Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations

Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum and Nasir Ghani

***Abstract*—The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted significant attention from the research community. To this end, several surveys were put forward addressing various IoT-centric topics including intrusion detection systems, threat modeling and emerging technologies. In contrast, in this work, we exclusively focus on the ever-evolving IoT vulnerabilities. In this context, we initially provide a comprehensive classification of state-of-the-art surveys, which address various dimensions of the IoT paradigm. This aims at facilitating IoT research endeavors by amalgamating, comparing and contrasting dispersed research contributions. Subsequently, we provide a unique taxonomy, which sheds the light on IoT vulnerabilities, their attack vectors, impacts on numerous security objectives, attacks which exploit such vulnerabilities, corresponding remediation methodologies and currently offered operational cyber security capabilities to infer and monitor such weaknesses. This aims at providing the reader with a multidimensional research perspective related to IoT vulnerabilities, including their technical details and consequences, which is postulated to be leveraged for remediation objectives. Additionally, motivated by the lack of empirical (and malicious) data related to the IoT paradigm, this work also presents a first look on Internet-scale IoT exploitations by drawing upon more than 30 GB of macroscopic, passive measurements' data. This aims at practically highlighting the severity of the IoT problem, while providing operational situational awareness capabilities, which undoubtedly would aid in the mitigation task, at large. Insightful findings, inferences and outcomes in addition to open challenges and research problems are also disclosed in this work, which we hope would pave the way for future research endeavors addressing theoretical and empirical aspects related to the imperative topic of IoT security.**

***Index Terms*—Internet of Things, IoT Vulnerabilities, IoT Data, IoT Security**

I. Introduction

THE CONCEPTION of the prominent Internet-of-Things (IoT) notion is envisioned to improve the quality of modern life. People-centric IoT solutions, for instance, significantly enhance daily routines of elderly and disabled people, thus increasing their autonomy and self-confidence [1]. Implantable and wearable IoT devices monitor and extract vital measurements to enable the real-time emergency alerting in order to increase patients' chances of survival [2]. This emerging technology is also being leveraged to reduce response times in reacting to abrupt health incidents such as the sudden infant death syndrome during sleep [3]. Moreover, advanced solutions for in-home rehabilitation strive to revolutionize physical therapy [4], while the Autism Glass [5] aims at aiding autistic children to recognize emotions of other people in real-time [6].

Safety-centric IoT solutions endeavor to minimize hazardous scenarios and situations. For example, the concept of connected vehicles prevents the driver from deviating from proper trajectory paths or bumping into objects. Further, such concept enables the automatic emergency notification of nearest road and medical assistance in case of accidents [7]. Additionally, autonomous, self-driving mining equipment keeps workers away from unsafe areas, while location and proximity IoT sensors allow miners to avoid dangerous situations [8]. Moreover, deployed IoT sensors at factories monitor environmental pollution and chemical leaks in water supply, while smoke, toxic gases and temperature sensors coupled with warning systems prevent ecological disasters [9]. Indeed, a number of case-studies have reported on the significant impact of IoT on natural resources' integrity and consumption. For instance, water pressure sensors in pipelines monitor flow activity and notify operators in case of a leak, while smart IoT devices and systems enable citizens to control water and energy consumption [9]. In fact, the IoT notion is introducing notable solutions for contemporary operations, well-being and safety. In this context, several ongoing IoT endeavors, such as those illustrated in Figure 1, promise to transform modern life and business models, hence improving efficiency, service level, and customer satisfaction.

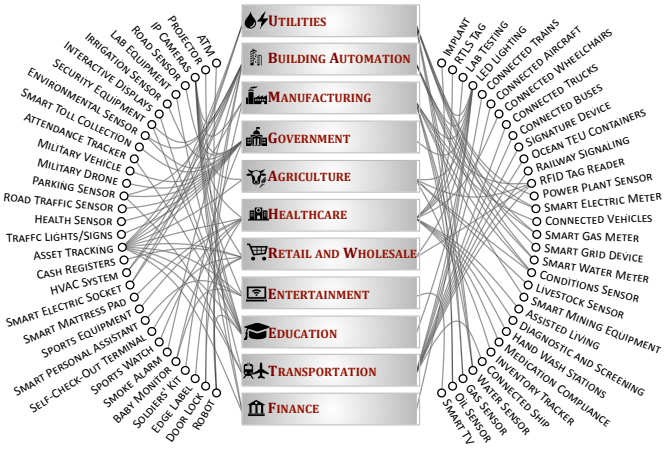


Fig. 1. IoT's penetration into contemporary life

The undeniable benefits proposed by the IoT paradigm,

NN and EBH are with FAU, USA; NG is with USF, USA; JC is with USC, USA; GK is with ETS, Canada

nevertheless, are coupled with serious security flaws. Profit-driven businesses and time-to-market along with the shortage of related legislation have stimulated manufacturers to overlook security considerations and to design potentially vulnerable IoT devices, opening the door for adversaries, which often exploit such devices with little or no effort. The negligence of a number of security considerations enables the exposure of sensitive information ranging from unprotected video streaming of baby monitors [10] to the uploading of unauthorized voice recordings, emails and passwords by Internet-connected IoT toys [11], [12]. Moreover, poorly designed devices allow the execution of arbitrary commands and re-programming of device firmware [13]. Indeed, given the Internet-wide deployment of IoT devices, such malicious manipulations have a profound impact on the security and the resiliency of the entire Internet. Among the many cases that recently attracted the public attention, the cyber attack launched by the IoT-specific malware Mirai [14] provides a clear example of the severity of the threat caused by instrumenting exploited IoT devices. In this case, the primary DNS provider in the US, Dyn, became the target of an orchestrated Denial of Service (DoS) attack, jeopardizing the profit and reputation of its clients. In fact, Dyn lost nearly 8% of its customers right after the mentioned attack [15]. Such and other security incidents impair the confidence in the IoT paradigm, hindering its widespread implementation in consumer markets and critical infrastructure. While the disclosure of private and confidential information coupled with the launch of debilitating DoS attacks cause various privacy violations and business disruptions, the most significant danger from exposed IoT devices remains the threat to people's lives and well-being. Security risks rendered by unauthorized access and reconfiguration of IoT medical devices, including implantable cardiac devices, have been already confirmed by the US Food and Drug Administration (FDA) [16]. Moreover, the hacking of traffic lights [17] and connected vehicles [18], [19] not only causes havoc and increases pollution, but also possesses the capability to cause injury and drastic accidents leading to fatalities. While benefits from using these IoT devices and corresponding technologies possibly outweigh the risks, undoubtedly, IoT security at large should be carefully and promptly addressed.

Several technical difficulties, including limited storage, power, and computational capabilities, challenge addressing various IoT security requirements. For instance, the simple issue of unauthorized access to IoT devices by applying default user credentials remains largerly unsolved. IoT manufacturers, though aware of this flaw, do not mitigate this risk by design, making consumers take responsibility of this technical task and to update their device firmware. Ironically, close to 48% of consumer individuals are unaware that their connected devices could be used to conduct a cyber attack, and around 40% of them never perform firmware updates. Such individuals argue that it is the responsibility of device manufacturers or software developers to remediate this security risk [20].

Although a plethora of security mechanisms currently exist aiming at enhancing IoT security, many research and operational problems remain unsolved, raising various concerns and thus undermining the confidence in the IoT paradigm. By thoroughly exploring the IoT security literature, one can identify several addressed topics related to IoT security (as elaborated in Section II). These include IoT-specific security mechanisms related to intrusion detection and threat modeling, as well as broader related topics in the context of emerging IoT protocols and technologies, to name a few.

To this end, we perceive a lack of an exhaustive, multidimensional approach, which specifically addresses the topic of IoT vulnerabilities. More imperatively, we pinpoint the scarcity of surveys, which attempt to (*i*) comprehend the impact of such ever-evolving vulnerabilities on various security objectives, (*ii*) identify the vectors which permit the rise of these vulnerabilities in the first place, (*iii*) characterize and analyze methods, techniques and approaches, which can be leveraged by an attacker to exploit such vulnerabilities, (*iv*) explore and assess possible remediation strategies, which aim at mitigating the identified vulnerabilities, and (*v*) shed the light on currently offered IoT cyber security situational awareness capabilities, which endeavor to identify, attribute, characterize and respond to such vulnerabilities or their possible exploitation attempts. Further, given that the problem of IoT security is still at its infancy due to the lack of IoT-relevant empirical data and IoT-specific attack signatures [21], we note the shortage of literature approaches, which can practically identify Internet-wide compromised IoT devices, in near real-time, and address this research development gap by exploring unique empirical data.

Specifically, in this survey, we uniquely approach IoT security by analyzing the aforementioned dimensions as they interrelay with certain identified IoT vulnerabilities. Specifically, we frame the contributions of this survey as follows:

- Amalgamating and classifying currently available IoT-relevant literature surveys to highlight research trends in this emerging field and to facilitate research initiation by new researchers through eliminating repetitive research efforts.
- Introducing a unique taxonomy by emphasizing and discussing IoT vulnerabilities in the context of various, previously unanalyzed dimensions through comparing, contrasting and analyzing near 100 research contributions. This aims at putting forward a new perspective related to IoT security, which we hope could be leveraged by readers from various backgrounds to address the issue of IoT security from their respective aspects of interest.
- Proposing a new, data-driven approach, which draws upon unique, previously untapped empirical data to generate Internet-scale notions of maliciousness related to the IoT paradigm. This aims at highlighting the severity of the IoT as deployed in consumer markets and critical infrastructure realms. The output of the approach in terms of cyber threat intelligence (i.e., near real-time inferred compromised IoT devices), malicious IoT data and IoT-specific attack signatures are made available to the research community at large (through an authenticated web service) to permit prompt IoT security remediation

and to widely promote data-driven research by employing IoT-relevant empirical data.
- Laying down a set of inferences, insights, challenges and open issues in the context of the discussed taxonomy and findings. Such outcomes facilitate future research endeavors in this imperative IoT security area.

The road-map of this survey is as follows. In the next section, we review and classify related surveys on various IoT-relevant topics and demonstrate the added value of the offered work. In Section III, we describe the survey's methodology, leading to the proposed taxonomy. In Section IV, we pinpoint the identified and extracted vulnerabilities, which form the basis of the taxonomy. In Section V, we present the proposed taxonomy, which emphasizes IoT vulnerabilities and elaborates on literature approaches, which address their various dimensions. The proposed data-driven approach to infer compromised IoT devices, and the threat and data sharing capabilities are elaborated in Section VI. In Section VII, we pinpoint several research challenges and topics that aim at paving the way for future work in the area of IoT security. Finally, in Section VIII, we discuss concluding remarks in the context of the presented taxonomy and empirical findings.

II. Related Surveys

The rapid growth and adoption of the IoT paradigm have induced an enormous attention from the research community. To highlight the latest findings and research directions in such an evolving field, a plethora of surveys were put forward to shed the light on recent IoT trends and challenges such as enabling technologies, application domains, and security methodologies. In this section, we scrutinize and classify a significantly representative number of such related surveys to outline their contributions in addition to clarifying how the presented work advances the state-of-the-art.

Atzori et al. [22] discussed two different perspectives of IoT research, namely, Internet-oriented or Things-oriented. The authors reviewed application domains, research challenges, and the most relevant enabling technologies with a focus on their role rather than their technical details. The authors further discussed the importance of security and indicated that numerous constraints such as limited energy and computation power of the IoT devices hinder the implementation of complex (and perhaps effective) security mechanisms.

In an alternate work, Gubbi et al. [23] elaborated on IoT-centric application domains and their corresponding challenges. The authors reviewed international activities in the field and presented a cloud-focused vision for the implementation of the IoT. The authors advocated that the application development platform dubbed as Aneka [24] allows the necessary flexibility to address the needs of different IoT sensors. The authors also pinpointed the importance of security in the cloud to fully realize the contemporary vision of the IoT paradigm.

Further, Xu et al. [25] presented an analysis of the core IoT enabling technologies and multi-layer architectures, along with an overview of industrial applications in the IoT context. The authors indicated that due to specific characteristics of IoT such as deployment, mobility and complexity, such paradigm suffers from severe security weaknesses, which cannot be tolerated in the realm of an industrial IoT.

Additionally, Al-Fuqaha et al. [26] reviewed IoT application domains, enabling technologies, their roles and the functionality of communication protocols adopted by the IoT. The authors distinguished between six core components that are crucial to delivering IoT services. These include identification, sensing, communication, computation, services, and semantics. The latter dimensions are presented in conjunction with their related standards, technologies and implementations. The authors analyzed numerous challenges and issues, including, security, privacy, performance, reliability, and management. To this end, they argued that the lack of common standards among IoT architectures render a core challenge hindering the protection of IoT from debilitating cyber threats.

A more recent study in the context of IoT is presented by Atzori et al. [27]. The authors synthesized the evolution of IoT and distinguished its three generations. According to the authors, these three epochs are respectively labeled as (i) tagged things, (ii) a web of things, and (iii) social IoT, cloud computing, and semantic data. The authors further debated that current technological advances on many aspects would indeed facilitate the realization of the next generation of IoT. By reviewing technologies attributed to each period, the authors presented certain desired transformational characteristics and applications.

Alternatively, Perera et al. [28] approached the IoT from a context-aware perspective. Aiming to identify available context-aware techniques and to analyze their applicability, the authors surveyed 50 diverse projects in this field and proposed a taxonomy of future models, techniques, functionality, and strategies. The authors noted that although security and privacy are addressed in the application layer, nevertheless, there still exists a need to pay close attention to such requirement in the middleware layer. The authors also shed the light on the security and privacy functionalities related to the surveyed projects.

While the aforementioned noteworthy research contributions specifically addressed the topics of IoT architectures and corresponding technologies, a number of other studies delved deep into its security aspects.

For instance, Sicari et al. [29] centered their work on the analysis of available solutions in the field of IoT security. Since IoT communication protocols and technologies differ from traditional IT realms, their security solutions ought to be different as well. The survey of a broad number of academic works led to the conclusion that despite numerous attempts in this field, many challenges and research questions remain open. In particular, the authors stressed the fact that a systematic and a unified vision to guarantee IoT security is still lacking. The authors then provided analysis of international projects in the field and noted that such endeavors are typically aimed at designing and implementing IoT-specific applications.

Further, Nia et al. [30] used the Cisco seven-level reference

TABLE I
A CLASSIFICATION OF REVIEWED SURVEYS ON IOT

Research area	[22]	[23]	[25]	[26]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	[34]	[35]	[36]	[37]	[38]
Protocols and Technologies	●	●	●	●	●	○	○	●	●	●	○	○	○	●	○	○
Application domains	●	●	●	●	●	○	○	○	○	○	○	○	○	●	○	○
Context awareness	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○
Legal frameworks	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○
Attacks	○	○	○	○	○	○	○	●	○	○	●	○	●	●	○	○
Access models	○	○	○	○	○	○	●	○	○	●	●	○	●	●	○	○
Security protocols	○	○	○	○	○	○	●	●	●	○	●	○	○	●	○	○
Intrusion detection techniques	○	○	○	○	○	○	○	○	○	○	○	○	●	○	●	●

Legend: ● area has been covered in the survey, ○ area has not been covered

model [39] to present various corresponding attack scenarios. The authors explored numerous IoT targeted attacks and pinpointed their possible mitigation approaches. The authors highlighted the importance of possessing a proactive approach for securing the IoT environment.

In contrast, Granjal et al. [31] analyzed how existing security mechanisms satisfy a number of IoT requirements and objectives. The authors centered their discussion around the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) concept [40], transportation, routing, and application layers. Among other limitations, they identified several constraints of key management mechanisms.

Very recently, Ouaddah et al. [32] presented a quantitative and a qualitative evaluation of available access control solutions for IoT. The authors highlighted how each solution achieved various security requirements, noting that the adoption of traditional approaches cannot be applied directly to IoT in many cases. The authors also declared that centralized and distributed approaches could complement each other when designing IoT-tailored access control.

Additionally, Roman et al. [33] centered their survey on numerous security features in addition to elaborating on the challenges of a distributed architecture to understand its viability for IoT. The authors concluded that while a distributed architecture might reduce the impact caused by a successful attack, it might also augment the number of attack vectors.

Alternatively, Weber and Studer in [34] discussed numerous IoT security threats and presented a review of available legal frameworks. The authors indicated that, based on available studies, the most significant progress in this area had been made within the European Union. Nevertheless, the authors revealed that IoT practical applications are still at their infancy.

Moreover, Zhang et al. [35] approached IoT security by analyzing reports related to IoT incidents. To this end, data mining techniques were leveraged to design a capability which crawled Internet publications, including academic research, news, blogs, and cyber reports. By correlating real IoT incidents with the available security solutions, the authors unveiled five weak areas in the context of IoT security, which require prompt attention. These areas include LAN and environmental mistrust, over-privileged applications, insufficient authentication and implementation flaws. The authors identified several domains that would require further exploration in order to advance the area of IoT security. The entire collection of accumulated and generated data and statistics are made available online by the authors.

