Security and Privacy in Cyber–Physical Systems: A Survey of Surveys

Jairo Giraldo, Esha Sarkar, and Alvaro A. Cardenas
University of Texas at Dallas

Michail Maniatakos and Murat Kantarcioglu
New York University Abu Dhabi

Editor's note:
The following is a survey on surveys and may help the interested reader to find a way through the jungle of literature on the security and CPS topics out there already. In order to ease the search, the authors have provided a classification in CPS Domains, Attacks, Defenses, Research-trends, Network-security, Security level implementation, and Computational Strategies which makes this survey a unique and I believe very helpful article.

—Jörg Henkel, Karlsruhe Institute of Technology

■ **The term cyber–physical** systems (CPSs) emerged just over a decade ago as an attempt to unify the emerging application of embedded computer and communication technologies to a variety of physical domains, including aerospace, automotive, chemical production, civil infrastructure, energy, healthcare, manufacturing, materials, and transportation.

In their program announcement, the National Science Foundation outlined their goal for considering these various industries under a unified lens: by abstracting from the particulars of specific applications in these domains, the goal of the CPS program is to reveal crosscutting fundamental scientific and engineering principles that underpin the integration of cyber and physical elements across all application sectors.

Figure 1 illustrates a general architecture for CPSs, where computation (top) interfaces through networks with physical processes (bottom).

Soon after the CPS term was coined, several research communities rallied to outline and understand how CPS security research is fundamentally different compared to conventional Information Technology (IT) systems. Because of the crosscutting nature of CPS, the background of early security position papers from 2006 to 2009 using the term CPS, ranged from real-time systems [1], [2], embedded systems [3], [4], control theory [5], and cyber-security [4], [6]–[9].

In the crosscutting spirit of CPS, these early papers discussed CPS security challenges from a multidisciplinary perspective: this is a differentiator of CPS security compared to earlier work on security for specific CPS domains, such as Supervisory Control and Data Acquisition (SCADA) systems in the power grid [10].

In the following years, CPS research evolved into a mature field spawning multiple surveys. One of the first surveys on CPS was written by Kim and Kumar [11], and it included several CPS research efforts real-time systems, wireless networks, and security. Recently, we have seen a large increase in the surveys of CPS focusing exclusively on security and/or privacy issues, and therefore we believe it is valuable to provide an overview of the different surveys to map systematically research trends, open challenges, and areas that have been unaddressed by previous work. While several of the surveys we include in this paper focus on a specific application [e.g., smart grids and intelligent transportation

Digital Object Identifier 10.1109/MDAT.2017.2709310
Date of publication: 29 May 2017; date of current version: 30 June 2017.

2168-2356/17 © 2017 IEEE

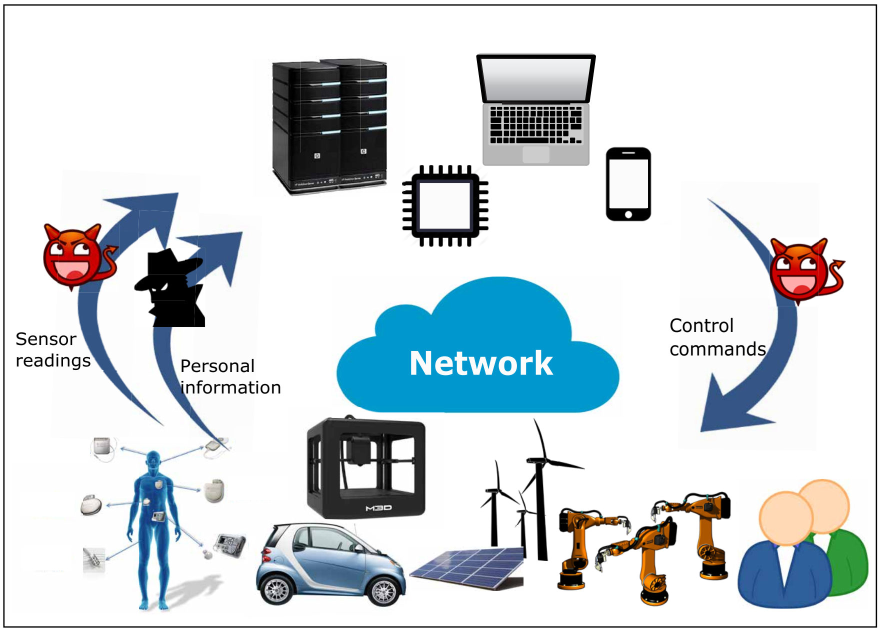

Figure 1. General representation of a CPS. Security challenges arise when the computation is corrupted by false sensor information or when the control centers send malicious control actions to the physical process.

systems (ITSs)] our hope is that by presenting them together, along with other related surveys in other CPS domains, we can encourage the type of crosscutting research to address problems in a variety of domains.

Taxonomy

We have categorized surveys on CPS security and privacy by focusing on one or more of the following characteristics:

- CPS domains,
- attacks,
- defenses,
- research trends,
- network security,
- security-level implementation, and
- computational strategies.

We mapped these characteristics in a taxonomy to help us to study the different features of each work, as depicted in Figure 2.

Different domains

We have identified five CPS domains that are the focus of most of the work addressed in the surveys. The smart grid has motivated most of the studies in security of CPS, but lately there has been an increasing interest on manufacturing, medical devices, industrial control systems (ICSs), and ITSs.

