, 2019.
[118] Gavin Phillips. How to Spot VPNFilter Malware Before It Destroys Your Router. Technical report, September 2018.
[119] He Terry, Aronce Rhoda-Mae, Dampanaboina Lalith, Jose Justin, King Michael, and Cohen Edward. Cyber threat intelligence for navigating the new business reality. Technical report, 2021.
[120] 2022 Mid year update. Cyber threat intelligence for navigating the unknowns of tomorrow. Technical report, 2022.
[121] Ivana Vojinovic. Ransomware Statistics in 2022: From Random Barrages to Targeted Hits. Technical report, October 2022.
[122] He Terry, Aronce Rhoda-Mae, Dampanaboina Lalith, Jose Justin, King Michael, and Cohen Edward. Updates relating to COVID-19, IT Security Incident, Outlook and Ordinary Dividend. Technical report, 2021.
[123] Office of Public Affairs. Emotet Botnet Disrupted in International Cyber Operation. Technical report, January 2021.
[124] Mohammad Wazid, Sherali Zeadally, and Ashok Kumar Das. Mobile banking: evolution and threats: malware threats and security solutions. *IEEE Consumer Electronics Magazine*, 8(2):56–60, 2019.
[125] Andrew Sanders. 15 (CRAZY) Malware and Virus Statistics, Trends & Facts. Technical report, January 2021.
[126] Mobile ad fraud & malware, Report 2021. A pandemic on mobile. Technical report, Secure-D Upstream, 2021.
[127] Victor Chebyshev. Mobile malware evolution 2020. Technical report, March 2021.
[128] Abbosh Omar and Bissell Kelly. Securing the digital economy, Reinventing the Internet for Trust. Technical report, 2019.
[129] Singleton Camille. X-Force Threat Intelligence Index 2021. Technical report, February 2021.
[130] Gavin Phillips. The State of Ransomware in the US: Report and Statistics 2019. Technical report, DECEMBER 2019.
[131] Rajat Singh Verma and BR Chandavarkar. Hard-coded credentials and web service in iot: Issues and challenges. *International Journal of Computational Intelligence & IoT, Forthcoming*, 2(3), 2019.
[132] Artur Marzano, David Alexander, Osvaldo Fonseca, Elverton Fazzion, Cristine Hoepers, Klaus Steding-Jessen, Marcelo HPC Chaves, Ítalo Cunha, Dorgival Guedes, and Wagner Meira. The evolution of bashlite and mirai iot botnets. In *2018 IEEE Symposium on Computers and Communications (ISCC)*, pages 00813–00818. IEEE, 2018.
[133] Salma Abdalla Hamad, Quan Z Sheng, Wei Emma Zhang, and Surya Nepal. Realizing an internet of secure things: A survey on issues and enabling technologies. *IEEE Communications Surveys & Tutorials*, 22(2):1372–1391, 2020.
[134] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. Understanding the mirai botnet. In *26th {USENIX} security symposium ({USENIX} Security 17)*, pages 1093–1110, 2017.
[135] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.
[136] Georgios Kambourakis, Constantinos Kolias, and Angelos Stavrou. The mirai botnet and the iot zombie armies. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pages 267–272. IEEE, 2017.
[137] Yogeesh Seralathan, Tae Tom Oh, Suyash Jadhav, Jonathan Myers, Jaehoon Paul Jeong, Young Ho Kim, and Jeong Neyo Kim. Iot security vulnerability: A case study of a web camera. In *2018 20th International Conference on Advanced Communication Technology*

(ICACT), pages 172–177. IEEE, 2018.
[138] Worst Passwords of 2018. Technical report, Security TeamsID, June 2020.
[139] Pamela Rentz. Better Check This List: Worst Passwords of 2018. Technical report, Techwell, January 2019.
[140] Tiago M Fernández-Caramés and Paula Fraga-Lamas. Teaching and Learning IoT Cybersecurity and Vulnerability Assessment with Shodan through Practical Use Cases. *Sensors*, 20(11):3048, 2020.
[141] Béla Genge and Călin Enăchescu. Shovat: Shodan-based vulnerability assessment tool for internet-facing services. *Security and communication networks*, 9(15):2696–2714, 2016.
[142] John Matherly. Complete guide to shodan. *Shodan, LLC*, 1:1–70, 2016.