In an alternative work, Alaba et al. [36] analyzed IoT security by reviewing existing security solutions and proposing a taxonomy of current threats and vulnerabilities in the context of various IoT deployment environments. Particularly, the taxonomy distinguished between four classes, including, application, architecture, communication, and data. The authors examined various threats and discussed them for each deployment domain. Moreover, a number of IoT challenges, which currently face the research community, were discussed. In this context, the authors argued that the heterogeneity of IoT devices along with their resource limitations define a serious issue, which hinders the scalability of possible security solutions.

In addition, Gendreau and Moorman [37] reviewed intrusion detection techniques proposed for the IoT. The survey validates the assertion that the concept of intrusion detection in the context of IoT remains at its infancy, despite numerous attempts. The authors also indicated that prevention of unauthorized access is a challenging goal due to the limited computational power of the IoT devices.

Zarpelão et al. [38] reached the same conclusion. The authors surveyed intrusion detection research efforts for IoT and classified them based on detection method, placement strategy, security threat, and validation strategy. The main observation of the authors is that intrusion detection schemes for IoT are still emerging. In particular, they noted that the proposed solutions do not cover a broad range of attacks and IoT technologies. Moreover, many of the currently offered schemes have never been thoroughly evaluated and validated.

To clarify the aforementioned works, we now present Table I, which summaries and classifies the contributions of the reviewed surveys. This aims at permitting readers from diverse backgrounds and new researchers in the IoT field to quickly and easily pinpoint already available contributions dealing with a common set of topics. It is evident that such efforts offer detailed studies related to IoT architectures and protocols, enabling technologies, threat modeling and remediation mechanisms. From such works, we noticed the lack of surveys, which specifically focus on the notion of IoT vulnerabilities. Particularly, we identify the research gap rendered by the nonexistence of a multidimensional perspective related

to such vulnerabilities; dealing with the comprehension of their impact on different security objectives, identification of ways attackers can exploit them to threaten the IoT paradigm and the resiliency of the entire Internet, elaboration of their corresponding remediation strategies and currently available cyber security awareness capabilities to monitor and infer such "in the wild" exploitations. Motivated by this, we offer such unique taxonomy in this work, which aims at shedding the light on IoT vulnerabilities and literature approaches which address their impact, consequences and operational capabilities. Further, stimulated by the lack of IoT-relevant empirical data and IoT-centric attack signatures [21], this work also alarms about the severity of the IoT paradigm by scrutinizing Internet-scale unsolicited data. To this end, the presented work offers a first-of-a-kind cyber-infrastructure, which aims at sharing the extracted cyber threat information and IoT-tailored empirical data with the research community at large.

III. Methodology

In this section, we briefly describe the employed systematic methodology, which was adopted to generate the offered taxonomy (of Section V). The results of this literature survey represent derived findings by thoroughly exploring nearly 100 IoT-specific research works extending from 2005 up to 2017, inclusively; the distribution of which is summarized in Figure 2. Please note that, for completeness purposes, Section VII will highlight on few emerging IoT security contributions which have appeared in 2018.

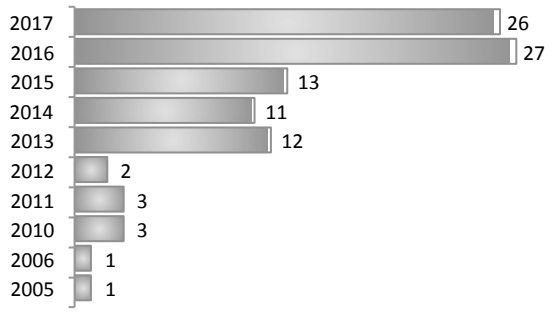


Fig. 2. Distribution of analyzed IoT research works by year

Initially, we meticulously investigated research contributions, which addressed various security aspects of the IoT paradigm. The aim was to extract relevant, common and impactful IoT vulnerabilities. We further confirmed their consistency with several public listings such as [41] and [42]. Subsequently, we attempted to categorize such vulnerabilities by the means they manifest; whether they are specifically related to IoT devices, affected by weaknesses in the networking subsystem (i.e., technologies, protocols, etc.) or they are caused by software/application issues. Moreover, we intended to establish a relationship between the inferred and extracted vulnerabilities and the core security objectives (i.e., confidentiality, integrity, availability) that they affect. We were further interested to synthesis how malicious actors would exploit such vulnerabilities. In this context, we selected research contributions in which the authors defined, analyzed, emulated or simulated an attack on the IoT. To identify possible and corresponding remediation techniques for each vulnerability, we extracted specific research works that proposed tailored solutions to address various aspects of IoT security. We categorized such approaches into several common classes. Finally, we intended to shed the light on methods, techniques and cyber security capabilities that would allow the proactive inference, characterization and attribution of malicious activities and emerging vulnerabilities, which might threaten the IoT paradigm. To this end, we explored research works which offered various mechanisms to (1) assess IoT devices and realms in order to discover their inherit or compound vulnerabilities, (2) monitor IoT-generated malicious activities, (3) infer Internet-scale IoT devices as deployed in consumer and Cyber-Physical Systems (CPS) sectors, and (4) identify attacks against IoT environments. Typical search engines and databases such as Google scholar, Scopus and Web of Science were employed to browse and identify relevant literature. IEEE Xplore and ACM digital libraries were the most explored indexing services to accomplish the literature search.

IV. IoT Vulnerabilities

Based on the previously outlined methodology, an exhaustive analysis of the research works related to the field of IoT security yielded nine (9) classes of IoT vulnerabilities. In this section, we describe such vulnerabilities, which aim at paving the way the elaboration of their multidimensional taxonomy as thoroughly described in Section V. For each class of vulnerabilities, we pinpoint a number of representative research works in their corresponding contexts. Please note that these works have been selected based upon their recency and/or significant number of citations. This aims at directing the reader, at an early stage of the paper, to relevant works related to the extracted vulnerabilities, noting that Section V will provide an exhaustive review addressing such vulnerabilities and their various dimensions.

Deficient physical security. The majority of IoT devices operate autonomously in unattended environments [43]. With little effort, an adversary might obtain unauthorized physical access to such devices and thus take control over them. Consequently, an attacker would cause physical damage to the devices, possibly unveiling employed cryptographic schemes, replicating their firmware using malicious node, or simply corrupting their control or cyber data. Representative research contributions in this context include [44]–[49].

Insufficient energy harvesting. IoT devices characteristically have limited energy and do not necessary possess the technology or mechanisms to renew it automatically. An attacker might drain the stored energy by generating flood of legitimate or corrupted messages, rendering the devices unavailable for valid processes or users. A few research works in this area include [50]–[53].

Inadequate authentication. The unique constraints within the context of the IoT paradigm such as limited energy and

computational power challenge the implementation of complex authentication mechanisms. To this end, an attacker might exploit ineffective authentication approaches to append spoofed malicious nodes or violate data integrity, thus intruding on IoT devices and network communications. Under such circumstances, the exchanged and employed authentication keys are also always at risk of being lost, destroyed, or corrupted. In such cases, when the keys are not being stored or transmitted securely, sophisticated (or otherwise effective) authentication algorithms become insufficient. Research contributions discussing such vulnerability include [54]–[59].

Improper encryption. Data protection is of paramount importance in IoT realms, especially those operating in critical CPS (i.e., power utilities, manufacturing plants, building automation, etc). It is known that encryption is an effective mechanism to store and transmit data in a way that only authorized users can utilize it. As the strength of cryptosystems depend on their designed algorithms, resource limitations of the IoT affects the robustness, efficiency and efficacy of such algorithms. To this end, an attacker might be able to circumvent the deployed encryption techniques to reveal sensitive information or control operations with limited, feasible effort. Representative research contributions in this context include [60]–[65].

Unnecessarily open ports. Various IoT devices have unnecessarily open ports while running vulnerable services, permitting an attacker to connect and exploit a plethora of vulnerabilities. Research works detailing such weaknesses include [66] and [61].

Insufficient access control. Strong credential management ought to protect IoT devices and data from unauthorized access. It is known that the majority of IoT devices in conjunction with their cloud management solutions do not force a password of sufficient complexity [67]. Moreover, after installation, numerous devices do not request to change the default user credentials. Further, most of the users have elevated permissions. Hence, an adversary could gain unauthorized access to the device, threaten data and the entire Internet. A number of research works dealing with this vulnerability include [65], [66], and [68]–[72].

Improper patch management capabilities. IoT operating systems and embedded firmware/software should be patched appropriately to continuously minimize attack vectors and augment their functional capabilities. Nevertheless, abundant cases report that many manufacturers either do not recurrently maintain security patches or do not have in place automated patch-update mechanisms. Moreover, even available update mechanisms lack integrity guarantees, rendering them susceptible to being maliciously modified and applied at large. Literature works such as [71], and [73]–[76] deal with this identified vulnerability.

Weak programming practices. Although strong programming practices and injecting security components might increase the resiliency of the IoT, many researchers have reported that countless firmware are released with known vulnerabilities such as backdoors, root users as prime access points, and the lack of Secure Socket Layer (SSL) usage. Hence, an adversary might easily exploit known security weaknesses to cause buffer overflows, information modifications, or gain unauthorized access to the device. Related research contributions include [59], [71], [74], and [77]–[79].

Insufficient audit mechanisms. A plethora of IoT devices lack thorough logging procedures, rendering it possible to conceal IoT-generated malicious activities. Research works related to this area include [45], [80], and [81].

V. Taxonomy of IoT Vulnerabilities: Layers, Impacts, Attacks, Remediation and Situational Awareness Capabilities

In this section, we elaborate on the proposed taxonomy by focusing on the previously extracted IoT vulnerabilities as they inter-relay with several dimensions.

A. Taxonomy Overview

Figure 3 illustrates the structure of the proposed taxonomy. The taxonomy frames and perceives IoT vulnerabilities within the scope of (*i*) Layers, (*ii*) Security impact, (*iii*) Attacks, (*iv*) Remediation methods, and (*v*) Situation awareness capabilities. In the sequel, we elaborate on such classes and their rationale.

Layers examines the influence of the components of the IoT realm on IoT vulnerabilities. This class is intuitively divided into three subclasses, namely, Device-based, Network-Based, and Software-based. Device-based addresses those vulnerabilities associated with the hardware elements of the IoT. In contrast, Network-based deals with IoT vulnerabilities caused by weaknesses originating from communication protocols, while Software-based consists of those vulnerabilities related to the firmware and/or the software of IoT devices.

Security Impact evaluates the vulnerabilities based on the threats they pose on core security objectives such as Confidentiality, Integrity, and Availability. IoT vulnerabilities which enable unauthorized access to IoT resources and data would be related to Confidentiality. Integrity issues consist of vulnerabilities which allow unauthorized modifications of IoT data and settings to go undetected. Vulnerabilities which hinder the continuous access to IoT would be related to Availability. It is clear that, given the cross-dependencies among the various security requirements, each identified IoT vulnerability might affect more than one security objective.

Attacks describe the security flaws categorized by the approach in which the inferred IoT vulnerabilities could be exploited. This class is divided into three subclasses, which elaborate on attacks against Confidentiality and Authentication, Data Integrity, and Availability.

Remediation is a classification of the available remediation techniques to mitigate the identified IoT vulnerabilities. This class is divided into Access and Authentication Controls, Software Assurance, and Security Protocols. Access and Authentication Controls include firewalls, algorithms and authentication schemes, biometric-based models, and context-aware permissions. Further, Software Assurance elaborates on the available capabilities to assert integrity constraints, while Security protocols deals with lightweight security schemes for proper remediation.

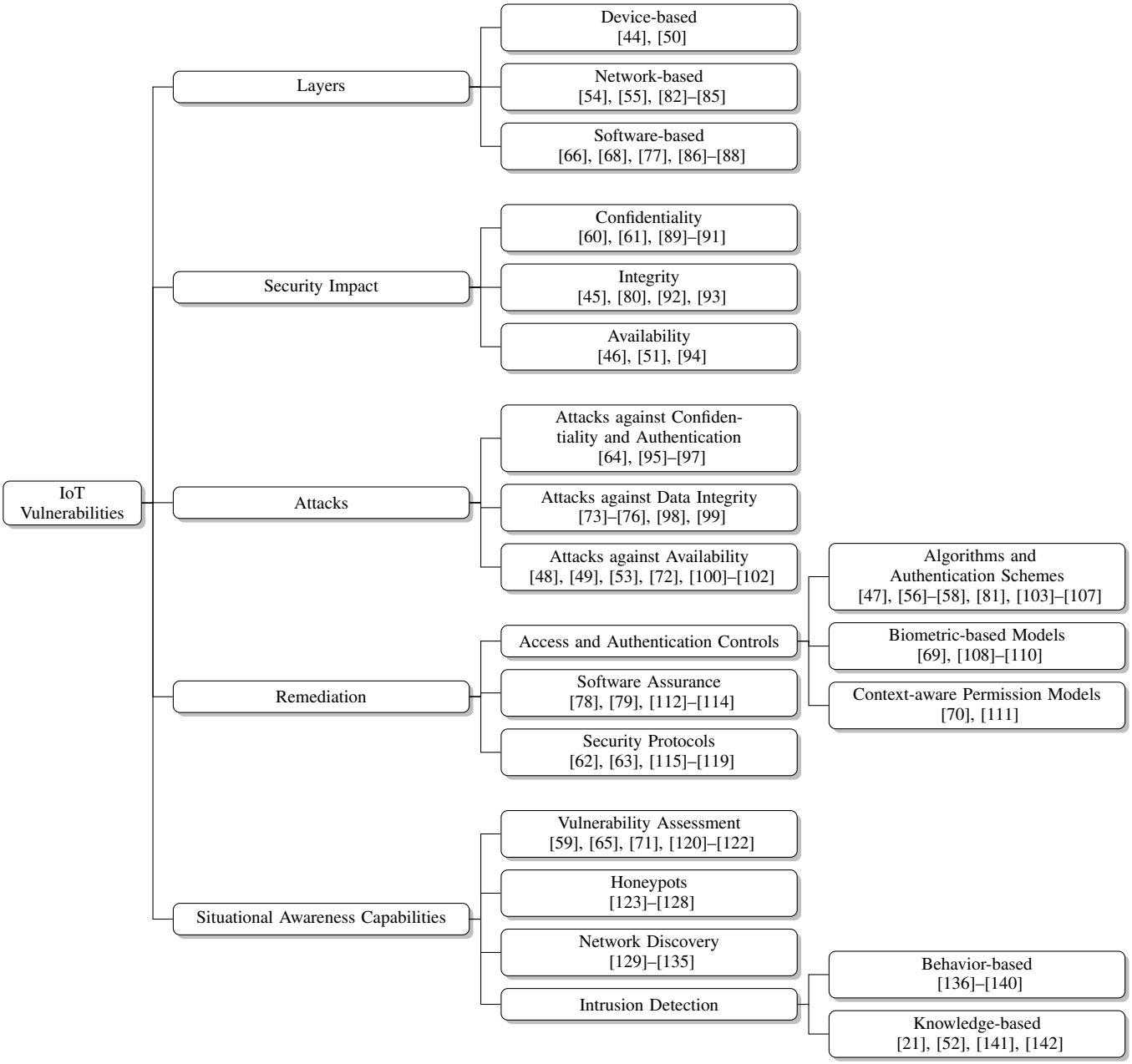


Fig. 3. A categorization of IoT vulnerabilities

Last but not least, **Situation Awareness Capabilities** categorizes available techniques for capturing accurate and sufficient information regarding generated malicious activities in the context of the IoT. This class elaborates on Vulnerability Assessment, Honeypots, Network Discovery, and Intrusion Detection. Vulnerability assessment deals with methods and techniques, which the research and cyber security operation communities can employ to assess IoT devices and their vulnerabilities (including 0-day vulnerabilities). Such approaches might include testbeds, attack simulation methods, and fuzzing techniques. Additionally, honeypots provide capabilities, which aim at capturing IoT-specific malicious activities for further investigation, while network discovery addresses methods for Internet-scale identification of vulnerable and compromised IoT devices. Finally, intrusion detection would detail detection methods applicable for inferring and characterizing IoT-centric malicious activities.

We now elaborate on the details of the aforementioned dimensions.

B. Layers

Broadly, IoT architectures and paradigms consist of three layers, namely, devices, network subsystems, and applications. IoT devices are typically responsible for sensing their environment by capturing cyber-physical data, while communication protocols handle two-way data transmission to the application layer, which in turns generates analytics and instruments the user interface. Indeed, security vulnerabilities exist at each tier

of such an IoT architecture, threatening core security goals by enabling various targeted attacks. In the sequel, in accordance with Figure 3, we examine the security of each layer and categorize their corresponding vulnerabilities.

1) Device-based Vulnerabilities: Since a large number of IoT devices operate in an unattended fashion with no or limited tamper resistance policies and methodologies, an attacker could take advantage of physical access to a device to cause damage, alter its services or obtain unlimited access to data stored on its memory. To this end, Wurm et al. [44] performed testing of consumer IoT devices and demonstrated how physical access to the hardware enables an adversary to modify boot parameters, extract the root password, and learn other sensitive/private information. Moreover, the authors executed a successful attempt to modify the ID of a smart meter, thus demonstrating the feasibility and practicality of energy theft. Further, the researchers performed several network attacks to retrieve the update file, taking advantage of the lack of encryption at the device level. The authors pinpointed various security enhancements in an attempt to mitigate some of the demonstrated threats such as blocking access to the Universal Asynchronous Receiver-Transmitter (UART), strengthening password-hashing algorithms, and encrypting the file system. In another work, Trappe et al. [50] highlighted the problem of IoT security in the context of the restricted power of the devices. The authors suggested energy harvesting, from both human-made and natural sources, as a suitable method to empower such devices to adopt complex security mechanisms. Nevertheless, it is known that the IoT paradigm faces various obstacles to harvest energy such as strict safety regulations and radio propagation limitations. The researchers suggested that utilizing the physical layer to support confidentiality could possibly be an opportunity for securing the IoT.