Several surveys focus on one specific domain, and we have tried to describe several surveys within their domains. Some other surveys are not domain-specific and describe more generic problems that affect all CPSs, and some other surveys focus on only one domain, but we could not find other surveys in the same domain. For instance, we have identified only one survey in the security of drones. Therefore, we have added a miscellaneous category to the taxonomy.

So, we have six main domains:

- smart grids,
- medical devices,
- ICSs,
- manufacturing,
- ITSs, and
- miscellaneous.

Security

We say a survey focuses on security when it addresses attacks that affect the integrity of the information or devices in the system. These attacks can affect directly the physical part of the process or the cyber elements. In our taxonomy, we consider two attacks covered by the surveys:

Physical: Attacks that tamper directly physical elements in the CPS. For instance, changing the batteries of an implantable medical device.

Cyber: The type of attacks that are deployed through malware, software, or by gaining access to elements of the communication network. For example, faking sensor information.

Privacy

CPS relies on granular and diverse sensors that may compromise the privacy of the users of these new technologies. Attacks on privacy are mostly passive, and may require to gain certain access to private data, or make inferences about specific information from public data.

Defenses

After identifying the vulnerabilities of a CPS, it is necessary to develop defenses that will prevent or make harder the access to adversaries. We classify the defenses in three groups:

Prevention: Prevention refers to security mechanisms that prevent attacks by providing authentication, access controls, security policies, and network segmentation.

Detection: Even though preventive strategies are necessary, adversaries with enough resources, time, and commitment can still bypass them and launch successful attacks against the CPS system. Detection strategies are designed to identify anomalous behavior and attacks in the system.

Response: Because most CPS have real-time constraints, a security mechanism may need to act automatically (without waiting for human intervention) to mitigate the detected attacks. Reactive response refers to the actions executed after an attack is detected, and aims to mitigate the impact of the attack and, if possible, restore the system. In particular, we focus on those that are launched online (as a reaction to the detection of the attack) and are mostly automatic. For instance, switching between real sensors to simulated sensors, or switching to redundant systems.

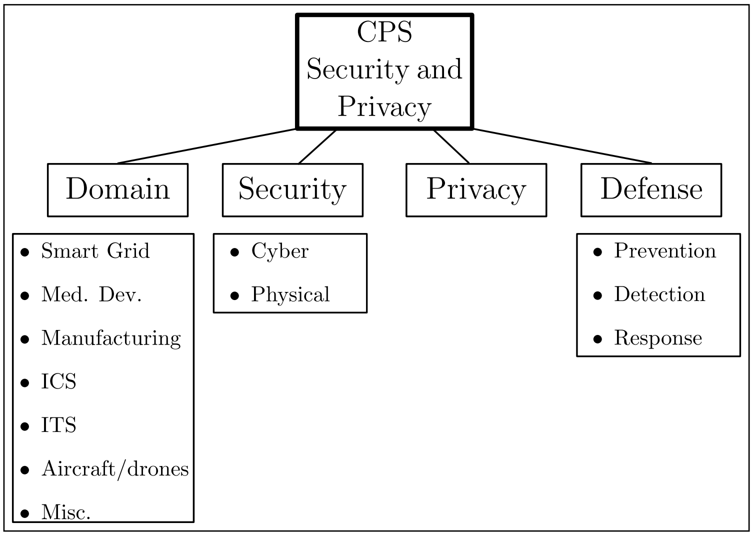

Figure 2. Taxonomy of CPS surveys

Smart grids

The power grid is one of the most complex, interconnected systems ever engineered. Unlike other essential resources that can be effectively stored like water or oil, electric power must be generated at the same time it is consumed, and therefore, any temporary disruption to this process can cause significant damages. It is no surprise that given our dependence on the correct operation of the power grid at all times, this CPS domain has captured most of the efforts of researchers. We now summarize several surveys on the topic.

The power grid consists of generation, transmission, and distribution and each of these systems has a different type of risk and potential attacks. He et al. [12] summarize possible cyberattacks at all the stages of the grid. For instance, attacks on generation, such as the Aurora attack, can desynchronize power generators and damage them; attacks on transmission can affect substations and relays, as well as one of the most studied types of attacks; state estimation attacks, where by modifying some measurements it is possible to inject stealthy false information to mislead the estimation of phase angles. Finally, attacks on distribution include electricity theft and information/privacy leakages by compromising smart meters. They also summarize defensive strategies, and they are similar to our proposed taxonomy. They focus on

- protection, by enhancing communications and introducing encrypted devices optimally located;
- attack-detection, by employing signature-based and behavior-based IDSs; and
- mitigation, which minimizes the potential disruptions and damages caused by an attack.

Liu et al. [13] focus their survey on the specific technologies of the power grid, rather than on the stages of the power grid. They focus on the security of

- device,
- network,
- dispatch and management,
- anomaly detection, and
- other issues.

For example, devices used in the power grid like remote terminal units or intelligent electronic devices allow administrators to connect from remote locations, and these can be exploited by adversaries. Networking issues are also important, and the authors point out that wireless networks are becoming more prevalent and care must be taken against jamming attacks. New functionalities of the smart grid may also introduce new vulnerabilities, such as the problem of demand response, where the electric utilities or demand response companies try to influence consumer behavior through a variety of incentives, but which may be a new vector of attack if the information exchanged between consumers and their providers is compromised.