[143] Areej Albataineh and Izzat Alsmadi. Iot and the risk of internet exposure: Risk assessment using shodan queries. In *2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pages 1–5. IEEE, 2019.
[144] Bitdefender. Remote Exploitation of the NeoCoolcam IP Cameras and Gateway. Technical report, Bitdefender, 2015.
[145] Joseph Bugeja, Désirée Jönsson, and Andreas Jacobsson. An Investigation of Vulnerabilities in Smart Connected Cameras. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pages 537–542. IEEE, 2018.
[146] Zakir Durumeric, Frank Li, James Kasten, Johanna Amann, Jethro Beekman, Mathias Payer, Nicolas Weaver, David Adrian, Vern Paxson, Michael Bailey, et al. The matter of heartbleed. In *Proceedings of the 2014 conference on internet measurement conference*, pages 475–488, 2014.
[147] Marco Carvalho, Jared DeMott, Richard Ford, and David A Wheeler. Heartbleed 101. *IEEE security & privacy*, 12(4):63–67, 2014.
[148] Yves Christian Elloh Adja, Badis Hammi, Ahmed Serhrouchni, and Sherali Zeadally. A blockchain-based certificate revocation management and status verification system. *Computers & Security*, 104:102209, 2021.
[149] Paul Mutton. Certificate revocation: Why browsers remain affected by Heartbleed. Technical report, Netcraft, April 2014.
[150] Baden Delamore and Ryan KL Ko. A global, empirical analysis of the shellshock vulnerability in web applications. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1129–1135. IEEE, 2015.
[151] Marcus Willett. Lessons of the SolarWinds Hack. *Survival*, 63(2):7–26, 2021.
[152] Oxford Analytica. SolarWinds hack will alter US cyber strategy. *Emerald Expert Briefings*, (oxan-db).
[153] Oxford Analytica. Fallout of SolarWinds hack could last for years. *Emerald Expert Briefings*, (oxan-es), 2020.
[154] Defining Insider Threats. Technical report, April 2021.
[155] Sherali Zeadally, Byunggu Yu, Dong Hyun Jeong, and Lily Liang. Detecting insider threats: Solutions and trends. *Information security journal: A global perspective*, 21(4):183–192, 2012.
[156] Insider threat. ENISA Threat Landscape. Technical report, European Union Agency for Cybersecurity (ENISA), 2020.
[157] 2021 Cyberthreat Defense Report. Technical report, CyberEdge Group, 2021.
[158] Webroot threat report. Technical report, Webroot, 2020.
[159] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. Sok: Security evaluation of home-based iot deployments. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1362–1380. IEEE, 2019.
[160] Jonathan Wells. *Better Practices for IoT Smart Home Security*. PhD thesis, Utica College, 2020.
[161] Nic Chantler and Roderic Broadhurst. Social engineering and crime prevention in cyberspace. *Proceedings of the Korean Institute of Criminology*, pages 65–92, 2008.
[162] Internet Crime Report 2020. Technical report, Federal Bureau of Investigation (FBI), 2021.
[163] Phishing Activity Trends Report, Fourth Quarter 2020. Technical report, APWG, February 2021.
[164] Is cybersecurity about more than protection? EY Global Information Security Survey 2018–19. Technical report, EY Global, 2018.
[165] Jon Boyens, Celia Paulsen, Rama Moorthy, and Nadya Bartol. Supply chain risk management practices for federal information systems and organizations. Technical report, National Institute of Standards and Technology (NIST), 2015.
[166] Marjorie Windelberg. Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, 12:4–11, 2016.
[167] Debra S Herrmann. *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*. CRC Press, 2007.
[168] Debra S Herrmann. *A practical guide to security engineering and information assurance*. CRC Press, 2001.
[169] Debra S Herrmann. Software safety and reliability. Institute of Electrical & Electronics Engineers, 2000.
[170] Ludovic Piètre-Cambacédès and Claude Chaudet. The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”. *International Journal of Critical Infrastructure Protection*, 3(2):55–66, 2010.
[171] IT SUPPLY CHAIN. National Security-Related Agencies Need to Better Address Risks. Technical report, March 2012.
[172] Obama Barack. Remarks by the President on Securing Our Nation’s Cyber Infrastructure. Technical report, May 2009.
[173] Cherian Samuel and Munish Sharma. *Securing cyberspace: International and Asian perspectives*. Institute for Defence Studies and Analyses, 2016.