2) Network-based Vulnerabilities: A number of research efforts addressed IoT-specific vulnerabilities caused by network or protocol weaknesses. For instance, the ZigBee protocol [143], which is developed for low-rate/low-power wireless sensor and control networks, is built on top of IEEE 802.15.4 and offers a stack profile that defines the network, security, and application layers [144]. ZigBee devices establish secure communications by using symmetric keys while the level of sharing of such keys among nodes depends on the security mode [145]. In this context, Vidgren et al. [54] illustrated how an adversary could compromise ZigBee-enabled IoT devices. Although pre-installation of the keys onto each device for a certain security mode is possible, in reality, the keys are transmitted unencrypted, rendering it feasible to leak sensitive information and to allow an adversary to obtain control over the devices. The authors demonstrated several attacks which aim at either gaining control or conducting denial of service on IoT. The researchers suggested that applying the "High-Security" level along with pre-installation of the keys would support the protection of sensitive information, which is essential especially for safety-critical devices. In alternative work, Morgner et al. [55] investigated the security of ZigBee Light Link (ZLL)-based lighting systems. In particular, the authors examined a touchlink commissioning procedure, which is precisely developed to meet requirements of connected light systems. This procedure is responsible for initial device setting within the network and managing network features such as communication between a bulb and a remote control. The authors demonstrated several possible attacks and evaluated their impact by adopting a tailored testing framework. They further pinpointed numerous critical features which affect the security state. In particular, insufficiency of key management and physical protection of the IoT device were elaborated; the former suffers from two significant drawbacks related to sharing pre-defined keys among manufacturers and carrying out the fallback mechanisms. Such observations triggered the interest in the appropriateness of Key Management System (KMS) protocols in the context of the IoT. Accordingly, Roman et al. [82] distinguished four KMS classes: a key pool framework, a mathematical framework, a negotiation framework (i.e., pre-shared key), and a public key framework. By analyzing properties of classes above, the authors concluded that a plethora of traditional protocols is not appropriate due to the unique characteristics demanded from the IoT. Table II provides a summary of KMS implementation barriers in the context of the IoT. It is worthy to note that the authors analyzed a limited number of scenarios. Thus, further investigation in this area seems to be required.

TABLE II
SUMMARY OF KMS IMPLEMENTATION BARRIERS

Protocol framework	Implementation barriers
Key pool framework	Insufficient connectivity
Mathematical framework	Physical distribution of client and server nodes
Negotiation framework	Restricted power of nodes Different network residence of client and server nodes
Public key framework	Insufficient security for some cases

Likewise, Petroulakis et al. [83] experimentally investigated the correlation between energy consumption and security mechanisms such as encryption, channel assignment, and power control. Table III presents the summary of their findings, illustrating that the combination of security mechanisms significantly increases energy consumption. Given the energy limitations of IoT devices, applying such security methods could lead to energy depletion and hence, affects the availability of the device and its provided services. Although the experiment was restricted to only one IoT device, the XBee Pro, the authors highlighted that the approach could be generic enough to be used to test other devices as well. Auxiliary, Simplicio et al. [84] demonstrated

TABLE III
EFFECT OF VARIOUS SECURITY MECHANISMS ON ENERGY CONSUMPTION

Security mechanism	Effect on energy consumption
Encryption	$\Uparrow 15-30\%$
Channel assignment	$\Uparrow 10\%$
Power control	$\Uparrow 4\%$
All three above	$\Uparrow 230\%$

that many of the existing lightweight Authenticated Key Agreement (AKA) schemes suffer from key escrow, which is undesirable in large-scale environments. The authors evaluated escrow-free alternatives to estimate their suitability for IoT. The researchers implemented and benchmarked various schemes and concluded that the Strengthened MQV (SMQV) protocol [146] in combination with implicit certificates avoids transition costs of full-fledged PKI-based certificates, and is a more efficient alternative for other lightweight solutions. Another matter to be considered in the context of network-based weaknesses is related to port blocking policies. To this end, Czyz et al. [85] explored IoT connectivity over IPv4 and IPv6 and indicated several insightful findings. The authors noted that a significant number of IoT hosts are only reachable over IPv6 and that various IoT protocols are more accessible on IPv6 than on IPv4. In particular, the researchers pinpointed that the exposure of the Telnet service in 46% of the cases was greater over IPv6 than over IPv4. The authors further contacted IoT network operators to confirm the findings and unveiled that many default port openings are unintentional, which questions IoT security at large.

3) Software-based Vulnerabilities: Attackers can also gain remote access to smart IoT nodes by exploiting software vulnerabilities. Such a possibility prompted the research community to investigate this matter. For instance, Angrishi [66] explored IoT-centric malware, which recruited IoT devices into botnets for conducting DDoS attacks. The researcher uncovered that 90% of investigated malware injected default or weak user credentials, while only 10% exploited software-specific weaknesses. Indeed, over the years, the issue of insufficient authentication remains unaddressed, rendering contemporary IoT devices vulnerable to many attacks. We illustrate this issue throughout the past 10 years in Figure 4.

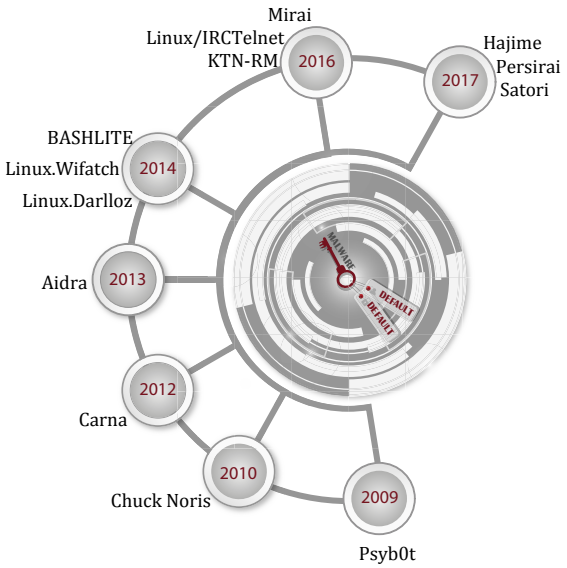


Fig. 4. Malware which exploit (IoT) default user credentials

A similar conclusion was reached by Markowsky et al. [68]. Referring to the Carna botnet [147], the author noted that it unveiled more than 1.6 million devices throughout the world that used default credentials. Auxiliary, Patton et al. [86] analyzed CPS. The authors employed the search engine Shodan [131] to index IoT devices that have been deployed in critical infrastructure. The researchers subsequently executed queries with default credentials to gain access to the devices. The authors' experimentation revealed that for various types of IoT, the magnitude of weak password protection varies from 0.44% (Niagara CPS Devices which are widely used in energy management systems) to 40% (traffic control cameras) of investigated devices. Although the conducted experiment was done on a small subset of CPS devices, the reported results, nevertheless, highlights the severity of the problem. Similarly, Cui and Stolfo [87] performed an Internet-scale active probing to uncover close to 540,000 embedded devices with default credentials in various realms such as enterprises, government organizations, Internet Service Providers (ISPs), educational institutions, and private networks. The authors revealed that during four months, nearly 97% of devices continued to provide access with default credentials. As a strategy to mitigate unauthorized access, the researchers argued that ISPs should be actively involved in the process of updating user credentials, since the majority of vulnerable devices are under their administration. Moreover, the authors noted that efficient host-based protection mechanism should be implemented. In the context of firmware vulnerabilities, Costin et al. [77] performed a large-scale static analysis of embedded firmware. The authors were able to recover plaintext passwords from almost 55% of retrieved password hashes. They also extracted 109 private RSA key from 428 firmware images and 56 self-signed SSL certificates out of 344 firmware images. By searching for such certificates in public ZMap datasets [148], the authors located about 35,000 active devices. Further, the researchers identified recently released firmware which contained kernel versions that are more than ten years old. The authors also unveiled that in more than 81% of the cases, web servers were configured to run as privileged users. The authors noted, however, that although the existence of these vulnerabilities seems to be tangible, nonetheless, without the proper hardware, it would be quite impossible to assess the firmware and its susceptibility to exploitations. Additionally, Konstantinou et al. [88] demonstrated how malicious firmware of power grids could corrupt control signals and cause a cascade of power outages. To simulate a firmware integrity attack and analyze its significance, the authors set up a testbed and conducted reverse engineering of the firmware. The researchers pinpointed that some vendors encode public firmware rendering it challenging to an adversary to reverse engineer it. Nevertheless, the authors successfully repackaged the firmware update file and simulated two types of attacks, unveiling that physical damage to the device and voltage instability are two possible drastic consequences.

To clarify our findings related to the aforementioned discussion, we present Table IV, which summarizes IoT vulnerabilities (of Section IV) based on their architectural

layers.

TABLE IV
IoT Vulnerabilities at Different Architectural layers

Layers	Vulnerabilities
Device-based	Deficient physical security Insufficient energy harvesting
Network-based	Inadequate authentication Improper encryption Unnecessarily open ports
Software-based	Insufficient access control Improper patch management capabilities Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.) Insufficient audit mechanism

Findings.
Indeed, by contrasting IoT architectural layers with the extracted vulnerabilities, we have identified several research gaps. We notice, for instance, that only limited number of IoT devices, their communication protocols, and applications have been assessed from a security point of view, while the research issue on how to extend this knowledge, taking into account IoT-specific traits such as manufacturers, deployment contexts, and types, remains completely obscure. Further, having myriads of authentication protocols, there is a lack of a systematic approach evaluating such protocols in various deployment scenarios. Moreover, while the issue of default credentials have received attention from the operational and research communities, the issue of dealing with significant number of deployed legacy IoT devices (containing hard-coded credentials) undoubtedly still demands additional investigation. Further, in the context of IoT vulnerable programming code, the factors which lead to such insecurities do not seem to have been thoroughly analyzed yet, hindering the realization of proper remediation techniques.

C. Security Impact

Given the extracted IoT vulnerabilities, we now elaborate on their impact on core security objectives, namely, confidentiality, integrity, and availability, consistent with the taxonomy of Figure 3.

1) Confidentiality: This security objective is designed to protect assets from unauthorized access and is typically enforced by strict access control, rigorous authentication procedures, and proper encryption. Nevertheless, the IoT paradigm demonstrates weaknesses in these areas resulting in information leakage. In this context, Copos et al. [89] illustrated how network traffic analysis of IoT thermostats and smoke detectors could be used to learn sensitive information. The authors demonstrated that this knowledge not only hinders the confidentiality of the inhabitants but could also potentially be utilized for unauthorized access to the facilities/homes. The authors captured network traffic generated by the IoT Nest Thermostat and Nest Protect devices, decrypted WPA encryption, and investigated connection logs. Further, they unveiled that although the traffic is encrypted, the devices still reveal destination IP addresses and communication packet sizes that could be successfully used to fingerprint occurring activities. As a simplistic countermeasure, the authors suggested generating same size and length packets and transmitting all the communications through a proxy server. Alternatively, Ronen and Shamir [60] analyzed the leakage of sensitive information such as WiFi passwords and encryption primitives by simulating attacks on smart IoT light bulbs. The researchers pinpointed that during the installation of the smart bulbs, WiFi passwords are transmitted unencrypted, rendering it possible to infer them for malicious purposes. To reduce the risk of information leakage, the authors recommended conducting penetration testing during the design phase, employing standardized and vetted protocols, and forcing authenticated API calls. Further, Wang et al. [90] demonstrated how the combination of motion signals leaked from wearable IoT devices and patterns in the English language allows an adversary to guess a typed text, including credentials. Similarly, the authors in [91] captured motion signals of wearable devices, extracted unique movement patterns, and estimated hand gestures during key entry (input) activities. This work thus demonstrated that it is feasible to reveal a secret PIN sequence of key-based security systems, which included ATM and electronic door entries. The authors also pinpointed that such type of analysis does not require any training or contextual information, making it quite simple for a malicious actor to learn sensitive information. The researchers noted that increasing robustness of the encryption scheme and injecting fabricated noise could possibly prevent such misdemeanors. Additionally, Sachidananda et al. [61] conducted penetration testing, fingerprinting, process enumeration, and vulnerability scanning of numerous consumer IoT devices. The authors' investigation unveiled that a large number of devices have unnecessarily open ports/services, which could be easily leveraged to leak confidential information related to operating systems, device types and transferred data.

2) Integrity: The integrity objective typically guarantees the detection of any unauthorized modifications and is routinely enforced by strict auditing of access control, rigorous hashing and encryption primitives, interface restrictions, input validations, and intrusion detection methods. However, various unique attributes of the IoT hinder the implementation of sufficient security mechanisms, causing numerous integrity violations against data and software. To this end, Ur et al. [45] investigated ownership rules, roles, and integrity monitoring capabilities of numerous types of home automation devices. The authors pinpointed various access control issues such as insufficiency of audit mechanisms and ability to evade the applied integrity rules. In particular, the researchers highlighted the inability to trace conducted activities and their sources. In addition, Ho et al. [80] investigated a number of integrity attacks such as state consistency events by

TABLE V
SECURITY IMPACT OF IOT VULNERABILITIES

Layers	Vulnerabilities	Security Impact			References
		Confidentiality	Integrity	Availability	
Device-based	Deficient physical security	○	●	●	[44]–[46], [51]
	Insufficient energy harvesting	○	○	●	[50], [51]
Network-based	Inadequate authentication	●	●	○	[54], [55], [80], [82]–[84], [89]
	Improper encryption	●	●	○	[60], [90]–[92]
	Unnecessarily open ports	●	○	●	[61], [85], [94]
Software-based	Insufficient access control	●	●	●	[45], [66], [68], [77], [86], [87], [92]–[94]
	Improper patch management capabilities	○	○	●	[46], [77], [88]
	Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.)	●	●	○	[77]
	Insufficient audit mechanism	○	●	○	[45], [80]

Legend: ● vulnerability has significant impact on particular security concept,
○ vulnerability does not have significant impact on a particular security concept

studying smart IoT lock systems. The authors demonstrated how network architectures, trust models, and reply activities could unlock the door, allowing unauthorized physical access. Moreover, the authors noted that most of the investigated devices do not provide access to integrity logging procedures, rendering it possible for tailored integrity violations to be executed without being noticed. In contrast, Ghena et al. [92] performed security evaluation of wireless traffic signals. The assessment was executed through attack simulations, aiming to exploit a remote access function of the controller. The authors noted that because of the lack of encryption along with the usage of default credentials, an adversary could gain control over the traffic cyber-infrastructure. To this end, an attacker could be able to change the timing of the traffic lights; altering minimum and maximum time for each state and switching or freezing the state of a particular traffic light. These attacks undeniably cause disruptions and safety degradations. The researchers, nevertheless, pinpointed that the Malfunction Management Unit (MMU) typically maintains safety by switching the controller to a known-safe mode in case of a detected integrity violation. The authors attested that, the employment of encryption on the wireless network, regularly updating device firmware, blocking unnecessary network traffic, and changing the default credentials on the operated devices would increase the security of the transport infrastructure. In an alternative work, Takeoglu et al. [93] conducted an experimental investigation of the security and privacy of a cloud-based wireless IP camera. The results demonstrated how elevated permissions of a user permitted root access to the file system, causing numerous integrity violations such as deleting or modifying files. The authors noted that auditing mechanisms and restricting administrator access would contribute to better device security, thus reducing integrity issues.

3) Availability: This security objective is designed to guarantee timely access to a plethora of resources (including data, applications and network infrastructure) and is often enforced by monitoring and adapting the handling capabilities of such assets, implementing redundancy mechanisms, maintaining backup systems and applying effective security policies and software (or firmware) update patches. Nevertheless, these mechanisms are not always adopted by the IoT. In this context, Costa et al. [51] discussed two groups of availability issues associated with wireless visual sensor networks. These conserns include hardware and coverage failures. While the first group deals with issues such as damage devices, energy depletion and nodes' disconnection, the second group refers to the quality of the information transmitted by the device. Further, Schuett et al. [46] demonstrated how firmware modifications could hamper the availability of IoT devices deployed in critical infrastructure. The authors repackaged firmware images, so they trigger a termination signal, ceasing the operation of the device or restricting the owners' access to such devices. The researchers conducted hardware analysis to identify the employed instructions used in the firmware images. To this end, they enumerated their sub-functions to perform tailored modifications, aiming at designing a number of attacks. The authors demonstrated the impact of remote termination commands, which as noted by the authors, could be relatively easily mitigated by updating the firmware. The authors concluded by stating that mapping firmware images to protected memory and digitally signing firmware updates could increase the efforts of an adversary, thus reducing the risk of such availability attacks. Moreover, recently, the U.S. Department of Homeland Security (DHS) had issued an alert [94] notifying IoT operators and users about the rise of permanent DoS attacks, which target devices with default credentials and open Telnet ports. In this sense, an attacker could disrupt device functions by corrupting its storage. DHS noted that mitigation strategies include changing the default credentials, disabling Telnet access and employing server clusters which are able to handle large network traffic.