In addition to security, new functionalities in the smart grid like smart meters also pose privacy concerns. Jawurek et al. [14] present one of the most comprehensive summaries of problems associated to privacy in smart grids. Smart meters can be used for a variety of applications, including load monitoring, forecasting, efficiency analysis, billing, demand respond, fraud detection, settlement, and interfacing with electric vehicles, and all of these activities can reveal potential sensitive data about the activities of a household. Jawurek et al. focus on adversaries that eavesdrop information to make inferences about users. They discuss the legal frameworks that try to enhance privacy of users by imposing laws and regulations (e.g., minimization principle). They state that in current smart grid deployments, the protection of personal information is achieved by policy tools; however, policy tools rely on the honesty of all parties that come into contact with data, which is not the case of malicious adversaries. The main privacy risks are are nonintrusive load monitoring (which allows an attacker to infer which device is being used), and use mode detection (which allow an adversary to infer what activity is being performed by the device, such as detecting television channels). To mitigate privacy risks, the authors highlight several techniques:

- anonymization,
- trusted computing (attestation),
- cryptographic approaches,
- perturbation [differential privacy (DP)], and
- verifiable computation.

They study all five techniques for aggregation, billing, and household computation. Finally, they introduce a technique based on the use of batteries to mask the amount of energy consumed.

One of the goals of the smart grid is to change the way consumers interact with their energy providers. The survey by Komninos et al. [15] focuses on electricity consumption at homes and buildings. “Smart homes” consist of households that are energy-aware by leveraging of sensors and networking technologies to communicate among appliances and smart meters with the power grid. Smart homes in particular communicate with the smart grid to support demand response programs, control distributed energy resources, and consumption monitoring. Moreover, various appliances in the smart home such as washing machines, pool pumps, PEVs, and air conditioning systems are intelligently managed to optimize its effects over the grid. The authors identify six security goals: confidentiality, integrity, availability, authenticity, authorization, and repudiation. Based on these goals, a wide number of attacks are identified; they are classified into passive (privacy) or active (security attacks that affect the information that is being shared). Active attacks include also physically tampering with smart meters or system sensors. Different countermeasures are identified for each of the security goals, such as encryption, digital watermarking, and intrusion detection systems. However, they do not discuss any response once an attack is detected.

Since most cyber-security vulnerabilities in smart grids are related to the protection of data, it is necessary to secure data, not only in transit (when it is injected in a network) but also at rest, i.e., the data stored and processed. The survey by Tan et al. [16] focuses on a taxonomy of the life cycle of smart grid data, which can be decomposed into four sequential stages: generation of data, acquisition, storage, and processing. Specific security characteristics are summarized for each stage. In particular, generation and acquisition include different sources of data such as PMUs and smart meters, and the acquisition process carried out by the communication infrastructure. Vulnerabilities in these two stages overlap with other surveys that focus on the different communication protocols, and the issues on sharing sensitive information. However, one unique characteristic of the survey by Tan’s et al. is the analysis of storage data and processing data. Data storage in the smart grid is a vital component used for a wide number of functionalities, such as failure detection, demand response, forecasting, and billing. The authors also tackle different defense mechanisms that they called data analytics. They argue that a huge amount of data can be processed to identify patterns, predict, and prescribe solutions, using statistical analysis, data mining, and data visualization.

Finally, smart grid testbeds are an important resource for security experimentation. Cintuglu et al. [17] review several smart grid testbeds and they highlight the importance of being able to evaluate the coupled interaction between the physical and cyber components. They propose several taxonomies based on the target research area of the testbed, the communication infrastructure, and the platform type. In particular, the authors show that several testbeds can be used to evaluate different types of cyberattacks, such as man-in-the-middle and eavesdropping attacks. Real vulnerabilities of the smart grid communication infrastructure are evaluated using protocols such as DNP3 and IEC 61850, and in some cases, intrusion detection algorithms can be implemented and tested. The authors identify testbeds as a fundamental component for creating better security and privacy awareness for consumers as well as asset owners.

Security in medical devices

Due to their safety and privacy risks, embedded medical devices are another CPS domain that has received significant attention in the literature. Modern implantable medical devices include pacemakers, defibrillators, neurostimulators, and drug delivery systems. These devices can usually be queried and reprogrammed by a doctor, but this also opens these devices to security and privacy threats.

Rushanan et al. [18] and Camara et al. [19] describe the types of adversaries that medical devices will be subject to, including the ability to eavesdrop all communication channels (passive) or read, modify, and inject data (active). The threats are mainly focused on telemetry interface, but Rushanan et al. [18] also take into account software, hardware, and sensor interfaces. To mitigate possible attacks in the telemetry interface, they propose authentication (e.g., biometric, distance bounding, and out-of-band channels), and the use of an external wearable device that allows or denies access to the medical device, depending on whether or not this extra wearable device is present or not. In addition to prevention, they also discuss attack-detection by observing patterns to distinguish between safe and unsafe behavior.

AlTawy and Youssef [20] consider the tradeoffs in CPS, with a case study on implantable medical devices. They consider both cyber and physical attacks tampering with batteries and switches. The authors argue that due to physical constraints, protecting these devices is hard. For instance, because these devices are inside the body, they have to be small, the RF radiation should be low, and power dissipation low. Also, due to the size, the battery should last for 8–10 years and power should be managed efficiently, as changing a battery might require surgery. For these reasons, cryptographic solutions should be efficient. Challenges related to attack-detection are also highlighted. Another tradeoff for access control is that in the case of emergency, it should be possible for health professionals to have access to these devices, and it is hard to determine with certainty what is an emergency condition and what is not.