[174] Mu Rongping and Fan Yonggang. Security in the cyber supply chain: A Chinese perspective. *Technovation*, 7(34):385–386, 2014.

[175] Scott Charney, Eric T Werner, and Trustworthy Computing. Cyber supply chain risk management: Toward a global vision of transparency and trust. *Microsoft Corporation paper*, pages 1–19, 2011.
[176] The Comprehensive National Cybersecurity Initiative. Technical report, 2008.
[177] Security and Privacy Controls for Information Systems and Organizations. Technical report, National Institute of Standards and Technology (NIST), 2020.
[178] Jon Boyens, Nadya Bartol, Jon Boyens, Rama Moorthy, Celia Paulsen, and Stephany A Shankles. Notional supply chain risk management practices for federal information systems. Technical report, US Department of Commerce, National Institute of Standards and Technology (NIST), 2012.
[179] H.r.6523 - ike skelton national defense authorization act for fiscal year 2011. Technical report, January. 7, 2011.
[180] Consultation Paper on Encouraging Telecom Equipment Manufacturing in India. Technical report, December, 2010.
[181] Martina F Ferracane and Hosuk Lee-Makiyama. China's technology protectionism and its non-negotiable rationales. *Brussels: European Centre for International Political Economy*, 2017.
[182] Technology Security and IT in China: Benchmarking and Best Practices. Technical report, July 2016.
[183] Alexander Sokolov, Vladimir Mesropyan, and Alexander Chulok. Supply chain cyber security: A Russian outlook. *Technovation*, 34(7):389–391, 2014.
[184] Bilal Al Sabbagh and Stewart Kowalski. A socio-technical framework for threat modeling a software supply chain. *IEEE Security & Privacy*, 13(4):30–39, 2015.
[185] Abel Yeboah-Ofori and Shareeful Islam. Cyber security threat modeling for supply chain organizational environments. *Future Internet*, 11(3):63, 2019.
[186] Chung Kit Wu, Kim Fung Tsang, Yucheng Liu, Hongxu Zhu, Yang Wei, Hao Wang, and Tsz Tat Yu. Supply chain of things: A connected solution to enhance supply chain productivity. *IEEE Communications Magazine*, 57(8):78–83, 2019.
[187] Stacy Simpson, Diego Baldini, Gunter Bitz, David Dillard, Chris Fagan, Brad Minnis, and Dan Reddy. Software integrity controls–an assurance-based approach to minimizing risks in the software supply chain. Technical report, Software Assurance Forum for Excellence in Code (SAFECode), June 2010.
[188] Christopher J Alberts, Audrey J Dorofee, Rita Creel, Robert J Ellison, and Carol Woody. A systemic approach for assessing software supply-chain risk. In *2011 44th Hawaii International Conference on System Sciences*, pages 1–8. IEEE, 2011.
[189] Tyson Storch. Toward a trusted supply chain: A risk based approach to managing software integrity. *Trustworthy Computing Microsoft Corporation*, pages 1–25, 2014.
[190] Bharat Bhargava, Rohit Ranchal, and Lotfi Ben Othmane. Secure information sharing in digital supply chains. In *2013 3rd IEEE international advance computing conference (IACC)*, pages 1636–1640. IEEE, 2013.
[191] Jun Huang, Xiang Li, Cong-Cong Xing, Wei Wang, Kun Hua, and Song Guo. DTD: A novel double-track approach to clone detection for RFID-enabled supply chains. *IEEE Transactions on Emerging Topics in Computing*, 5(1):134–140, 2015.
[192] Sk Subidh Ali, Mohamed Ibrahim, Jeyavijayan Rajendran, Ozgur Sinanoglu, and Krishnendu Chakrabarty. Supply-chain security of digital microfluidic biochips. *Computer*, 49(8):36–43, 2016.
[193] Joseph P Skudlarek, Tom Katsioulas, and Michael Chen. A platform solution for secure supply-chain and chip life-cycle management. *Computer*, 49(8):28–34, 2016.
[194] Dongrong Zhang, Xiaoxiao Wang, Md Tauhidur Rahman, and Mark Tehranipoor. An on-chip dynamically obfuscated wrapper for protecting supply chain against IP and IC piracies. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 26(11):2456–2469, 2018.