Given the aforementioned information, which interplay IoT vulnerabilities with their impacted security objectives, we present Table V which summarizes IoT vulnerabilities in the context of their attack vectors and security objectives. Such summary would be of interest to readers that are aiming to comprehend what has been accomplished already to address such IoT vulnerabilities and would facilitate IoT research initiation in the highlighted areas.

Findings.
We observe the absence of studies which measure the effect of violations of various security objectives in different deployment domains. Indeed, a confidentiality breach in the context of light bulbs is not as critical as in the context of medical devices. Such intelligence would priotorize the remediation depending on the deployment domain. Further, while weak programming practices have a significant security impact, we notice the shortage of research work which systematically assess how such practices violate different security objectives in the context of IoT. Moreover, we infer the lack of studies analyzing the efficiency of IoT audit mechanisms. Indeed, exploring existing audit mechanisms along with assessing their robustness in the context of different IoT devices under various deployment environments would provide valuable insights and would enable the development of proper mitigation strategies.

D. Attacks

After elaborating on the relationships between IoT vulnerabilities, their attack vectors from an architectural perspective and their corresponding impacted security objectives, we now discuss literature-extracted IoT attacks, which tend to exploit such vulnerabilities, as illustrated in the taxonomy of Figure 3.

1) Attacks against Confidentiality and Authentication: The primary goal of this class of attack is to gain unauthorized access to IoT resources and data to conduct further malicious actions. This type of attack is often induced by executing brute force events, evesdropping IoT physical measurements, or faking devices identities.

Broadly, *dictionary attacks* aim at gaining access to IoT devices through executing variants of brute force events, leading to illicit modifications of settings or even full control of device functions. In this context, very recently, Antonakakis et al. [95] illustrated how a dictionary attack could compromise millions of Internet-connected devices and turn them into a malicious army to launch orchestrated attacks against core Internet services. The authors analyzed over 1,000 malware variants to document the evolution of the Mirai malware, learn its detection avoidance techniques and uncover its targets. By monitoring requests to a network telescope (i.e., a set of routable, allocated yet unused IP addresses) and employing filters to distinguish Mirai traffic, the authors identified 1.2 million Mirai infected IP addresses associated with various deployment environments and types of IoT devices. Figure 5 illustrates a summary of this attack. The infection mechanism was executed in various phases, including rapid scanning for target identification, brute-force logins for learning the device operating settings, and downloading architecture-specific malware for exploitation and usage. Further, *side-channel attacks* (i.e., power analysis) endeavor to recover devices cryptographic keys by leveraging existing correlations between

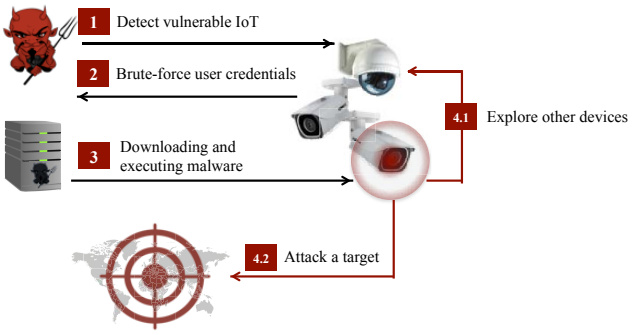


Fig. 5. Mirai attack process

physical measurements and the internal states of IoT devices [149]. This attack consists of two phases, namely, information acquisition and correlation analysis. In the former step, an adversary observes the associations between a number of physical attributes such as power consumption and electromagnetic emission for different inputs parameters. Such correlations are typically referred to as side-channel information and could be exploited for malicious purposes. To evaluate the method of physically measuring power, O'Flynn and Chen [96] inserted a resistive shunt into the power supply of the targeted IoT wireless node, which uses the IEEE802.15.4 protocol. The captured power traces were then used for detecting the location of software encryption and for recovering the respective encryption key. The authors noted that this attack is quite hard to detect because the captured node is absent in the network for only a short time. Similarly, Biryukov et al. [64] illustrated a vulnerability related to the Advanced Encryption Standard (AES), which is widely used in the IEEE802.15.4 protocol as a building block for encryption, and authentication messages in IoT communications. To assess the resiliency of AES, the authors employed an algorithm for symbolic processing of the cipher state and described an optimal algorithm that recovers the master key. In particular, the researchers showed how a protected implementation of AES based on S-box and T-table strategies could be broken even when an adversary controls a limited amount of information. Additionally, an attacker can manipulate the identity of compromised devices aiming to maliciously influence the network. To this end, Rajan et al. [97] modeled *sybil attacks* in IoT context and evaluated the impact on the network performance. The authors defined two types of sybil identities and labeled them as stolen and fabricated identities. The researchers implemented the malicious behavior of nodes with such fake identities. In particular, they evaluated the performance of the network when packets are dropped or selective forwarded. Based on behavioral profiling of IoT devices, the authors proposed a detection technique rooted in trust relationship between nodes.

Examples of real attacks against confidentiality.
2016: Mirai botnet [95]
BrickerBot [72]
IoT toys leaking millions of voice messages [12]

2) Attacks against Data Integrity: The sabotage of IoT data is also quite damaging to the IoT paradigm. Attacks against integrity are prompted by injection of false data or modification of device firmware.

False Data Injection (FDI) attacks fuse legitimate or corrupted input towards IoT sensors to cause various integrity violations. For instance, lunching such attacks could mislead the state estimation process of a IoT device, causing dramatic economic impact or even loss of human life [150]. In this context, Liu et al. [98] simulated data injection attacks on power utilities. The authors investigated the scenarios in which an attacker aims to inject random measurements to IoT sensors. In particular, this work pinpointed the severity of such attack class by revealing that an attacker would only need to compromise 1% of the IoT meters in the system to severely threaten the resiliency of the entire power grid. The authors pinpointed several requirements for conducting such an attack, including, a thorough knowledge of the systems' dynamics, and the ability to manipulate the measurements before they are used for state estimation. Although these requirements seem to be challenging to achieve, the authors report several cases which prove that that such requirements do not prevent the accomplishment of the attack, leading to catastrophic negative impacts. In a closely related work, Liu et al. [99] proposed and validated numerous strategies which allows the proper execution of FDI attacks, with limited network information while maintaining stealthiness. To this end, the authors examined network characteristics of an IoT-empowered power grid and built a linear programming model that minimized the number of required measurements. The researchers conducted various experiments rooted in emulation studies to validate their model. Another category of attacks, namely, *firmware modification*, is rendered by malicious alteration of the firmware, which induces a functional disruption of the targeted device. Figure 6 depicts the attacks' three-step procedure; reconnaissance, reverse engineering, and repackaging and uploading. Given the significant negative impact of

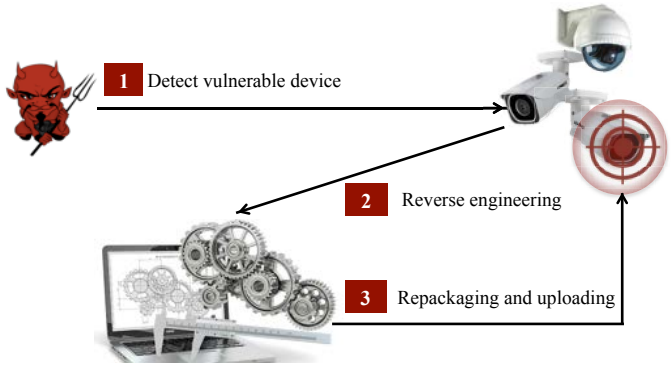


Fig. 6. Stages of firmware modification attack

such attacks on the IoT paradigm, the research community has been quite active in exploring related issues and solutions. For instance, Basnight et al. [73] illustrated how firmware could be maliciously modified and uploaded to an Allen-Bradley ControlLogix which is Programmable Logic Controller (PLC). By conducting reverse engineering, the authors were able to initially learn the functionality of the firmware update mechanism to subsequently modify the configuration file, rendering it possible to inject malicious code into a firmware update. The authors pinpointed that the resource limitation of PLC devices hinders the implementation of a robust algorithm that would attempt to verify data integrity. In alternative work, Cui et al. [74] analyzed a large number of LaserJet printer firmware and executed firmware modification attacks by reverse engineering a number of hardware components. The authors identified over 90,000 unique, vulnerable printers that are publicly accessible over the Internet. The authors alarmed that such devices were located in governmental and military organizations, educational institutions, ISPs, and private corporations. The researchers unveiled that many firmware are released with known vulnerabilities and about 80% of firmware images rely on third-party libraries that contain known vulnerabilities. Moreover, the authors noted that update mechanisms typically do not require authentication, facilitating a firmware modification attack. In addition, the researchers stated that the rate of current IoT firmware patches is significantly low, noting that 25% of the patched printers do not address the default user credentials' issue. The authors also pinpointed the lack of IoT host-based defense/integrity mechanisms, which can prevent firmware modification attacks.

Meanwhile, Konstantinou and Maniatakos [75] defined firmware modifications as a new class of cyber-physical attacks against the IoT paradigm (within the context of a smart grid) and illustrated how an adversary could disrupt an operation of circuit breakers by injecting malicious tripping commands to the relay controllers. By conducting reverse engineering, the authors determined the details of the operating system, extracted the functionality of various critical routines, and located key structures to be modified. The analysis of the obtained files exposed passwords of a large number of deployed IoT devices and disclosed the encryption key. The authors further uploaded a modified firmware to an embedded device and revealed that the update validation employed a simplistic checksum which can be easily circumvented. The researchers analyzed different attack scenarios and concluded that maliciously modified IoT firmware could indeed cause a cascade of power outages within the context of the smart grid. Further, Bencsath et al. [76] introduced a general framework for Cross-Channel Scripting (CCS) attacks targeting IoT embedded software, proved its feasibility by implementing it on Planex wireless routers, and demonstrated how this vulnerability could create an entry point to install malicious code to turn the devices into bots in coordinated botnets. The framework consisted of three stages, namely, vulnerability exploitation, platform identification, and malicious firmware updates. Through this, the authors highlighted the feasibility of CCS attacks targeting the IoT paradigm.

Example of real attack against integrity.

2015: Baby monitor "converses" to children [151]

3) Atacks against Availability: The primary goal of Denial of Service (DoS) attacks against IoT is to prevent the legitimate users' timely access to IoT resources (i.e., data and services). This type of attack is often induced by revoking device from the network or draining IoT resources until their full exhaustion.

As noted earlier, IoT devices typically reside in unattended and physically unprotected realms. In this context, an adversary could capture, alter or destroy a device to retrieve stored sensitive information, including secret keys. We label this group of attacks, following literature terminology, as *device capture*. In this context, Smache et al. [48] formalized a model for node capturing attacks, given a secure IoT WSN. The authors defined the attack as consisting of a combination of passive, active, and physical attack events that is executed by an intelligent adversary. Figure 7 illustrates such misdemeanor by highlighting its three phases.

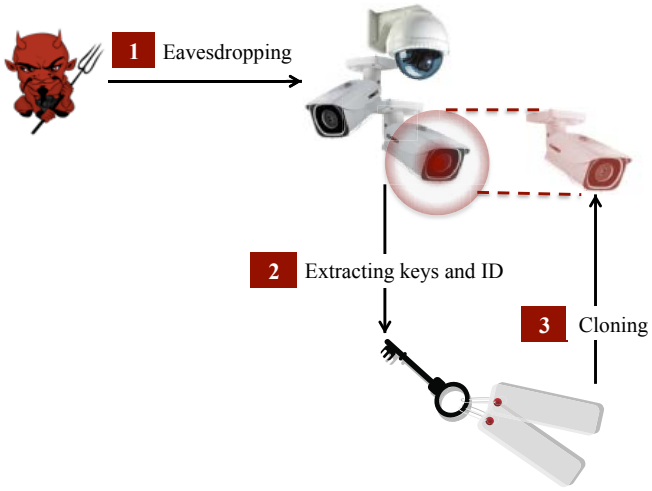


Fig. 7. Node capturing attack phases

This attack includes (*i*) eavesdropping and selecting victim nodes, during which an attacker investigates the network to identify a suitable target, (*ii*) extracting sensitive information, and (*iii*) cloning a node. The authors also assessed the capability of an intrusion detection system in detecting such malicious behaviors by monitoring incoming network packets as well as monitoring device memory. Further, Zhao [49] analyzed the resiliency to node-capture attacks of random key predistribution IoT schemes, namely, the q-composite extension of the scheme proposed by Eschenauer and Gligor in [152], and provided several design guidelines for secure sensor networks by employing such scheme. In auxiliary work, Bonaci et al. [100] proposed an adversary model of node capture attacks. The authors formulated the network security issue into a control theoretic problem set. By applying this framework to an IoT network, the authors simulated and analyzed the network performance and stability under physical intervention. They also proposed (*i*) an algorithm for identifying corrupted nodes, (*ii*) node revocation methods and (*iii*) key refreshment techniques for node validation. Although this model does not protect IoT node from being captured by an adversary, it allows securing network from the consequences of such an attack.

Additionally, Radware [72] recently witnessed and alarmed about nearly 2,000 attempts to compromise IoT honeypots. Further investigation of such attacks unveiled that it was designed to damage the devices, so that the latter become inoperable. A study of this attack, which the authors labeled as Permanent Denial of Service (PDoS), revealed that an adversary exploited default credentials and performed several Linux commands that led to storage corruptions, Internet connectivity disruptions, and wiping of all files on the devices. IoT devices with open Telnet ports were identified as the primary target of such the attack.

Further, *sinkhole attacks* modify the network topology and degrade IoT network performance. To this end, the attacker empowers the malicious nodes with the ability to advertise artificial routing paths to incude as many nodes as possible in order to obligee them to send packets thoughs such bogus paths. The malicious node than either drop or selective forwards the information. By simulating a sinkhole attack in an 6LoWPAN IoT network, Wallgren et al. [101] observed huge traffic passing through the attacker nodes. It is worthy to pinpoint that coupled with other attacks, sinkhole attacks would cause more significant harm for routing protocols.

Also known as vampire attacks, the *batarry draining attacks* are broadly defined by Vasserman and Hopper [53] as the transmission of a message (or a datagram) in a way which demands significantly more energy from the network and its nodes to be employed and acted upon in contrast with typical messages. The authors in [53] evaluated two subtypes of such attacks, namely, *carousel* and *stretch attacks*. On one hand, carousel attacks permit an adversary to send messages as a series of loops such that the same node appears in the route several times. On the other hand, stretch attacks allow malicious nodes to artificially construct long routes so that the packets traverse through a larger, inversely optimal number of IoT nodes. Conducted simulations illustrated that a given network under such attacks increase its energy consumption up to 1,000% depending on the location of the adversary. The authors pinpointed that the combination of these attacks could tremendously increases the level of consumed power, and thus, drain energy quite promptly. The researchers attested that carousel attacks could be prevented by validating source routes for loops and discarding nodes which have initially sent such messages. In case of stateful protocols, which are typically network topology-aware, the attacks mentioned here become relatively limited.

Besides, Pielli et al. [102] investigated *jamming attacks*, which aim at disrupting IoT network communications and reducing the lifetime of energy-constrained nodes by creating interference and causing packet collisions. By leveraging a game theoretic approach, the authors studied jamming attack scenarios in the context of various strategies. The results demonstrated a trade-off between communication reliability and device lifetime. Nevertheless, jamming is a severe problem in the IoT context, especially that legacy nodes are inherently vulnerable to such attacks.

TABLE VI
ATTACKS TARGETING IOT PARADIGM

	Dictionary Attack	Side-Channel Attack	Sybil Attack	False Data Injection	Firmaware Modification Attack	Device Capture	Sinkhole Attack	Battery Draining Attack	Jumming Attack	References
Deficient physical security	○	●	○	○	●	●	○	○	○	[48], [49], [64], [73]–[76], [96], [100]
Insufficient energy harvesting	○	○	○	○	○	○	●	●	●	[53], [101], [102]
Insufficient authentication	●	○	●	●	○	●	●	○	○	[48], [49], [95], [97]–[101]
Improper encryption	○	●	○	○	○	○	○	○	○	[64], [96]
Unnecessarily open ports	●	○	○	○	○	○	○	○	○	[72]
Insufficient access control	●	○	○	○	○	○	○	○	○	[72], [95]
Improper software update capabilities	○	○	○	○	●	○	○	○	○	[73]–[76]
Weak programming practice (e.g. root user, lack of SSL, plain text password, back-door, ect.)	●	○	○	●	●	○	○	○	○	[73]–[76], [95], [98], [99]
Insufficient audit mechanism	●	○	○	●	●	●	○	○	○	[48], [49], [73]–[76], [95], [98]–[100]

Legend: ● an attack leverages particular vulnerability, ○ an attack does not leverages particular vulnerability

Example of real attack against availability.

2016: Cold Finland [153]

Given the aforementioned information, which elaborates on literature-extracted attacks that could possibly exploit the IoT vulnerabilities as pinpointed in Section IV, we now present Table VI which summarizes the relationship between the detailed attacks and targeted vulnerabilities.

Findings.