Security in ICS

Security of ICS is a term used to refer to technologies to monitor and control industrial, electrical, and even manufacturing processes. An introduction to these systems as well as how their protection is different from IT networks is summarized in the NIST document SP 800-82 [21]. This document is a summary of the best practices and technology recommendations from a wide variety of security solutions.

Beyond the best practices, a concise survey of research done in ICS security was given by Krotofil and Gollmann [22]. As with other CPS domains, the ICS industry has relied on obscurity to claim their systems are secure, but the authors argue that this notion has been debunked by many studies that revealed software, hardware, and firmware vulnerabilities, and unfortunately by real-world attacks. They discuss protocol-related vulnerabilities for Modbus/TCP, DNP3, and IEC 61850 along with other fieldbus and other sensor/actuator-related vulnerabilities. They also discuss several countermeasures, focusing on the different types of information that intrusion detection systems can look into: information about packets and SCADA event logs, critical states of the systems, and network-based anomaly detection.

McLaughlin et al. [23] suggest an eight-step process for an exhaustive vulnerability assessment, from document analysis to final testing. The mitigation strategies focus largely on novel control architectures that customize their mechanism according to the domain: checking of control code, a run-time reference monitor architecture, an architecture that gives an estimate of time for reaching unsafe states, and an architecture with a trusted computing base.

Urbina et al. [24] focus on leveraging the physical characteristics of the system itself to detect attacks (i.e., physics-based intrusion detection). The authors discuss the need to have a clearly defined

- model of the physical system,
- trust assumptions,
- statistical test used for anomaly detection, and
- a way to evaluate the effectiveness of the anomaly detector (metrics).

These four characteristics are then identified in a wide variety of publications across several CPS domains, including power systems, ICSs, control theory, automated vehicles, video cameras, electricity theft, and medical devices. They also summarize the differences between using real-world systems, testbeds, and simulations. They conclude by discussing the common assumptions and shortcomings of this class of research, and suggest several improvements, including where to place the security monitor, and also propose a new metric for evaluating the effectiveness of physics-based intrusion detection models.

Security and privacy concerns of industrial Internet of things (IoTs) are also addressed by [25]. As mitigations, the authors propose the use of integrity checking techniques through software and hardware. The authors also point out that although remote device management is crucial, exporting heterogeneous information from IoT devices to external services may create privacy risks, and argue that we should look at better ways to provide local management.

Another survey that reviews prevention and detection approaches for cyberattacks in ICS is given by Cheminod et al. [26]. The authors agree with one of our conclusions: while there is a wide diversity of prevention and detection solutions, there are few proposed approaches that are able to react to attacks and to recover or heal the protected system.

Manufacturing

Security in manufacturing has been for many years a part of critical infrastructure security, but as the manufacturing process became more sophisticated, the threats increased. Wells et al. [27] give a high-level view about the concerns of this industry. They also mention that quality control techniques traditionally used in the manufacturing industry can be leveraged to detect attacks.

Pan et al. [28] take the analysis further by developing a twofold taxonomy. The first part classifies attacks according to the attack mechanism deployed, the vulnerability it exploited, which component of the system can be targeted, and what is the impact. The second part to analyze security is to focus on how quality control can detect attacks. There are physical and cyber-tests: the physical tests include nondestructive tests such as visual inspection, weight measure, dimension measure, 3-D laser scanning, interferometry, X-ray, and CT, and destructive mechanical tests like employing the tensile and yield properties of the material. The authors mention a third avenue for physical testing via side-channel analysis based on temperature, power, and timing. The cyber-domain-based measures work more on the confidentiality front, stating design file hashing and network authentication as suitable measures. The survey mentions a lack of research in faults injected in physical parts that have no computational logic, which calls for a mechanical engineering-based outlook to these measures.

Zeltmann et al. [29] discuss how manufacturing defects could be introduced by compromised design files. Characterization of these samples are done using tensile strengthening and nondestructive ultrasonic inspection. The authors also demonstrate how finite element analysis can help in understanding the impact of defects. A comparative study is also done in detecting these distortions for different sizes of defects and different orientations of printing. This paper also gives insight into the similarities between 3-D printing and an IC manufacturing chain, but since the volume of production is different, similar defenses cannot be used.

Intelligent transportation

Vehicles and the infrastructure that supports them are being modernized with new physical sensors (cameras, loop detectors, etc.), collaborative sensing (e.g., Waze), autonomous vehicles (e.g., cooperative cruise control), and collaborative information sharing (vehicle to infrastructure and vehicle-to-vehicle communications). This leads to several new security and privacy considerations.

van der Heijden et al. [30] compare mechanisms to detect malicious nodes and malicious data in ITSs. The authors start the analysis of misbehavior detection by defining a domain-specific taxonomy of misbehaviors based on whether the anomaly arose from inconsistent nodes or data. The paper surveys attack-detection schemes on three levels: local, cooperative, and global. For detecting misbehavior, the authors state that linkability between the on-board units (OBU) and messages is crucial and the schemes are developed based on the degree of linkability available.