[195] Alireza Esfahani, Georgios Mantas, Jose Ribeiro, Joaquim Bastos, Shahid Mumtaz, Manuel A Violas, A Manuel De Oliveira Duarte, and Jonathan Rodriguez. An efficient web authentication mechanism preventing man-in-the-middle attacks in industry 4.0 supply chain. *IEEE Access*, 7:58981–58989, 2019.
[196] Thomas Bocek, Bruno B Rodrigues, Tim Strasser, and Burkhard Stiller. Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE symposium on integrated network and service management (IM)*, pages 772–777. IEEE, 2017.
[197] Haoyan Wu, Zhijie Li, Brian King, Zina Ben Miled, John Wassick, and Jeffrey Tazelaar. A distributed ledger for supply chain physical distribution visibility. *Information*, 8(4):137, 2017.
[198] Paolo Bellavista, Christian Esposito, Luca Foschini, Carlo Giannelli, Nicola Mazzocca, and Rebecca Montanari. Interoperable Blockchains for Highly-Integrated Supply Chains in Collaborative Manufacturing. *Sensors*, 21(15):4955, 2021.
[199] Lei Xu, Lin Chen, Zhimin Gao, Yanling Chang, Eleftherios Iakovou, and Weidong Shi. Binding the physical and cyber worlds: A blockchain approach for cargo supply chain security enhancement. In *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–5. IEEE, 2018.
[200] MediLedger 2018 Progress Report. Technical report, 2018.
[201] TradeLens Documentation, 2018. Accessed:2021-08-06.
[202] Simone Figorilli, Francesca Antonucci, Corrado Costa, Federico Pallottino, Luciano Raso, Marco Castiglione, Edoardo Pinci, Davide Del Vecchio, Giacomo Colle, Andrea Rosario Proto, et al. A blockchain implementation prototype for the electronic open source

traceability of wood along the whole supply chain. *Sensors*, 18(9):3133, 2018.
[203] Kentaroh Toyoda, P Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki. A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain. *IEEE access*, 5:17465–17477, 2017.
[204] Miguel Pincheira Caro, Muhammad Salek Ali, Massimo Vecchio, and Raffaele Giaffreda. Blockchain-based traceability in agri-food supply chain management: A practical implementation. In *2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany)*, pages 1–4. IEEE, 2018.
[205] Waltonchain White Paper (V 1.0.4). Technical report, February 2018.
[206] Hyperledger. How walmart brought unprecedented transparency to the food supply chain with hyperledger fabric. page 7, 2019.
[207] Sidra Malik, Volkan Dedeoglu, Salil S Kanhere, and Raja Jurdak. Trustchain: Trust management in blockchain and iot supported supply chains. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 184–193. IEEE, 2019.
[208] Sean Barnum. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, 11:1–22, 2012.
[209] Robert J Ellison and Carol Woody. Supply-chain risk management: Incorporating security into software development. In *2010 43rd Hawaii International Conference on System Sciences*, pages 1–10. IEEE, 2010.
[210] Christopher Huth, Aydin Aysu, Jorge Guajardo, Paul Duplys, and Tim Güneysu. Secure and Private, yet Lightweight, Authentication for the IoT via PUF and CBKA. In *International Conference on Information Security and Cryptology*, pages 28–48. Springer, 2016.
[211] Aakanksha Tewari and Brij B Gupta. An analysis of provable security frameworks for RFID security. In *Handbook of computer networks and cyber security*, pages 635–651. Springer, 2020.
[212] Brij B Gupta, Gregorio Martinez Perez, Dharma P Agrawal, and Deepak Gupta. *Handbook of computer networks and cyber security*. Springer, 2020.
[213] Xiaoxiao Wang, Dongrong Zhang, Miao He, Donglin Su, and Mark Tehranipoor. Secure scan and test using obfuscation throughout supply chain. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(9):1867–1880, 2017.
[214] Nikolaos Karapanos and Srdjan Capkun. On the Effective Prevention of {TLS} Man-in-the-Middle Attacks in Web Applications. In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pages 671–686, 2014.
[215] Sherali Zeadally and Jacques Bou Abdo. Blockchain: Trends and future opportunities. *Internet Technology Letters*, 2(6):e130, 2019.
[216] Niels Hackius and Moritz Petersen. Blockchain in logistics and supply chain: trick or treat? In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23*, pages 3–18. Berlin: epubli GmbH, 2017.