We note the shortage of research works devoted to studying IoT-specific attacks, given that many contributions have been dedicated to addressing the issue of threat classifications in WSN. We also observe that the same attacks could exploit various vulnerabilities of IoT paradigm, rather than targeting only one of them. In this context, dictionary, firmware modification, and device capturing attacks render the most severe damage. Further, we notice the deficiency of endeavors that aim at generating tangible notions of IoT maliciousness, especially that intrusion detection techniques would highly benefit from such knowledge.

E. Remediation

Coherent with the taxonomy of Figure 3, IoT vulnerabilities can further be classified by their corresponding remediation strategies. We distinguish three classes of such strategies, namely, access and authentication controls, software assurance, and security protocols. We elaborate on their details in the sequel.

1) Access and Authentication Controls: To address a number of IoT vulnerabilities, authentication and authorization techniques are typically adopted. Nevertheless, given the low computational power of IoT devices, such mechanisms continue to be challenged in such contexts. However, there has been some recent attempts to address this. To this end, Hafeez et al. [57] proposed Securebox, a platform for securing IoT networks. The platform provides a number of features including device isolation in addition to vetting device to device communications. The platform intercepts any connection request from a connected IoT device to a remote destination and subsequently verifies if various security policies match the requested connection. When a suspicious activity is detected, the platform quarantines such attempt and alarms the user in an attempt to provide cyber security awareness. Nonetheless, the proposed solution is still theoretical and indeed requires thorough empirical experimentation. In contrast, Qabulio et al. [47] proposed a generic framework for securing mobile wireless IoT networks against physical attacks. In particular, the authors leveraged messages directed towards the base station to infer spoofed/cloned nodes. The authors proposed techniques by exploiting time differences in inter-arrival rate to detect spoofed packets. The proposed framework was successfully tested by employing the Contiki OS [154] and the COOJA simulator [155]. In alternative work, Hei et al. [103] proposed a lightweight security scheme to defend against resource depletion attacks. By employing Support Vector Machines (SVM) to explore patterns generated by Implantable Medical Devices (IMD), the authors throttled malicious authentications, thus saving a significant amount of energy related to the IMD. The researchers achieved a notable accuracy for detecting unauthorized access attempts; 90% and 97% accuracy for linear and non-linear SVM classifiers, respectively. Given that the proposed scheme employs a smartphone as a mechanism to conduct classification, it might have some issues if the

smartphone is stolen or forgotten by the patient. In this case, it is unclear how access will be granted. Further, the proposed scheme was designed and tested only on one type of IoT device and thus might not be generic enough to be employed for various IoT types. Similarly, Yang et al. [81] proposed an RFID-based solution aiming to address several IoT security challenges such as device authentication, confidentiality, and integrity of devices through their supply chain. Indeed, on the way from the manufacturer to the end users, the devices or their components could be stolen, replaced by malicious ones or modified. By binding the RFID tags with the control chip of the IoT devices, the authors aimed to prevent these situations. To this end, the solution indexes the following traces: (i) unique combination of tag and device IDs, (ii) session keys, and (iii) the supply path. The verification of these traces ensures that the IoT devices were not replaced by fake ones. Although the proposed solution holds promise to provide security through the supply chain, it is still in its design phase and ultimately requires thorough evaluation. Further, by adopting the Constrained Application Protocol (CoAP), Jan et al. [104] proposed a lightweight authentication algorithm for verifying IoT devices' identities before running them in an operational network. In particular, the authors argued that using a single key for authentication purposes reduces connection overheads and computational load. By limiting the number of allowed connections for each ID to a single one, the authors aimed to restrict multiple connections between malicious nodes and servers at a given time, hence, protecting the network against a plethora of attacks such as eavesdropping, key fabrication, resource exhaustion and denial of service. However, the proposed algorithm does not defend the IoT network if the malicious node actively spoofs multiple identities.

In alternate work, Kothmayr et al. [56] introduced a two-way authentication scheme for the IoT paradigm based on the Datagram Transport Layer Security (DTLS) [156] protocol. The scheme is suggested to be deployed between the transport and application layers. The evaluation of the proposed mechanism in a real IoT testbed demonstrated its feasibility and applicability in various IoT settings. Further, Sciancalepore et al. [105] presented a Key Management Service (KMS) protocol that employs certificates, by applying the Elliptic Curve Qu-Vanstone (ECQV) [157] algorithm. The evaluation results demonstrated that the approach demands low bandwidth and reasonable ROM footprint. Although the algorithm can be considered applicable to the IoT paradigm, the authors did not assess its security under various IoT settings. Moreover, the employed certificates require secure management and the authors did not clarify how to satisfy this requirement. Along the same line of thought, Porambage et al. [58] introduced a lightweight authentication mechanism, namely PAuthKey, for WSNs in distributed IoT applications, which aimed at ensuring end-to-end security and reliable data transmission. Besides this, Park et al. [106] proposed a more complex solution. The authors adopted ECQV [157] certificates and employed the concept of Cryptographically Generated Address (CGA) [158]. The integration of this combination into the existing IEEE 802.15.4 [159] protocol indeed yielded promising results. In particular, in contrast to PAuthKey [58], the proposed scheme required less energy and execution time. Likewise, Garcia-Morchon et al. [107] proposed two security architectures by adapting the DTLS [156] and the HIP [160] protocols for IoT devices with Pre-Shared Keys (PSK). The schemes' evaluations demonstrated that authentication based on DTLS negatively affects network performance and thus performs much worse than HIP-based authentication. In particular, DTLS induces a larger memory footprint while HIP added significant overhead in the context of key management. Both designs aimed to achieve several security features such as mutual authentication between the IoT device and the domain manager, assurance of legitimate access to the network, and enforcement of standardized communication protocols.

Alternatively, many researchers have concentrated on biometric-based access control. Biometrics often refers to various characteristics such as fingerprints, iris, voice, and heartbeat. In this context, Rostami et al. [108] introduced an access-control policy, namely Heart-to-heart, for IMD. The policy offers a compelling balance between resistance against a number of attacks and level of accessibility/usability in an emergency situation. Specifically, the researchers proposed a lightweight authentication protocol which exploits Electrocardiography (ECG) randomness to defend against active attacks. Following an emerging trend rendered by the adoption of biometrics for authentication, Hossain et al. [109] presented an infrastructure for an end-to-end secure solution based on biometric characteristics. The proposed architecture consists of four layers. These include IoT devices, communication, cloud, and application. The sensors collect biometric features and transmit them through encrypted communication channels to a cloud, where they are processed by the application layer. The authors illustrated prevention methods against numerous types of attacks such as replication attacks, in which an attacker copies data from one session to be employed in a new session. Similarly, Guo et al. [110] noted that traditional access control such as a passwords is outdated. The authors proposed an access control approach which includes biometric-based key generation; a robust technique against reverse engineering and unauthorized access. To protect biometric information, the authors suggested to employ an additional chip that acts as a permutation block, in order to permit secure communications between programmable and non-programmable components. Executed simulation results exhibited reliability characteristics and a relatively small amount of information leakage. The authors attested that such an approach for authentication could also enhance IoT applications by, for instance, extracting gender and age information from biometrics and generating relevant statistics, or maintaining public safety by promptly identifying illegitimate individuals. In the same way, Dhillon et al. [69] proposed a lightweight multi-factor authentication protocol to elevate the security of the IoT. The proposed scheme employs a gateway node which requires the user to register prior to initiating any communication. To this end, a user generates their identity, credentials, personal biometric traits, and a random number. The combination of these features create a hash value, which is used for authentication. Once registered, the user can demand access through a smart device

by logging in to the desired IoT service/application using their biometrics and credentials. Security is enforced by utilizing one-way hash, perceptual hash functions, and XOR operations that are computationally less expensive and, thus, suitable in IoT environments. Evaluation of this approach demonstrated that the proposed access method considerably limits information leakage in case of physical, denial-of-service and replay attacks. Nevertheless, complexity analysis of the proposed scheme should be conducted to strongly validate its applicability for resource-constrained IoT devices.

In addition, few research contributions have been dedicated to context-aware permission models. For instance, Jia et al. [70] aimed to design a context-based permission system that captures environmental IoT contexts, analyze previous security-relevant details, and take further mitigative action. To this end, the authors conducted an extensive analysis of possible intrusion scenarios and designed a method which fingerprints attack contexts withing certain IoT applications. In a similar context, Fernandes et al. [111] introduced a method of restricting access to sensitive IoT data. The authors designed a system dubbed as FlowFence, which allows controlling the way data is used by the application. The researchers achieved this goal by granting access to sensitive data only to user-defined data flow patterns while blocking all undefined flows. The proposed solution empowers developers with the ability to split their application into two modules; the first module operates sensitive IoT information in a sandbox, while the second component coordinates the transmission of such sensitive data by employing integrity constraints. The validation of FlowFence in a consumer IoT realm demonstrated the preservation of confidential information, with limited increase in overhead. Besides academic research, security vendors are also introducing smart security solutions. Among those, Dojo [161], Cujo [162], Rattrap [163], and Luma [164] stand out and provide network security services for IoT devices in home and critical CPS environments. Their features include firewall capabilities, secure web proxy, and intrusion detection and prevention systems. Although these products promise to protect home networks with little effort from the user, their configuration settings are not always straight forward, often resembling a black-box solution, while their evaluation in real IoT realms has not been exhaustively reported.

2) Software Assurance: Given the potential impact of exploiting IoT software, the proper software assurance ought to be an integral part of the development life-cycle. This aims at reducing the vulnerabilities of both source and binary code to provide resiliency to the IoT paradigm. To this end, Costin el al. [112] proposed a scalable, automated framework for dynamic analysis aiming to discover vulnerabilities within embedded IoT firmware images. The authors performed their investigation by emulating firmware and adapting available free penetration tools such as Arachni [165], Zed Attack Proxy (ZAP) [166] and w3af [167]. By testing close to 2,000 firmware images, the authors discovered that nearly 10% of them contains vulnerabilities such as command injection and cross-channel scripting. Further, Li et al. [113] noted that traditional code verification techniques lack domain-specificity, which is crucial in IoT contexts, notably for embedded medical devices. In particular, the authors pinpointed that delays in code execution paths could even threaten the life of an individual. However, curently available techniques do not verify the delays. With the aim to improve the trustworthiness of the software embedded in medical devices, the authors proposed to extend traditional code verification techniques by fusing safety-related properties of specific medical device to code model checker such as CBMC [168]. To this end, the researchers transformed safety properties to testable assertions against which the checker verifies the programming code. The implementation of the proposed techniques for the software verification of pacemaker, which is implantable electronic device that regulates heartbeats, unveiled that the software code failed various safety properties.

Applying the aforementioned and similar techniques aims at finding vulnerabilities without executing software code, thus requiring access to source code. The assessment of binary code, on the other hand, is more applicable when programming code is not available. Many traditional techniques could be adopted for the IoT paradigm. For instance, Zaddach et al. [114] presented a framework dubbed as Avatar for dynamic analysis of embedded IoT systems by utilizing an emulator and a real IoT device. In particular, an emulator executes firmware code, where any Input/Output (IO) is forwarded to the physical device. Consequently, signals and interrupts are collected on the device and injected back into the emulator. An evaluation of the framework proved its capability to assist in IoT security-related firmware assessment; reverse engineering, vulnerability discovery and hard-coded backdoor detection. Alternatively, Feng at al. [78] demonstrated how learning of high-level features of a control flow graph could improve the performance of firmware vulnerability search methods. The proposed approach employs unsupervised learning methods to identify control flow graph features extracted from a binary function. Such features are then transformed into a numeric vector for applying Locality Sensitive Hashing (LSH). By leveraging a method rooted in visual information retrieval to optimize the performance of the vulnerability search mechanism, the authors demonstrated the efficiency and accuracy of the proposed scheme. Moreover, an analysis of more than 8,000 IoT firmware unveiled that many of them are vulnerable to known OpenSSL vulnerabilities, opening the door for DoS attacks and leakage of sensitive information. Along the same line, Elmiligi et al. [79] introduced a multidimensional method to analyze embedded systems security at different levels of abstraction. The foundation of the approach is mapping the attacks to three dimensions, namely, programming level, integration level, and a life cycle phase. This permitted the capability to analyze more than 25 IoT-centric security scenarios. The authors illustrated how the proposed evaluation methodology indeed improves the security of IoT embedded systems during various product life-cycles.

3) Security Protocols: Zhang et al. [115] argued that enclosing each node in tamper-resistant hardware is unrealistic

TABLE VII
SUMMARY OF REMEDIATION STRATEGIES

Vulnerability	Remediation Strategy			References
	Access and Authentication Controls	Software Assurance	Security Protocols	
Deficient physical security	●	○	○	[47], [81], [115]
Insufficient energy harvesting	●	○	●	[103], [115], [116]
Inadequate authentication	●	○	○	[56]–[58], [81], [104]–[107], [161]–[164]
Improper encryption	○	○	●	[62], [63], [118]
Unnecessarily open ports	○	○	○	[-]
Insufficient access control	●	●	●	[69], [70], [108]–[111], [119]
Improper patch management capabilities	○	○	○	[-]
Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, ect.)	○	●	○	[78], [79], [112]–[114]
Insufficient audit mechanism	●	○	○	[81]

Legend: ● strategy covers particular vulnerability, ○ strategy does not cover particular vulnerability

and cost inefficient. With the aim to design an energy efficient and compromise-tolerant scheme, Zhang et al. proposed the Coverage Interface Protocol (CIP). The authors advocated that the proposed protocol can protect a device from both, external physical attacks and attacks originating from compromised nodes. The CIP consists of two components, namely, a Boundary Node Detection scheme (BOND) and a Location-Based Symmetric Key management protocol (LBSK). BOND equips IoT nodes with the ability to recognize their boundary nodes, while LBSK establishes related keys to secure core network operations. While the proposed scheme seems to be efficient by saving energy, its large-scale evaluation in a real IoT testbed would definitely aid in realizing its advantages and disadvantages. Alternatively, Rao et al. [116] proposed the predictive node expiration-based, energy-aware source routing protocol, which attempts to optimize the overall energy efficiency of the IoT sensor network. This aims at ensuring that the sensed information effectively reaches the sink through a reliable path. Further, Glissa and Meddeb [117] considered various potential attacks on 6LoWPAN and proposed a multi-layered security protocol, namely, the Combined 6LoWPSec. The proposed scheme aimed at limiting attacks on IPv6 IoT communications. By leveraging security features of IEEE 802.15.4, the authors designed an algorithm which operates at the MAC layers. In contrast to gathering security-related information at each node hop, the authors proposed approach enables security implementation at the device level. Evaluation of 6LoWPSec demonstrated power efficiency under a number of attack scenarios.

Given that IoT applications often utilize the cloud to store and share data, Shafagh et al. [62] approached IoT security by designing a data protection framework, dubbed as Talos, where the cloud curates encrypted data while permitting the execution of specific queries. The proposed solution relied on Partial Homomorphic Encryption (PHE). Through executing micro-benchmarking and system performance evaluation, the authors experimentally demonstrated that the proposed solution consumed modest energy level, while providing a measurable increase in security level. The same researchers extended Talos in [118] and presented a next generation PHE solution for IoT; designed and implemented using additive homomorphic schemes. The proposed protocol is composed of three main building blocks. These include a client engine, a cloud engine, and an identity providers; only the client engine has access to the keying material. This component is also responsible for encryption/decryption, triggering key revocations, and several sharing-related activities. The cloud engine, on the other hand, provides the database interface and features, and only operates on encrypted data. The responsibility to verify user identity is given to the third party identity provider. In the context of implementation, the researchers prototyped their solution for the mobile platform and thoroughly evaluated its inner workings. The authors concluded that the proposed protocol possesses reasonable overhead in processing time and end-to-end latency. Auxiliary, Wei et al. [63] recently offered a scalable, one-time file encryption protocol, which combined robust cryptographic techniques to protect files from arbitrary users. By adopting techniques and technologies rooted in identity-based encryption, the authors designed and implemented a capability to securely transmit key pairs via SSL/TLS channels. Further, Yang et al [119] proposed a lightweight access protocol for IoT in healthcare. In this context, access to IoT data should be granted in two different situations under usual and emergency modes/situations. In the first mode, the proposed scheme employs attribute-based access, thus family members and health providers would have different privileges. In case of emergency, on the other hand, an emergency contact person utilizes a password to extract a secret key to decrypt patient's medical files. As reported by the authors, the scheme does not leak access-related information, and requires lower communication and computation costs than other existing attribute-based access control schemes in the context of IoT.

Having elaborated on the above, we now summarize the key findings in Table VII, which depict the relationship between the extracted IoT vulnerabilities and their corresponding remediation approaches.