Vehicular ad hoc NETworks (VANETs) focus on the interaction between OBU and road-side units (RSU) and depending on these interactions, they form V2V or V2I systems. Sakiz and Sen [31] wrote a survey of the mechanisms typically proposed for defense in VANETs. Apart from watchdog-based defenses, the survey has a high inclination toward model-based security mechanisms, such as mechanical modeling, trust-based modeling, and Markov-chain modeling. As a part of security-technique analysis, the survey does a comparative study of the infrastructure of the system and the attacks that the particular technique can thwart. The study also mentions that most of these defenses aim at discovering misbehavior at a particular layer and urges researchers to work on reliability of links.

One of the major challenges of modeling a transportation system is its agility and that problem becomes magnified while developing security features in them. Additional problems of security are scalability, lack of clear line of defense, and real-time operations [31]. Moreover, the nomenclature of subdomains does not follow a strictly standardized format, making it difficult to compare security approaches. Looking specifically at the car, Zheng et al. [32] also summarize security problems in cars and modern infotainment systems.

Aircraft and drones

The expansion of unmanned aerial vehicles has increased security and privacy concerns. In general, there is a lack of security standards for drones and it has been shown that they are vulnerable to attacks that target either the cyber and/or physical elements [33]. Altawy and Youssef [33] survey various possible attacks that may affect privacy, and also discuss how several attacks like falsifying GPS information, or manipulating control commands can make the drones to malfunction. They also review possible physical attacks, such as theft or weather changes. The authors also point out possible solutions to mitigate the impact of these attacks, such as encryption and IDS.

Another relevant CPS problem arises from the aviation community and the efforts to modernize aircraft and their infrastructure (e.g., radar modernization or replacement). Sampigethaya et al. [34] highlight the main features of, what they call, the e-enabled aircraft, which consists of the integration of advanced sensing, computing, networks, and onboard software modules. Because of the higher dependence of flight on data communications, several cyber-threats have emerged. In particular, data links can be subject malicious disruption and misuse that may cause leakage on sensitive information or even disastrous collisions. The authors focus ADS-B and IP ATM (Internet-protocol-based aeronautical telecommunication network) and they review their vulnerabilities and ongoing work on security enhancement. In particular, the automatic-dependent surveillance-broadcast (ADS-B) protocol, which is a satellite-based successor of the radar technology, has been implemented in most aircraft because it enables accurate tracking of an aircraft by using an onboard GPS receiver. This in turn broadcasts that position to the ground station and other aircraft; however, it has been reported that ADS-B is vulnerable to cyberattacks since security was not considered in its design. Strohmeier et al. [35] review several vulnerabilities of the use of insecure RF communications. The possible attacks can be as simple as eavesdropping to more elaborated as false data injection. The authors survey some outlining solutions specifically for ADS-B focused on authentication and location verification, as well as other methods intended for other type of wireless networks that can be applied to ADS-B, such as cryptography and fingerprinting.

Other CPS domains

There are other surveys that focus on CPS security in a crosscutting way, combining several domains. For example, depending on the adversary capacities, different elements can be targeted. According to [36], it is possible to divide all elements in a CPS into three categories:

- Cyber: elements that do not have direct contact with the physical world.
- Physical: all the elements that are merely physical and do not have a direct relation with the cyber-elements.
- Cyber–physical: all the devices that link the physical and the cyber world (e.g.,sensors and actuator with software or communication capabilities).

Wang et al. [37] focus their attention on state estimation and control design when the control system is under attack. They address three different types of attacks: DoS, replay attacks, and deception attacks. One of the differences with other works, is the analysis of control and estimation under resource constraints. The authors point out the importance of taking into account constraints caused by the physical process such as energy constraints, timing constraints due to the limited processing runtime of

CPUs, and communication network constraints that tackle how control performance is affected by the quality of communications. Even though very important points are highlighted, there is no concise study of works that address both cyberattacks with system constraints. As a matter of fact, we can argue that very few works in cyber-security of control systems take into account limitations imposed by the control process or the communication infrastructure.

Another perspective to tackle security issues in CPS was studied by Nguyen et al. [38], where it was shown how software models can help in the design and verification of CPS. Since the level of abstraction is higher than code-level, model-based strategies bring several benefits. For instance, it is possible to consider security concerns in early phases of the design process, and verify and validate methods and tools to address those issues. The authors developed a systematic mapping study that revealed various trends on model-based security analysis. For instance, there has been an increasing interest on model-based security to analyze vulnerabilities and threats in the past two years, but there is lack of research focusing on mitigating the vulnerabilities. Also, it has been shown that more than 90% of the research in model-based security is developed in academia and most of them focus on smart grids, i.e., about 44%.

Lun et al. [39] provide a quantitatively analytical survey that selected 118 research papers on CPS security. These aspects were covered by answering three fundamental questions about publication trends, focus on existing research, and the strategies used to validate the mechanisms. The paper analyzes how the publications were distributed among journals, conferences, workshops, book chapters, and institutions. The focus areas addressed in this survey reflected a particular aspect of the domain-like application, principle of security considered, system models, components, noise models, anomaly detection, communication, and the various attacks the research thwarted. The mechanisms also form a focus area of research and the validation of these mechanisms form the third part of the paper. The strategies were broadly divided into simulation-based, testbed-based, and real-world data based. The authors also look into the models developed for the system by the attacker and the system engineer. The work is extremely well researched, broad, and quantifiable aiming for a crisp understanding of the readers.