[217] Mahtab Kouhizadeh and Joseph Sarkis. Blockchain practices, potentials, and perspectives in greening supply chains. *Sustainability*, 10(10):3652, 2018.
[218] Saveen A Abeyratne and Radmehr P Monfared. Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9):1–10, 2016.
[219] Kari Korpela, Jukka Hallikas, and Tomi Dahlberg. Digital supply chain transformation toward blockchain integration. In *proceedings of the 50th Hawaii international conference on system sciences*, 2017.
[220] Andreas Kamilaris, Agusti Fonts, and Francesc X Prenafeta-Bold\'ν. The rise of blockchain technology in agriculture and food supply chains. *Trends in Food Science & Technology*, 91:640–652, 2019.
[221] Oi Wa Amy Lam and LEI Zhibin. Textile and apparel supply chain with distributed ledger technology (DLT). In *2019 20th IEEE International Conference on Mobile Data Management (MDM)*, pages 447–451. IEEE, 2019.
[222] Si Chen, Rui Shi, Zhuangyu Ren, Jiaqi Yan, Yani Shi, and Jinyu Zhang. A blockchain-based supply chain quality management framework. In *2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, pages 172–176. IEEE, 2017.
[223] Po-Yeuan Chang, Min-Shiang Hwang, and Chao-Chen Yang. A blockchain-based traceable certification system. In *International Conference on Security with Intelligent Computing and Big-data Services*, pages 363–369. Springer, 2017.
[224] Feng Tian. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In *2016 13th international conference on service systems and service management (ICSSSM)*, pages 1–6. IEEE, 2016.
[225] Daniel Tse, Bowen Zhang, Yuchen Yang, Chenli Cheng, and Haoran Mu. Blockchain application in food supply information security. In *2017 IEEE international conference on industrial engineering and engineering management (IEEM)*, pages 1357–1361. IEEE, 2017.
[226] Mitsuaki Nakasumi. Information sharing for supply chain management based on block chain technology. In *2017 IEEE 19th conference on business informatics (CBI)*, volume 1, pages 140–149. IEEE, 2017.
[227] Kaijun Leng, Ya Bi, Linbo Jing, Han-Chi Fu, and Inneke Van Nieuwenhuyse. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Generation Computer Systems*, 86:641–649, 2018.
[228] Petri Helo and Yuqiuge Hao. Blockchains in operations and supply chains: A model and reference implementation. *Computers & Industrial Engineering*, 136:242–251, 2019.
[229] Branimir Rakic, Tomaz Levak, Ziga Drev, Sava Savic, and Aleksandar Veljkovic. First purpose built protocol for supply chains based on blockchain. Technical report, 2017.
[230] CargoX Business Overview and Technology Bluepaper. Technical report, 2018.

[231] Ambrosus White Paper. Technical report, 2017.
[232] Sebastian Haag and Reiner Anderl. Digital twin–proof of concept. *Manufacturing Letters*, 15:64–66, 2018.
[233] Stefan Boschert and Roland Rosen. Digital twin—the simulation aspect. In *Mechatronic futures*, pages 59–74. Springer, 2016.
[234] Badis Hammi, Achraf Fayad, Rida Khatoun, Sherali Zeadally, and Youcef Begriche. A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal*, 14(3):3440–3450, 2020.
[235] Kristin Lauter. The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless communications*, 11(1):62–67, 2004.
[236] Sherali Zeadally, Ashok Kumar Das, and Nicolas Sklavos. Cryptographic technologies and protocol standards for Internet of Things. *Internet of Things*, page 100075, 2019.
[237] Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot, and Ahmed Serhrouchni. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, 78:126–142, 2018.
[238] Alireza Shamsoshoara, Ashwija Korenda, Fatemeh Afghah, and Sherali Zeadally. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Computer Networks*, 183:107593, 2020.
[239] George Baryannis, Samir Dani, and Grigoris Antoniou. Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. *Future Generation Computer Systems*, 101:993–1004, 2019.
[240] David Zage, Kristin Glass, and Richard Colbaugh. Improving supply chain security using big data. In *2013 IEEE International Conference on Intelligence and Security Informatics*, pages 254–259. IEEE, 2013.
[241] Elena Camossi, Tatyana Dimitrova, and Aris Tsois. Detecting anomalous maritime container itineraries for anti-fraud and supply chain security. In *2012 European Intelligence and Security Informatics Conference*, pages 76–83. IEEE, 2012.