Findings.
Physical access to IoT devices could ultimately cause their damage, unveiling their cryptographic schemes, replicating them by malicious ones, and corrupting their data. While all the aforementioned issues are quite severe, we notice the lack of their corresponding remediation strategies. Further, while several firewalls are already proposed in the context of the IoT, mostly those that are designed by the industry, it remains unclear whether their marketing hype matches their security expectations. Even though emerging solutions such as biometric and context-aware permission models promise to improve access controls in IoT realms, they undoubtedly raise a number of concerns and issues. Among them, how well the proposed biometric-based access control would maintain the security of the biometrics and to which extent would context-aware permission models be practically implemented. Moreover, both of their large-scale implementation, evaluation and validation in tangible IoT realms require further investigation. Further, although there exists a number of research efforts which propose IoT-tailored encryption schemes, we notice the shortage of studies which exhaustively and thoroughly assess and analyze their advantages and disadvantages under different malicious and benign IoT scenarios. We also pinpoint the lack of approaches which aim at overcoming the insufficiency of IoT audit mechanisms in reducing the possibility to conceal the involvement of the IoT in malicious activities. Finally, we note the deficiency of remediation techniques concentrated on unnecessarily open ports and improper patch management. Indeed, such methods would ensure meeting various security objectives, as pinpointed in Table V.

F. Situational Awareness Capabilities

Having a myriad of IoT devices with numerous unique traits such as type, manufacturer, firmware version, and context in which they operate in, it is indeed quite challenging to continuously infer evolving IoT-specific vulnerabilities. Moreover, adversaries will continue to became more advanced and skilled, executing sophisticated, stealthy attacks, thus exploiting zero-day and other critical vulnerabilities. To guarantee a certain level of IoT security and resiliency, the effectiveness of any security mechanism would need to be subject to regular assessments and scrutiny. In this context, IoT vulnerabilities, in accordance with the taxonomy of Figure 3, could be further classified by various (operational) security assessments and monitoring strategies. We distinguish four classes of such categories, including, vulnerability assessment techniques, honeypots, network discovery methods, and intrusion detection mechanisms.

1) Vulnerability Assessment: Executing security evaluations undoubtedly aids in discovering IoT vulnerabilities prior to them being exploited. Various methods ranging from testbeds to attack simulation and fuzzing techniques have been decisive in obtaining effective and actionable information related to the cyber threat posture of the IoT paradigm.

A research direction in this area focuses on designing new testbeds or adopting existing methods to perform IoT vulnerability assessment. One of such testbeds, which utilize a number of open source software such as Kali Linux, Open VAS, Nessus, Nexpose, and bindwalk, was proposed by Tekeoglu et al. [71]. Such proposed approach enables the capturing of network traffic for analyzing its features to identify IoT security vulnerabilities. In particular, the authors noted several insightful inferences; most of the investigated IoT devices do not lock-out users after failed login attempts; several unnecessary open ports facilitate targeted attacks; and a large number of devices are operated with outdated versions of their software and firmware. The authors advocated that the proposed testbed could be leveraged to conduct various experiments. While the testbed seems quite practical, its operating procedure is still rather manual. Further, Siboni et al. [65] designed a unique testbed for wearable devices. The framework performs the traditional vulnerability tests along with security assessments in different contexts, which is crucial and quite practical when dealing with the IoT paradigm. The technical architecture of the proposed testbed consists of various modules; a functional module which is responsible for test management, a module which is tied to the execution of standard security tests, a unit for generating insights related to context-aware assessments, and a module dedicated for the analysis and report generation. Such a layered architecture allows deploying relevant simulators and measurements for a particular IoT device. As a proof-of-concept, the framework was used for different wearable IoT devices such as Google Glass and smartwatch.

In another work, Reaves and Morris [120] designed two testbeds for IoT within Industrial Control Systems (ICS) to compare different implementation types and to infer the most efficient way to identify vulnerabilities. One of the testbeds consists of physical devices in a laboratory environment, while the other emulates device behavior using Python scripts. To test the response of the system in cases of adding devices to the network or infiltration of the radio signals, the researchers simulated three kinds of attacks. The authors reported their results by indicating that both implementations efficiently emulate real systems. However, some unique IoT traits, including their manufacturing characteristics, should be tested separately. In an alternative work, Furfaroa et al. [59] offered a scalable platform, known as SmallWorld, which enables security professionals to design various scenarios to assess vulnerabilities related to IoT devices. By uniquely reproducing the behavior of human users and their corresponding events, the authors created a practical capability to achieve the intended objective. The architecture of their proposed platform is composed of five layers; including physical, abstraction, core service, API, and management layers. Such a composition offers data replication mechanisms, provides a scalable platform, puts forward an API for deploying IoT-tailored simulation scenarios, and facilitates the gathering and analysis of related

descriptive statistics. Through variously investigated case studies in the context of home automation applications, the authors illustrated the effectiveness of the platform by permitting formal evaluation of IoT security. The researchers stated that such an approach allows identifying IoT security issues prior to operating such IoT devices in production contexts. Since fuzzy-based approaches similar to [169] are widely applied in traditional IT realms, Lahmadi et al. [121] designed a testing framework that enables developers to assess the security of the 6LoWPAN [40] protocol. By employing mutation algorithms to messages at different network layers, the testing suite analyzes deviations from expected and actual responses of IoT devices. The authors focused on the Contiki 6LoWPAN implementation, leaving other variants for future work. Along the same research direction, Cui et al. [122] applied a fuzzy technique [169] to ZigBee networks to locate and analyze vulnerabilities within IoT networks. The authors combined Finite State Machines (FSM) with a structure-based fuzzy algorithms suited for the MAC protocol of Zigbee. To verify the proposed technique, the researchers conducted a series of performance tests. The results unveiled that compared to random-based algorithms, the proposed FSM-fuzzy framework is more cost-effective, while compared to a structure-based algorithm, its results are more accurate.

2) Honeypots: Behaving like real IoT assets while having no value for an attacker, honeypots trap and analyze an adversary by intentionally creating security vulnerabilities. These devices (or their software counterparts) capture malicious activities for further investigation of attack vectors or to generate attack patters, which could be used for future mitigation. Honeypots, however, mimic a very specific type of devices in a particular environment, introducing major scalability issue in the context of the IoT ecosystem.

Pa Pa et al. [123] were among the first to pioneer IoT-specific honeypots. The researchers offered a trap-based monitoring system dubbed as IoTPOT, which emulates Telnet services of various IoT devices to analyze ongoing attacks in depth. The authors observed a significant number of attempts to download external malware binary files. The authors distinguished three steps of Telnet-based attacks, namely, intrusion, infection and monetization. During the first phase, the researchers observed numerous login attempts with a fixed or a random order of credentials. The authors distinguished 10 main patterns of command sequences which are used to prepare the environment for the next step. In the second stage of an attack, the device downloads the malware, while in the last step, controlled by an attacker, the device conducts DDoS attacks, Telnet and TCP port scans, and spread malware. Moreover, the authors presented IoTBOX, a multi-architecture malware sandbox, that is used for analysis of captured binaries. Consequently, five distinct malware families were discovered. The authors, however, did not provide geo-location information about the sources of the attacks. In alternative work, Guarnizo et al. [124] presented the Scalable high-Interaction Honeypot platform (SIPHON) for IoT devices. The authors demonstrated how by leveraging worldwide wormholes and few physical devices, it is possible to mimic numerous IoT devices on the Internet and to attract malicious traffic. The authors further provided insights regarding such traffic, including the popularity of target locations, scanned ports, and user agents. Similarly, Vasilomanolakis et al. [125] proposed HosTaGe, a honeypot that aims to detect malicious activities targeting ICS networks. HosTaGe supports the identification of attacks in various protocols as HTTP, SMB, Telnet, FTP, MySQL, SIP, and SSH. Upon detection, the proposed honeypot generates effective attack signatures to be employed in IDS for future detection and thus mitigation. In another work, to detect targeted attacks against ICS which rely on Programmable Logic Controllers (PLC), Buza et al. [126] designed the Crysys honeypot. Such honeypot, which was evaluated in a lab environment, was capable to detect port scans and numerous brute-force attempts via SSH. Additionally, Litchfield et al. [127] proposed a CPS framework supporting a hybrid-interaction honeypot architecture. The proposed honeypot known as HoneyPhy aims to provide the ability to simulate the behavior of both CPS processes and IoT devices. The framework consists of three modules; Internet interfaces, process modules, and device models. The first component maintains connections, manages outgoing packets, and alters traffic packets if necessary. The second element correctly emulates the systems' dynamics related to the physical process. Finally, the last component encompasses CPS devices and mimics their logic. The proposed honeypot was instrumented in a lab environment where its capability to simulate real systems was assessed and reported. In alternative work, Dowling et al. [128] designed a honeypot which simulates a ZigBee gateway to explore attacks against ZigBee-based IoT devices. By modifying an existing SSH honeypot, namely Kippo [170], using a set of Python scripts, the authors monitored three-month activities targeting the Zigbee gateway. The researchers reported six types of executed attacks. These include dictionary and bruteforce attacks, scans, botnets and a number of other independent events. The authors reported that dictionary attacks represented nearly 94% of all attacks.

3) Network Discovery: Given the large-scale deployment of vulnerable IoT devices, it is essential to have a scalable capacity to identify (vulnerable or compromised) devices at large for prompt remediation. To this end, network discovery techniques become an utmost priority.

In this context, Fachkha et al. [129] recently analyzed attackers' intentions when targeting protocols of Internet-facing CPS. The authors leveraged passive measurements to report on a large number of stealthy scanning activity targeting more than 20 heavily employed CPS protocols. Alternatively, Galluscio el al. [130] illustrated the widespread insecurity of IoT devices by proposing a unique approach to identify unsolicited IoT nodes. By leveraging large darknet (passive) data and applying a correlation algorithm, the authors determined nearly 12,000 attempts to exploit different Internet host generated by compromised IoT devices. The approach supports the inference of such compromised devices in various IoT deployment environments, rendering it

possible to leverage the proposed approach for an Internet-scale application. From an industrial perspective, the search engine for Internet-connected devices Shodan [131] crawles the Internet 24/7 and updates its repository in real-time to provide an recent list of IoT devices. By grabbing and analyzing banners and device meta-data, Shodan conducts testing for various vulnerabilities including Heartbleed, Logjam, and default passwords. In a similar manner, the search engine Censys [132] collects data (including IoT information) through executing horizontal scans of the public IPv4 address space and provides public access to raw data through a web service. In contrast, Meidan et al. [133] leveraged network traffic analysis to classify IoT devices connected to an organization's network. By applying single-session classifiers, the authors were able to distinguish IoT devices among other hosts with 99% accuracy. The proposed method holds promise to enable reliable identification of IoT connections in an enterprise setting. Similarly, Formby et al. [134] designed two approaches for device fingerprinting. The first method leverages the cross-layer response time while the second utilizes the unique physical properties of IoT devices. The accuracy of both methods is 99% and 92%, respectively.

4) Intrusion Detection: An effective approach to infer malicious attempts generated from the IoT paradigm is to employ Intrusion Detection Systems (IDS). Such mechanisms support both detection and prompt response to malicious activities. Given the limited resources of IoT devices, most deployed intrusion detection techniques are network-based with an active response system, which operates by halting communications of the compromised nodes.

Raza et al. [136] pioneered an IDS, known as SVELTE, for IoT contexts. The authors explained how monitoring of inconsistencies in node communications by observing network topology protects IoT devices against various known attacks. The system consists of three centralized modules that are deployed in a 6LoWPAN Border Router. The first component, namely 6Mapper, gathers information about the network, reconstructs a Destination-Oriented Directed Acyclic Graph (DODAG), and infuses the node's parent and neighbors information into DODAG. The second module is responsible for analysis and intrusion detection, while the third module acts as a simplistic firewall which filters unwanted traffic before it reaches the resource-constrained network. The proposed approach proved its ability in accurately detecting various malicious misdemeanors. More recently, to enhance the security within 6LoWPAN networks, Shreenivas et al. [137] extended SVELTE with two additional modules. The first is an intrusion detection module that uses Expected Transmissions (ETX) metrics, monitoring of which can prevent an adversary from engaging 6LoWPAN nodes in malicious activities. The second module consists of a technique which attempts to locate malicious nodes inside the 6LoWPAN network. To make these extensions possible, the authors complemented the 6Mapper with an ETX value, making it part of each received request. An intrusion is determined by comparing the parent and children's ETX values; the parent's ETX should be lower than that of its children. In cases where an attacker compromises the node and its neighbors, it is hard for 6Mapper to distinguish the inconsistencies using ETX values. To mitigate this limitation, the authors proposed to utilize the knowledge of node location and cluster the nodes to identify their immediate neighbors. The technique allows the determination of IoT devices with fake identities, thus proactively preventing various attacks.

Further, Yang et al. [138] proposed a scheme that enables the detection of FDI attacks in IoT-based environmental surveliance at an early stage. To this end, the authors leveraged state estimation techniques based on Divided Difference Filtering (DDF) to detect false aggregated data and Sequential Hypothesis Testing (SHT) to determine the nodes that are suspected of injecting false data. The detection framework comprises of two modules: *(i)* local false data detection and *(ii)* malicious aggregate identifier. The first module conducts the threshold-based detection of the data falsification, while the second module utilizes the result of the first one to take further decision. An evaluation of the scheme demonstrated high detection rate with a low false positive rate. In alternative work, Thanigaivelan et al. [139] leveraged collaboration between 1-hop neighbor nodes to design a distributed anomaly detection system for the IoT paradigm. Each node is responsible for monitoring the behavior of its neighbors. In particular, the approach monitors packet size and data rate. Once an anomaly is detected, the abnormally-behaving node is isolated from the network by discarding the packets at the link layer, and the observed event is escalated to a parent node. Further, Parno et al. [140] proposed two distributed schemes, namely, randomized and line-selected multicast, for detecting nodes' replications. The first proposed algorithm is based upon a broadcast protocol in which each node floods the network with its identity and location information. Further, randomly selected nodes collect this data and check whether locations are the same for particular nodes. Two conflicting points would trigger the network to revoke a node. This algorithm assumes that each node is aware of its position and network by employing an identity-based public key system. The second proposed algorithm eliminates the step where each node broadcast its location within the network but instead shares it with randomly selected nodes directly. If a node that is responsible for detection receives two different locations for the same identity, it triggers a network response to revoke that node. The authors evaluated both algorithms in a lab environment and confirmed that the second method requires fewer communication packets, while the first method provides higher resiliency since it prevents an adversary from anticipating the node which is responsible for detection.

In another work, Bostani et al. [141] proposed a novel real-time intrusion detection framework for detecting malicious behaviors against routing protocols within an IoT network. In particular, the authors investigated sinkhole and selective-forwarding attacks. Both router and root nodes participate in the detection decision making. Analysis begins with the router node, which applies specification-based detection mechanisms to its host nodes and sends the results to the root node. In turns, a detection mechanism employed at the root node employs the unsupervised optimum-path forest algorithm for projecting clustering models using the

TABLE VIII
IOT SECURITY SITUATIONAL AWARENESS CAPABILITIES

Vulnerability	Situational Awareness Capabilities				References
	Vulnerability Assessment	Honeypots	Network Discovery	Intrusion Detection	
Deficient physical security	●	○	○	●	[120], [140]
Insufficient energy harvesting	○	○	○	●	[52], [136], [137], [141]
Inadequate authentication	●	○	●	●	[59], [65], [133], [134], [136], [138], [140], [142]
Improper encryption	●	○	○	○	[65], [121], [122]
Unnecessarily open ports	●	●	○	○	[65], [71], [123]–[127]
Insufficient access control	●	●	●	○	[65], [71], [123]–[132]
Improper patch management capabilities	●	○	○	○	[71]
Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, etc.)	●	○	○	●	[59], [65], [71], [136], [138], [142]
Insufficient audit mechanism	○	○	○	●	[136], [138], [142]
Compromised device identification	○	○	●	●	[21], [52], [130], [136]–[142]

Legend: ● capability covers particular vulnerability, ○ capability does not cover particular vulnerability

incoming data packets. The results of both analysis are leveraged as input to the voting mechanism for intrusion detection. Alternatively, aiming to reduce energy depletion in a wireless sensor network, Patel and Soni [52] proposed to keep the energy level of a node in a routing table. Further, the communication protocol calculates the threshold energy ($Th(E)$) and compare it with the energy level (EN_i) of the next node. In case $EN_i > Th(E)$ a communcation packet is sent, otherwise, the protocol employs the procedure of route repairment. In a different work, Midi et al. [142] proposed a self-adaptive knowledge-driven IDS, namely Kalis, that is capable of detecting attacks against IoT environments across a wide range of protocols. Kali could be implemented as a smart firewall to filter suspicious incoming traffic from the Internet. By observing the available events and determining features of entities and networks, the system determines which detection technique to activate to infer a security incident. By keeping in mind the heterogeneous nature of IoT devices, communication protocols, and software, the authors designed the system, so that it does not require software alterations, complies with various communication standards, is extensible to new technologies, and avoids significant performance overhead. Moreover, the proposed system enables knowledge sharing and collaborative detection techniques. System evaluation demonstrated the accuracy of the approach in detecting various attacks. Additional, Yu et al. [21] argued that traditional host-based solutions are not applicable in IoT realms due to device constraints and their deployment in various environments. To overcome such limitations, the authors specified three dimensions through which the network traffic related to IoT has to be subjected. These include an environmental and security-relevant contexts along with cross-device interactions. The authors proposed a crowd-sourced repository for sharing and exchanging attack signatures. Finally, the researchers suggested a security enforcement technique, which extends Software-Defined Networks (SDNs) and Network Functions Virtualization (NFV) to the IoT context and employs the concept of micro-middleboxes for real-time remediation of vulnerable IoT devices.