Han et al. [40] and Mitchell et al. [41] focus exclusively on the topic of intrusion detection systems for CPS. The first paper states that future CPSs will be able to self-maintain, self-repair, and self-upgrade themselves and for that self-detection of intrusion is now a forefront research topic. First, the authors explain the background of external and internal vulnerabilities, which the attackers tap, and the detection techniques are explained. The available detection techniques could be broadly classified into signature based, anomaly-based, and stateful protocol analysis-based mechanisms. Developing a generalized framework, the authors propose five necessary characteristics of intrusion detection in CPS:

- they should be able to function in a distributed topology,
- should provide runtime data,
- should be able to thwart both unknown and known attacks,
- should be system fault tolerant, and
- should not hamper privacy.

Mitchell et al. [41] propose a different classification of IDS, with two main groups: detection technique and audit material. The first includes knowledge-based detection, which consists of those techniques that have prior knowledge of bad behavior and are able to determine whether the system (or data) is misbehaving. Another detection class is behavior-based, which are useful for zero-day attacks since they do not look for something specific. On the other hand, audit material can be classified into host-based that focus on analyzing logs, and network-based audit, which monitors network activity to determine if a node is compromised (e.g., via deep packet inspection).

Detection and isolation mechanisms have been widely studied for different types of attacks and there is a vast literature that introduces strategies for CPSs. After detecting an attack or identifying vulnerabilities in a CPS, it is necessary to respond to those attacks such that their impact over the CPS is attenuated. Combita et al. [42] identify different trends on automatic attack detection and response:

- preventive and
- reactive responses.

First, preventive response takes place when vulnerabilities in a CPS have been identified. As a consequence, the system structure can be modified in order to increase the system resiliency to attacks. For instance, increasing the amount of sensors such that attacks are identified faster or adding extra layers of security to those elements that are more vulnerable to cyberattacks. On the other hand, reactive response consists on taking actions as soon as an alarm is raised. In this case, the control mechanism is modified online (in real-time) to counteract the attack. Since the adversary is intelligent and can also react to the defense action, the interaction between attacker and defender is typically modeled using game theory.

Table 1 Taxonomy of related work. Columns are organized by publication venue.

	Liu et al. [13]	Jawurek et al. [14]	He et al. [12]	Komninos et al. [15]	Tan et al. [16]	Cintuglu et al. [17]	Camara et al. [19]	Rushanan et al. [18]	Altaway et al. [20]	Krotofil et al. [22]	McLaughlin et al. [23]	Urbina et al. [24]	Stouffer et al. [21]	Sadeghi et al. [25]	Cheminod et al. [26]	Wells et al. [27]	Pan et al. [28]	Zeltmann et al. [29]	Sakiz et al. [31]	Zheng et al. [32]	Van et al. [30]	Combita et al. [42]	Humayed et al. [36]	Wang et al. [37]	Nguyen et al. [38]	Cortes et al. [43]	Han et al. [40]	Mitchell et al. [41]	Lun et al. [39]	Altawy et al. [33]	Strohmeier et al. [35]	Sampigethaya et al. [34]
Venue	Smart Grid						M. Dev.			ICS						Manuf.			ITS			Misc.										
Security																																
Cyber	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Physical	●	○	○	●	○	○	●	●	◐	●	●	○	●	○	○	◐	●	●	◐	○	●	○	●	○	○	○	○	○	○	●	○	○
Privacy	●	●	○	●	●	○	●	●	●	○	○	○	●	○	○	○	○	○	○	○	◐	○	●	○	○	●	○	○	○	●	○	●
Defenses																																
Prevention	●	●	●	●	●	○	●	●	●	○	●	◐	●	◐	●	○	◐	○	◐	○	○	●	●	○	○	●	○	○	●	●	●	●
Detection	●	●	●	●	●	◐	●	●	○	●	●	●	●	○	●	○	◐	◐	●	○	●	○	●	◐	○	○	●	●	●	◐	◐	◐
Response	○	○	●	○	●	○	○	○	○	●	○	○	●	○	◐	○	○	○	○	○	●	●	●	○	○	○	○	○	●	○	○	○

Legend: ● Feature considered by authors, ◐ Feature mentioned or briefly considered, ○ Feature not studied in the survey.

Privacy in abstract control theoretic systems is also growing in importance. Cortes et al. [43] focus on DP and how it has been extended to network control systems. They tackle different types of control theory problems. One of the problems is *consensus*, where a set of agents share information with an aggregator that returns the average of all the nodes. They propose a DP that ensures that inferences about the initial states cannot be obtained. Another classical control problem considered is filtering. They show how to obtain the estimation of an output signal using a Kalman filter that preserves DP, such that it is not possible to infer from the output, which input signals were used. The final problem they consider is distributed optimization. In this scenario, agents want to cooperate with each other to determine a global optimizer, but they do not want to reveal relevant information about themselves, as for instance, their private objective functions.

Recommendations and future research directions

We have reviewed several surveys from different application domains using our proposed taxonomy and we have summarized this in Table 1. We have identified various research trends in the literature as well as some fields where there is a lack of survey works.

From the 32 papers that we analyzed, only eight (25 %) described any form of active response to cyberattacks. Most solutions focus on prevention using cryptography and/or intrusion detection systems. Clearly, there are a variety of open problems on how to isolate and mitigate an attack when it is detected and we found only one survey that tackles this problem. It is necessary that the future work addresses the main benefit of intrusion detection, i.e., after detecting an attack, what should we do?

On the other hand, 40% of the papers addressed privacy issues. In particular, we can observe that privacy in medical devices and smart grids is a major concern, while for manufacturing or ICS, keeping information private does not seem to be relevant. This is because smart grids and medical devices deal directly with data from users, which contains sensitive information.

While we have summarized a survey focusing on DP when applied to control systems, there is no survey that tackles general privacy problems in control systems. In the past few years, there has been an increasing interest in strategies that preserve a certain level of privacy for control systems in addition to DP, such as homomorphic cryptography in feedback systems, and data minimization by changing sampling period. ■

Acknowledgments

This work is supported by NSF CNS-1547502, CNS-1553683, CNS-1111529, CNS-1228198, CICI-1547324, by ONR N000141512182, and by NIST 70NANB16H019.

References

[1] F. Mueller, “Challenges for cyber-physical systems: Security, timing analysis and soft error protection,” in *Proc. High-Confidence Softw. Platforms Cyber-Physical Syst. (HCSP-CPS) Workshop, Alexandria, VA, USA,* 2006, p. 4.

[2] M. Sun et al., “Addressing safety and security contradictions in cyber-physical systems,” in *Proc. 1st Workshop Future Directions Cyber-Physical Syst. Secur. (CPSSW09),* 2009.

[3] E. A. Lee, “Cyber-physical systems—Are computing foundations adequate?” in *Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, vol. 2, Austin, TX, USA 2006.

[4] M. Anand et al., “Security challenges in next generation cyber physical systems,” in *Proc. Beyond SCADA: Networked Embedded Control for Cyber Physical Systems*, vol. 41, 2006, pp. 1–4.

[5] A. A. Cardenas, S. Amin, and S. Sastry, “Secure control: Towards survivable cyber-physical systems,” in *Proc. IEEE 28th Int. Conf.,* 2008, pp. 495–500.

[6] H. Tang and B. M. McMillin, “Security property violation in cps through timing,” in *Proc. IEEE 28th Int. Conf.,* IEEE, 2008, pp. 519–524.

[7] C. Neuman, “Challenges in security for cyber-physical systems,” in *DHS Workshop on Future Directions in Cyber-Physical Systems Security*, CPS-VO, 2009, pp. 22–24.

[8] A. A. Cardenas, S. Amin, and S. Sastry, “Research challenges for the security of control systems,” in *Proc. 3rd Conf. Hot Topics in Security,* USENIX Assosciation, 2008, pp. 1–6.

[9] A. Cardenas et al., “Challenges for securing cyber physical systems,” in *Proc. Workshop Future Directions Cyber-Physical Syst. Secur.*, 2009, p. 5.

[10] P. Oman, E. Schweitzer, and D. Frincke, “Concerns about intrusions into remotely accessible substation controllers and scada systems,” in *Proc. 27th Annu. Western Protective Relay Conf.*, 2000, vol. 160.

[11] K.-D. Kim and P. R. Kumar, “Cyberphysical systems: a perspective at the centennial,” *Proc. IEEE*, vol. 100, pp. 1287–1308, 2012.

[12] H. He and J. Yan, “Cyber-physical attacks and defences in the smart grid: A survey,” *IET Cyber-Physical Syst. Theory Appl.*, vol. 1, no. 1, pp. 13–27, 2016.

[13] J. Liu et al., ”Cyber security and privacy issues in smart grids,” *IEEE Commun. Surveys Tuts.,* vol. 14, no. 4, pp. 981–997, 2012.

[14] M. Jawurek, F. Kerschbaum, and G. Danezis, “SoK: Privacy technologies for smart grids—A survey of options,” Microsoft Res., Cambridge, U.K., 2012.

[15] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in smart grid and smart home security: Issues, challenges and countermeasures,” *IEEE Commun. Surveys Tuts.,* vol. 16, no. 4, pp. 1933–1954, 2014.

[16] S. Tan et al., “Survey of security advances in smart grid: A data driven approach,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 397–422, 2017.

[17] M. H. Cintuglu et al., “A survey on smart grid cyber-physical system testbeds,” *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 2017.

[18] M. Rushanan et al., “SoK: Security and privacy in implantable medical devices and body area networks,” in *Proc. 2014 IEEE Symp. Secur. Privacy*, 2014, pp. 524–539.

[19] C. Camara, P. Peris-Lopez, and J. E. Tapiador, “Security and privacy issues in implantable medical devices: A comprehensive survey,” *J. Biomed. Inform.*, vol. 55, pp. 272–289, June 2015.

[20] R. AlTawy and A. M. Youssef, “Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices,” *IEEE Access*, vol. 4, pp. 959–979, 2016.

[21] V. P. M. A. K. Stouffer, S. Lightman, and A. Hahn, “NIST special publication 800-82 revision 2. initial public draft. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc),” NIST, May 2015.

[22] M. Krotofil and D. Gollmann, “Industrial control systems security: What is happening?” in *Proc. 11th IEEE Int. Conf. Informatics (INDIN),* Jul. 2013, pp. 670–675.

[23] S. McLaughlin et al., “The cybersecurity landscape in industrial control systems,” *Proc. IEEE,* vol. 104, no. 5, pp. 1039–1057, May 2016.