To contribute to the objective of detecting IoT maliciousness, several research attempts have been made on large-scale vulnerability notifications. Nonetheless, a plethora of them center on compromised websites hosting IoT devices [171], [172], while only one investigated the effectiveness of IoT situational awareness. To this end, Li et al. [135] demonstrated how message content and contact point affect fix rate of vulnerabilities for ICS. In particular, the results indicate that the most effective method is direct notification with detailed information. However, the authors pinpointed that the majority of contacts did not respond or fixed their problem. Thus, the effectiveness of such notification remains an open question and undoubtedly requires attention from the security research and operational communities.

The relationship between the available situational awareness capabilities in addressing the pinpointed IoT vulnerabilities is summarized and illustrated in Table VIII.

Findings.
Many techniques already exist that aim at identifying IoT security weaknesses, learning attackers' behaviors and continuously monitoring devices for proper remediation. Nevertheless, the status of their practical implementation in IoT contexts remains somehow ambiguous. Further, many approaches do not seem to be generic enough to address the heterogeneity of IoT paradigm. Additionally, while we note that intrusion detection techniques in IoT realms demonstrate advanced progress, some of their methodologies leave the room for further research. Indeed, relying only on IDS mechanisms in an attempt to monitor intrusions seems to be not very effective, since they only detect limited attacks as illustrated in Table IX. Nevertheless, passive data-driven approaches hold promise to overcome these limitations, while, in general, the probability of inferring exploited devices remains obscure and requires further investigation.

TABLE IX
INTRUSION DETECTION TECHNIQUES DEPLOYED IN IOT ENVIRONMENTS

Attack	Behavior-based					Knowledge-based		
	[136]	[137]	[138]	[139]	[140]	[141]	[52]	[142]
Dictionary attack	○	○	○	○	○	○	○	○
Side-Channel attack	○	○	○	○	○	○	○	○
Sybil attack	●	○	○	○	○	○	○	○
False Data Injection	●	○	●	○	○	○	○	●
Firmaware modification attack	○	○	○	○	○	○	○	○
Device capture	○	○	○	○	●	○	○	○
Sinkhole Attack	●	○	○	○	○	●	○	○
Battery draining attack	○	●	○	○	○	○	●	○
Selective-forwarding	●	●	○	○	○	●	○	●
Anomaly detection	○	○	○	●	○	○	○	○

Legend: ● a technique detects an attack, ○ a technique does not detect an attack

VI. EMPIRICAL EVALUATION OF IOT MALICIOUSNESS

The elaborated vulnerabilities undoubtedly open the door for adversaries to exploit IoT devices. While the provided taxonomy, discussed literature approaches and complementarity mitigation and awareness capabilities provide a unique, methodological approach to IoT security, in this section, we provide a concrete, first empirical perspective of Internet-wide IoT exploitations. This aims at (1) providing a practical "flavor" to the presented survey in addition to warning about the severity of such exploitations and (2) highlighting the need for more empirical approaches when addressing the IoT security issue, especially at large-scale. While it is a known fact the the latter objective is quite difficult to achieve due to the lack of IoT-relevant empirical data and the widespread deployments of such IoT devices in Internet-wide realms, in this section, we explore unique, macroscopic data to achieve this objective. To this end, we leverage passive measurements rendered by scrutinizing darknet data. Indeed, such data represents Internet-scale traffic targeting routable, allocated yet unused IP addresses. The absence of Internet services associated with these IP addresses render them an effective approach to amalgamate Internet-wide unsolicited events [173].

We scrutinize approximately 33 GB of darknet data that was recently collected from a /8 network telescope. We further correlate it with data collected from Shodan. As previously noted, Shodan indexes Internet-wide IoT devices by performing banner analysis on the results of active probes. The correlation was executed based on matching header information between data collected from Shodan and source IP information targeting the darknet.

The worldwide distribution of exploited devices is illustrated in Figure 8. It is evident that the United States hosts more exploited devices related to both consumer and industrial environments than any other country. At the same time, we observe that IoT deployments in industrial settings are more exploited in China, while in the consumer sectors, the leading countries seem to be Taiwan and Russia. It is worthy to mention that we have identified exploitations in more than 140 countries, which indicates that such an abuse is highly distributed, questioning the currently available IoT remediation

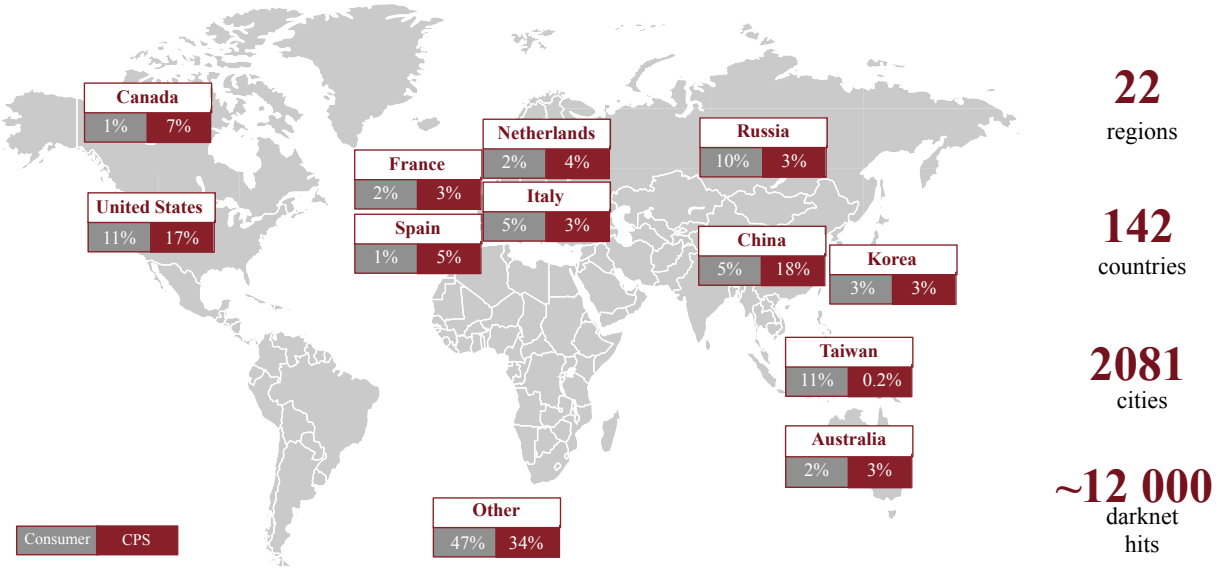
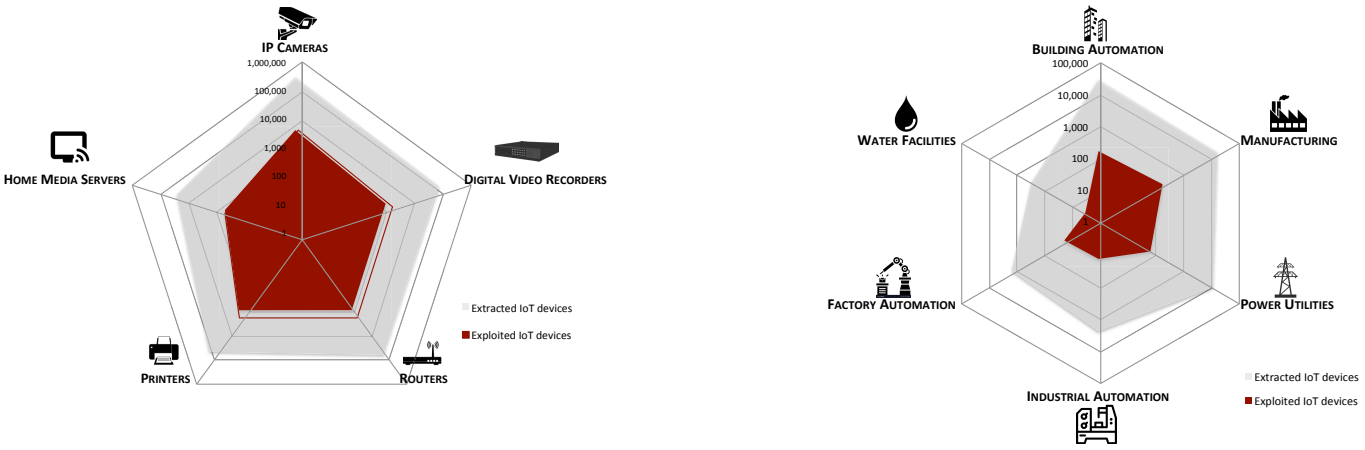


Fig. 8. Global distribution of exploited IoT devices



(a) in consumer sectors

(b) in CPS sectors

Fig. 9. Distribution of extracted and exploited IoT sevices

approaches, which typically operate in significantly localized realms.

The distribution of extracted IoT information (from Shodan) versus those that are exploited in consumer realms is illustrated in Figure 9a. It is evident that the ratio of exploited devices to those that are extracted is approximately the same for various IoT devices, while their number drastically differ. Figure 9b depicts the distribution of extracted and exploited devices in CPS realms. Such insights demonstrate that the manufacturing, factories, and water facilities host more exploited devices than any other sector. Nevertheless, CPS environments attract adversary slightly less than consumer sectors. We postulate that the difference could arise from the fact that in CPS environments, security policies are more robust and strict than in consumer realms. While such results are very preliminary, they aim at shedding the light on the large-scale insecurity of the IoT paradigm. In future work, we aim at performing a thorough analysis of such exploitations, characterizing their unsolicited activities and generated traffic in addition to exploring their malware infections.

VII. IoT Vulnerabilities: Challenges and Future Perspective

In this section, we outline a number of research and operational challenges and pinpoint several initiatives (both technical and non-technical) for future work, which we believe are worthy of being pursued in this imperative field of IoT security.

Please note that while the current offered literature survey did not glimpse into IoT security research contribution of 2018, nonetheless, for completeness purposes, we have identified a number of emerging topics which seem to be gaining noteworthy attention from the research community. Such topics include the design and implementation of blockchain technology for IoT security [174]–[177], deep learning methodologies for inferring and characterizing IoT maliciousness [178], [179], and the adoption of SDN and cloud paradigms for IoT resiliency [180]–[182].

Challenge 1.
One of the most significant challenges for future work is the design and implemention of Internet-scale solutions for addressing the IoT security problem. The widespread deployment of IoT in different private environments prevents visibility of IoT-related security incidents and thus hinders the adequate analysis of such data in order to identify, attribute and mitigate maliciousness. The investigation of empirical data, which enables Internet-scale detection of IoT maliciousness is of paramount importance. A significant hurdle to such approaches involves the development of mechanisms to acquire relevant data in a timely fashion. By building such (operational) capabilities based on empirical measurements, we gain substantial benefits. The first being that such an analysis is non intrusive, thus does not require resources from the IoT network or the devices. The second is related to the collection of sufficient information for generating IoT-centric malicious signatures, which is currently unavailable. These signatures could be deployed at local IoT realms for proactive mitigation.

Possible future initiatives.
The cyber security capability which leverages Internet-scale empirical measurements and data-driven approaches and methodologies to identify exploited IoT devices would indeed effectively complement currently available approaches to provide IoT resiliency.

There is a paramount need for collaborative knowledge and information exchange regarding the notion of maliciousness from various sources (including ISPs, IoT operations, researchers, etc.) to successfully address the IoT security issue.

Challenge 2.
As noted, empirical measurements for inferring IoT maliciousness is essential, yet solely insufficient to secure the IoT paradigm. Indeed, vulnerable yet unexploited IoT devices can not be addresses by employing the latter approach. Consequently, numerous devices remain vulnerable for future

exploitation. Although novel ways for vulnerabilities' identification efficiently address a number of IoT weaknesses, they mainly focus on particular devices. Hence, such methods lack device variability and scalability. In this context, there is a need for IoT-tailored testbeds which would enable automated vulnerability assessments for various devices in different deployment contexts.

Possible future initiatives.
Applying transfer learning algorithms [183] to the currently available knowledge related to IoT vulnerabilities could ameliorate and automate the tasks of vulnerability assessment and simulation in order to extrapolate this knowledge to various IoT devices, platforms and realms. This holds promise to conduct vulnerability assessment in a large-scale to contribute to prompt IoT remediation.

Additionally, investigating innovative IoT-specific trust models [70] that are employed in various contexts would enable the development of proper IoT remediation strategies.

Challenge 3.
This challenge addresses secure access to IoT devices and their data. It is indisputable that the ability to gain access to IoT devices by either brute-forcing their default credentials or by exploiting certain vulnerabilities remains a primary attack vector. While modifying default credentials is a necessary strategy, a myriad of legacy IoT devices with hard-coded or default credentials remain in use rendering it possible for an attacker to take advantage of such vulnerabilities to execute various misdemeanors. We noticed that approaches which attempt to address this issue are rarely investigated in the literature. Further, while using traditional password-based access methods seem to be the most frequently employed, new techniques rooted in biometric and context-aware methods are currently emerging for the IoT. However, we noticed the lack of comprehensive analysis, which enables the thorough comprehension of the advantages and disadvantages of these methods along with their corresponding implementation technicalities and challenges.

Possible future initiatives.
There is need to explore techniques and methods to increase users' awareness about the consequences of potential IoT threats and possible technical and non-technical strategies to reduce the risk of exposure.

Further, developing numerous approaches to enforce credential updates and automate the deployment of frequent firmware updates seems to need much attention from the research comunity. Such approaches should arise from inferred vulnerabilities using research methodologies (including IoT-malware instrumentation) as well as from IoT industrial (manufacturing) partners and market collaborators.

Challenge 4.
To assure sufficient level of IoT software security, proper and prompt operational actions should be established for the identified vulnerabilities. From the conducted survey, we noticed a noteworthy shortage of research and development methodologies, which address this issue. Another problem of significant importance is related to secure IoT code. IoT applications rely on tailored software applications, which could characteristically be vulnerable. We also noticed the lack of methods which aim at vetting deployed IoT code. Although many software assessment techniques are available, case studies similar to [184] report that nearly 50% of organizations that have deployed IoT never assess their applications from the software security perspective.

Possible future initiatives.
There is need to execute exploratory studies to inspect the time required from the discovery of IoT vulnerabilities to their disclosure to producing patches and subsequently deploying them at the affected IoT devices. Indeed, this would drive and enhance risk management for the IoT paradigm, especially for those IoT devices deployed at critical CPS environments.

Further, the investigation of the dependencies between weak programming practices and vendors, platforms, device types, and deployment environments would enable the selection of more reliable software vendors as well as encourage vendors to produce more secure code.

Along this line of thought, there is need to enforce stringent IoT programming standards and develop automated code tools to vet IoT applications in order to effectively remediate IoT software vulnerabilities, thus further contributing to IoT security and resiliency.

VIII. Concluding Remarks

The IoT paradigm refers to scenarios where network connectivity and computing capability extends to embedded sensors, allowing these devices to generate, exchange and consume data with minimal human intervention [185]. Such paradigm is being realized and facilitated by critical advancements in computing power, electronics miniaturization, and network interconnections. Indeed, the large-scale deployment of IoT devices promises to transform many aspects of our contemporary lives, offering more personal security, helping to minimize energy consumption, providing the possibility to remodel agriculture, and energy production, to name a few. While IoT deployments have been receiving much hype, their unique characteristics coupled with their interconnected nature indeed present new security challenges. Various technical difficulties, such as limited storage, power, and computational capabilities hinder addressing IoT security requirements, enabling a myriad of vulnerable IoT devices to reside in the Internet-space. Indeed, unnecessarily open ports, weak programming practices coupled with improper software update capabilities serve as entry points for attackers by allowing

malicious re-programming of the devices, causing their malfunction and abuse. Moreover, the insufficiency of IoT access controls and audit mechanisms enable attackers to generate IoT-centric malicious activities in a highly stealthy manner.

This survey aims at shedding the light on current research directions and their technical details from a multidimensional perspective focusing on IoT vulnerabilities. The relatively comprehensive study emanates many open research questions in the context of the security of the IoT paradigm. Specifically, Internet-scale solutions addressing the IoT security issue remain one of the most prominent challenge towards IoT resiliency. Research efforts are also required in the context of studying IoT-specific attacks and their malicious signatures. Indeed, such knowledge is essential in providing effective remediation solutions. Further, suitable schemes, which take into account IoT-specific threats coupled with their unique characteristics, undoubtedly require to be designed and integrated into firmware development cycles to contribute to securing IoT devices.

This survey and the initial empirical exploration presents a solid foundation for future research efforts. To this end, we foresee a number of future initiatives as briefed in this survey, including, exploring diverse strategies which aim at inferring malicious IoT devices in a large-scale for prompt remediation, empirical studies to investigate and characterize the generated traffic of such compromised IoT devices and formal attribution methodologies which would generate insightful inferences related to the causes and intentions of such Internet-wide IoT exploitations.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude in advance to the anonymous reviewers and editors for their constructive feedback. This work was supported by grants from the U.S. National Science Foundation (NSF) (Office of Advanced Cyberinfrastructure (OAC) #1755179 and #1541352).

REFERENCES

[1] M. C. Domingo, "An overview of the internet of things for people with disabilities," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 584–596, 2012.