[24] D. I. Urbina et al., “Survey and new directions for physics-based attack detection in control systems,” NIST, Tech. Rep. NIST GCR 16-010, 2016.

[25] A. R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial Internet of Things,” in *Proc. 52nd ACM/EDAC/IEEE Design Automation Conf. (DAC),* Jun. 2015, pp. 1–6.

[26] M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” *IEEE Trans. Ind. Informat.,* vol. 9, no. 1, pp. 277–293, Feb 2013.

[27] L. J. Wells et al., “Cyber-physical security challenges in manufacturing systems,” *Manufacturing Lett.*, vol. 2, no. 2, pp. 74–77, 2014.

[28] Y. Pan et al., “Taxonomies for reasoning about cyber-physical attacks in iot-based manufacturing systems,” *Int. J. Interact. Multimed. Artif. Intell.,* vol. 4, no. Special Issue on Advances and Applications in the Internet of Things and Cloud Computing, 2017.

[29] S. E. Zeltmann et al., “Manufacturing and security challenges in 3D printing,” *Jom.*, vol. 68, no. 7, pp. 1872–1881, 2016.

[30] R. W. van der Heijden et al., “Survey on misbehavior detection in cooperative intelligent transportation systems,” *arXiv preprint arXiv:1610.06810,* 2016.

[31] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: Vanets and iov,” *Ad Hoc Netw.,* vol. 61, pp. 33–50, 2017.

[32] X. Zheng et al., “Investigating security vulnerabilities in modern vehicle systems,” in *Proc. Int. Conf. Applications and Techniques in Information Security,* Springer, 2016, pp. 29–40.

[33] R. Altawy and A. M. Youssef, “Security, privacy, and safety aspects of civilian drones: A survey,” *ACM Trans. Cyber-Physical Systems,* vol. 1, no. 2, p. 7, 2016.

[34] K. Sampigethaya et al., “Future e-enabled aircraft communications and security: The next 20 years and beyond,” *Proc. IEEE,* vol. 99, no. 11, pp. 2040–2055, 2011.

[35] M. Strohmeier, V. Lenders, and I. Martinovic, “On the security of the automatic dependent surveillance-broadcast protocol,” *IEEE Commun. Surveys Tuts.,* vol. 17, no. 2, pp. 1066–1087, 2015.

[36] A. Humayed et al., “Cyber-physical systems security—A survey,” *IEEE Internet Things J.,* to be published.

[37] D. Wang et al., “Recent advances on filtering and control for cyber-physical systems under security and resource constraints,” *J. Franklin Inst.,* vol. 353, no. 11, pp. 2451–2466, 2016.

[38] P. H. Nguyen, S. Ali, and T. Yue, “Model-based security engineering for cyber-physical systems: A systematic mapping study,” *Inf. Softw. Technol.*, vol. 83, pp. 116–135, 2017.

[39] Y. Z. Lun et al., “Cyber-physical systems security: A systematic mapping study,” *arXiv preprint arXiv:1605.09641,* 2016.

[40] S. Han et al., “Intrusion detection in cyber-physical systems: Techniques and challenges,” *IEEE Systems J.*, vol. 8, no. 4, pp. 1052–1062, Dec. 2014.

[41] R. Mitchell and I.-R. Chen, “A survey of intrusion detection techniques for cyber-physical systems,” *ACM Comput. Surveys (CSUR),* vol. 46, no. 4, p. 55, 2014.

[42] L. F. Combita et al., “Response and reconfiguration of cyber-physical control systems: A survey,” in *Proc. IEEE 2nd Colombian Conf. Automat. Control (CCAC)*, 2015, pp. 1–6.

[43] J. Cortes et al., “Differential privacy in control and network systems,” in *Proc. IEEE 55th Conf. Decision Control (CDC),* 2016, pp. 4252–4272.

Jairo Giraldo is a Research Associate with the Computer Science Department, University of Texas at Dallas. His research interests include security and privacy in control systems, multiagent systems, and distributed control of the smart grid. He has a PhD degree from the Universidad de los Andes, Bogota, Colombia, in 2015. He is a member of IEEE.

Esha Sarkar is a PhD student at the Tandon School of Engineering, NYU, New York, NY, USA. Her research interests include fingerprinting of industrial control systems components and security of industrial control systems.

Alvaro A. Cardenas is an Assistant Professor at the Department of Computer Science, University of Texas at Dallas. His research interests include cyber–physical systems and IoT security and privacy. He has a PhD degree from the University of Maryland. He is a member of IEEE.

Michail Maniatakos is an Assistant Professor at New York University Abu Dhabi and the Director of the Modern Microprocessor Architectures (MoMA) lab. His research interests include robust microprocessor architectures, privacy-preserving computation, as well as industrial control systems security. He has a PhD degree from Yale University. He is a member of IEEE. Contact him at michail.maniatakos@nyu.edu.

Murat Kantarcioglu is a Professor of Computer Science and the Director of the UTD Data Security and Privacy Lab at The University of Texas at Dallas. His research interests include creating technologies that can efficiently extract useful information from any data without sacrificing privacy or security. He has a PhD degree in Computer Science from Purdue University. He is a Senior Member of IEEE and ACM Distinguished Scientist.

■ Direct questions and comments about this article can be sent to Jairo Giraldo, University of Texas at Dallas; e-mail: jag140730@utdallas.edu.