[2] M. Chan, D. Estève, J.-Y. Fourniols, C. Escriba, and E. Campo, "Smart wearable systems: Current status and future challenges," *Artificial intelligence in medicine*, vol. 56, no. 3, pp. 137–156, 2012.

[3] A. G. Ferreira, D. Fernandes, S. Branco, J. L. Monteiro, J. Cabral, A. P. Catarino, and A. M. Rocha, "A smart wearable system for sudden infant death syndrome monitoring," in *Industrial Technology (ICIT), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1920–1925.

[4] I. Bisio, A. Delfino, F. Lavagetto, and A. Sciarrone, "Enabling iot for in-home rehabilitation: Accelerometer signals classification methods for activity and movement recognition," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 135–146, 2017.

[5] "The autism glass project at stanford medicine," http://autismglass.stanford.edu/.

[6] "Autism glass takes top student health tech prize," https://www.scientificamerican.com/article/autism-glass-takes-top-student-health-tech-prize-slide-show1/.

[7] R. Coppola and M. Morisio, "Connected car: technologies, issues, future trends," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, p. 46, 2016.

[8] "Internet of things applications part 2: The mining industry," https://centricdigital.com/blog/digital-trends/internet-of-things-applications-pt2-the-mining-industry/.

[9] "Smart cities - international case studies," http://www.iadb.org/en/topics/emerging-and-sustainable-cities/international-case-studies-of-smart-cities,20271.html.

[10] M. Stanislav and T. Beardsley, "Hacking iot: A case study on baby monitor exposures and vulnerabilities," *Rapid 7*, 2015.

[11] "How this internet of things stuffed animal can be remotely turned into a spy device," https://motherboard.vice.com/en_us/article/qkm48b/how-this-internet-of-things-teddy-bear-can-be-remotely-turned-into-a-spy-device.

[12] "Internet of things teddy bear leaked 2 million parent and kids message recordings," https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings.

[13] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[14] B. Herzberg, D. Bekerman, and I. Zifman, "Breaking down mirai: An iot ddos botnet analysis," https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html, october, 2016.

[15] "Financial impact of mirai ddos attack on dyn revealed in new data," https://www.corero.com/blog/797-financial-impact-of-mirai-ddos-attack-on-dyn-revealed-in-new-data.html.

[16] U. Food and D. Administration, "Cybersecurity vulnerabilities identified in st. jude medical's implantable cardiac devices and merlin@home transmitter: Fda safety communication," https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm, january, 2017.

[17] M. Prigg, "How to get green lights all the way to work: Hackers reveal how simple it is to control traffic lights in major cities using just a laptop," http://www.dailymail.co.uk/sciencetech/article-2730096/How-green-lights-way-work-Hackers-reveal-simple-control-traffic-lights-major-cities-using-just-laptop.html, august, 2014.

[18] C. McGoogan, "Bmw, audi and toyota cars can be unlocked and started with hacked radios," http://www.telegraph.co.uk/technology/2016/03/23/hackers-can-unlock-and-start-dozens-of-high-end-cars-through-the/, april, 2016.

[19] T. Guardian, "Team of hackers take remote control of tesla model s from 12 miles away," https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes, september, 2016.

[20] Canonical Ltd, "Who should bear the cost of iot security: consumers or vendors?" https://insights.ubuntu.com/2017/02/07/who-should-bear-the-cost-of-iot-security-consumers-or-vendors/.

[21] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. ACM, 2015, p. 5.

[22] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[23] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[24] Y. Wei, K. Sukumar, C. Vecchiola, D. Karunamoorthy, and R. Buyya, "Aneka cloud application platform and its integration with windows azure," *arXiv preprint arXiv:1103.2590*, 2011.

[25] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[26] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[27] L. Atzori, A. Iera, and G. Morabito, "Understanding the internet of things: definition, potentials, and societal role of a fast evolving paradigm," *Ad Hoc Networks*, 2016.

[28] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[29] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[30] A. M. Nia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*.

[31] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE*

Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

[32] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[33] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[34] R. H. Weber and E. Studer, "Cybersecurity in the internet of things: Legal aspects," *Computer Law & Security Review*, vol. 32, no. 5, pp. 715–728, 2016.

[35] N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K. Chen, Y. Tian *et al.*, "Understanding iot security through the data crystal ball: Where we are now and where we are going to be," *arXiv preprint arXiv:1703.09809*, 2017.

[36] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, 2017.

[37] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things," in *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*. IEEE, 2016, pp. 84–90.

[38] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in i nternet of things," *Journal of Network and Computer Applications*, 2017.

[39] CISCO, "The internet of things reference model," http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf, 2014.

[40] Z. Shelby and C. Bormann, *6LoWPAN: The wireless embedded Internet*. John Wiley & Sons, 2011, vol. 43.

[41] "Top 10 iot vulnerabilities (2014)," https://www.owasp.org/index.php/Top_IoT_Vulnerabilities.

[42] "Iot security part 3 (101 iot top ten vulnerabilities)," https://payatu.com/iot-security-part-3-101-iot-top-ten-vulnerabilities/.

[43] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (iot) security: Current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015, pp. 336–341.

[44] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial iot devices," in *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*. IEEE, 2016, pp. 519–524.

[45] B. Ur, J. Jung, and S. Schechter, "The current state of access control for smart devices in homes," in *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014, 2013.

[46] C. Schuett, J. Butts, and S. Dunlap, "An evaluation of modification attacks on programmable logic controllers," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 1, pp. 61–68, 2014.

[47] M. Qabulio, Y. A. Malkani, and A. Keerio, "A framework for securing mobile wireless sensor networks against physical attacks," in *Emerging Technologies (ICET), 2016 International Conference on*. IEEE, 2016, pp. 1–6.

[48] M. Smache, N. El Mrabet, J.-J. Gilquijano, A. Tria, E. Riou, and C. Gregory, "Modeling a node capture attack in a secure wireless sensor networks," in *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. IEEE, 2016, pp. 188–193.

[49] J. Zhao, "On resilience and connectivity of secure wireless sensor networks under node capture attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 557–571, 2017.

[50] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 14–21, 2015.

[51] D. G. Costa, I. Silva, L. A. Guedes, F. Vasques, and P. Portugal, "Availability issues in wireless visual sensor networks," *Sensors*, vol. 14, no. 2, pp. 2795–2821, 2014.

[52] A. A. Patel and S. J. Soni, "A novel proposal for defending against vampire attack in wsn," in *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference on*. IEEE, 2015, pp. 624–627.

[53] E. Y. Vasserman and N. Hopper, "Vampire attacks: draining life from wireless ad hoc sensor networks," *IEEE transactions on mobile computing*, vol. 12, no. 2, pp. 318–332, 2013.

[54] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen, "Security threats in zigbee-enabled systems: vulnerability evaluation, practical experiments, countermeasures, and lessons learned," in *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE, 2013, pp. 5132–5138.

[55] P. Morgner, S. Mattejat, and Z. Benenson, "All your bulbs are belong to us: Investigating the current state of security in connected lighting systems," *arXiv preprint arXiv:1608.03732*, 2016.

[56] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "Dtls based security and two-way authentication for the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, 2013.

[57] I. Hafeez, A. Y. Ding, L. Suomalainen, A. Kirichenko, and S. Tarkoma, "Securebox: Toward safer and smarter iot networks," in *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*. ACM, 2016, pp. 55–60.

[58] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications," *International Journal of Distributed Sensor Networks*, 2014.

[59] A. Furfaro, L. Argento, A. Parise, and A. Piccolo, "Using virtual environments for the assessment of cybersecurity issues in iot scenarios," *Simulation Modelling Practice and Theory*, vol. 73, pp. 43–54, 2017.

[60] E. Ronen and A. Shamir, "Extended functionality attacks on iot devices: The case of smart lights," in *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*. IEEE, 2016, pp. 3–12.

[61] V. Sachidananda, S. Siboni, A. Shabtai, J. Toh, S. Bhairav, and Y. Elovici, "Let the cat out of the bag: A holistic approach towards security analysis of the internet of things," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*. ACM, 2017, pp. 3–10.

[62] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Talos: Encrypted query processing for the internet of things," in *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2015, pp. 197–210.

[63] B. Wei, G. Liao, W. Li, and Z. Gong, "A practical one-time file encryption protocol for iot devices," in *Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on*, vol. 2. IEEE, 2017, pp. 114–119.

[64] A. Biryukov, D. Dinu, and Y. Le Corre, "Side-channel attacks meet secure network protocols," in *International Conference on Applied Cryptography and Network Security*. Springer, 2017, pp. 435–454.

[65] S. Siboni, A. Shabtai, N. O. Tippenhauer, J. Lee, and Y. Elovici, "Advanced security testbed framework for wearable iot devices," *ACM Transactions on Internet Technology (TOIT)*, vol. 16, no. 4, p. 26, 2016.

[66] K. Angrishi, "Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets," *arXiv preprint arXiv:1702.03681*, 2017.

[67] H. P. Enterprise, "Internet of things research study," *Internet of Things Research Study*, 2015.

[68] L. Markowsky and G. Markowsky, "Scanning for vulnerable devices in the internet of things," in *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2015 IEEE 8th International Conference on*, vol. 1. IEEE, 2015, pp. 463–467.

[69] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for iot services," *Journal of Information Security and Applications*, 2017.

[70] Y. J. Jia, Q. A. Chen, S. Wang, A. Rahmati, E. Fernandes, Z. M. Mao, A. Prakash, and S. J. Unviersity, "Contexiot: Towards providing contextual integrity to appified iot platforms," To appearin The Network and Distributed System Security Symposium (NDSS), 2017.

[71] A. Tekeoglu and A. Ş. Tosun, "A testbed for security and privacy analysis of iot devices," in *Mobile Ad Hoc and Sensor Systems (MASS), 2016 IEEE 13th International Conference on*. IEEE, 2016, pp. 343–348.

[72] "brickerbot results in pdos attack," https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/.

[73] Z. Basnight, J. Butts, J. Lopez, and T. Dube, "Firmware modification attacks on programmable logic controllers," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 76–84, 2013.

[74] A. Cui, M. Costello, and S. J. Stolfo, "When firmware modifications attack: A case study of embedded exploitation." in *NDSS*, 2013.

[75] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Nov 2015, pp. 283–288.

[76] B. Bencsáth, L. Buttyán, and T. Paulik, "Xcs based hidden firmware modification on embedded devices," in *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*. IEEE, 2011, pp. 1–5.

[77] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, and S. Antipolis, "A large-scale analysis of the security of embedded firmwares." in *USENIX Security*, 2014, pp. 95–110.

[78] Q. Feng, R. Zhou, C. Xu, Y. Cheng, B. Testa, and H. Yin, "Scalable graph-based bug search for firmware images," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 480–491.

[79] H. Elmiligi, F. Gebali, and M. W. El-Kharashi, "Multi-dimensional analysis of embedded systems security," *Microprocessors and Microsystems*, vol. 41, pp. 29–36, 2016.

[80] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity internet of things devices," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 2016, pp. 461–472.

[81] K. Yang, D. Forte, and M. M. Tehranipoor, "Protecting endpoint devices in iot supply chain," in *Computer-Aided Design (ICCAD), 2015 IEEE/ACM International Conference on*. IEEE, 2015, pp. 351–356.

[82] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[83] N. E. Petroulakis, E. Z. Tragos, A. G. Fragkiadakis, and G. Spanoudakis, "A lightweight framework for secure life-logging in smart environments," *Information Security Technical Report*, vol. 17, no. 3, pp. 58–70, 2013.

[84] M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," *Computer Communications*, 2016.

[85] J. Czyz, M. J. Luckie, M. Allman, and M. Bailey, "Don't forget to lock the back door! a characterization of ipv6 network security policy." in *NDSS*, 2016.

[86] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker, and H. Chen, "Uninvited connections: a study of vulnerable devices on the internet of things (iot)," in *Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint*. IEEE, 2014, pp. 232–235.

[87] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 97–106.

[88] C. Konstantinou and M. Maniatakos, "Impact of firmware modification attacks on power systems field devices," in *Smart Grid Communications (SmartGridComm), 2015 IEEE International Conference on*. IEEE, 2015, pp. 283–288.

[89] B. Copos, K. Levitt, M. Bishop, and J. Rowe, "Is anybody home? inferring activity from smart home network traffic," in *Security and Privacy Workshops (SPW), 2016 IEEE*. IEEE, 2016, pp. 245–251.

[90] H. Wang, T. T.-T. Lai, and R. Roy Choudhury, "Mole: Motion leaks through smartwatch sensors," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 2015, pp. 155–166.

[91] C. Wang, X. Guo, Y. Wang, Y. Chen, and B. Liu, "Friend or foe?: Your wearable devices reveal your personal pin," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 2016, pp. 189–200.

[92] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure." *WOOT*, vol. 14, pp. 7–7, 2014.

[93] A. Tekeoglu and A. S. Tosun, "Investigating security and privacy of a cloud-based wireless ip camera: Netcam," in *Computer Communication and Networks (ICCCN), 2015 24th International Conference on*. IEEE, 2015, pp. 1–6.

[94] "Brickerbot permanent denial-of-service attack (update a)," https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A.

[95] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," 2017.

[96] C. OFlynn and Z. Chen, "Power analysis attacks against ieee 802.15. 4 nodes," in *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Springer, 2016, pp. 55–70.

[97] A. Rajan, J. Jithish, and S. Sankaran, "Sybil attack in iot: Modelling and defenses," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Sept 2017, pp. 2323–2327.

[98] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[99] X. Liu, Z. Bao, D. Lu, and Z. Li, "Modeling of local false data injection attacks with reduced network information," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1686–1696, 2015.

[100] T. Bonaci, L. Bushnell, and R. Poovendran, "Node capture attacks in wireless sensor networks: A system theoretic approach," in *Decision and Control (CDC), 2010 49th IEEE Conference on*. IEEE, 2010, pp. 6765–6772.

[101] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 794326, 2013.

[102] C. Pielli, F. Chiariotti, N. Laurenti, A. Zanella, and M. Zorzi, "A game-theoretic analysis of energy-depleting jamming attacks," in *2017 International Conference on Computing, Networking and Communications (ICNC)*, Jan 2017, pp. 100–104.

[103] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–5.

[104] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*. IEEE, 2014, pp. 205–211.

[105] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for iot systems," in *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*. ACM, 2015, pp. 37–42.

[106] C.-S. Park, "A secure and efficient ecqv implicit certificate issuance protocol for the internet of things applications," *IEEE Sensors Journal*, 2016.

[107] O. Garcia-Morchon, S. L. Keoh, S. Kumar, P. Moreno-Sanchez, F. Vidal-Meca, and J. H. Ziegeldorf, "Securing the ip-based internet of things with hip and dtls," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 2013, pp. 119–124.

[108] M. Rostami, A. Juels, and F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 1099–1112.

[109] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward end-to-end biometrics-based security for iot infrastructure," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 44–51, 2016.

[110] Z. Guo, N. Karimian, M. M. Tehranipoor, and D. Forte, "Hardware security meets biometrics for the age of iot," in *Circuits and Systems (ISCAS), 2016 IEEE International Symposium on*. IEEE, 2016, pp. 1318–1321.

[111] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, "Flowfence: Practical data protection for emerging iot application frameworks," in *USENIX Security Symposium*, 2016.

[112] A. Costin, A. Zarras, and A. Francillon, "Automated dynamic firmware analysis at scale: a case study on embedded web interfaces," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ACM, 2016, pp. 437–448.

[113] C. Li, A. Raghunathan, and N. K. Jha, "Improving the trustworthiness of medical device software with formal verification methods," *IEEE Embedded Systems Letters*, vol. 5, no. 3, pp. 50–53, 2013.

[114] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti, "Avatar: A framework to support dynamic security analysis of embedded systems' firmwares." in *NDSS*, 2014.

[115] C. Zhang, Y. Zhang, and Y. Fang, "Defending against physical destruction attacks on wireless sensor networks," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*. IEEE, 2006, pp. 1–7.

[116] V. R. Rao and A. Kumar KM, "Predictive node expiration based energy-aware source routing (pneb esr) protocol for wireless sensor networks," in *Proceedings of the 7th ACM India Computing Conference*. ACM, 2014, p. 14.

[117] G. Glissa and A. Meddeb, "6lowpan multi-layered security protocol based on ieee 802.15. 4 security features," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017, pp. 264–269.

[118] H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, "Secure sharing of partially homomorphic encrypted iot data," in *Proceedings of the 15th ACM Conference on Embedded Network Sensor System*. ACM, 2017.

[119] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare internet-of-things," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2017.

[120] B. Reaves and T. Morris, "An open virtual testbed for industrial control system security research," *International Journal of Information Security*, vol. 11, no. 4, pp. 215–229, 2012.

[121] A. Lahmadi, C. Brandin, and O. Festor, "A testing framework for discovering vulnerabilities in 6lowpan networks," in *Distributed Computing in Sensor Systems (DCOSS), 2012 IEEE 8th International Conference on*. IEEE, 2012, pp. 335–340.

[122] B. Cui, S. Liang, S. Chen, B. Zhao, and X. Liang, "A novel fuzzing method for zigbee based on finite state machine," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, p. 762891, 2014.

[123] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "Iotpot: A novel honeypot for revealing current iot threats," *Journal of Information Processing*, vol. 24, no. 3, pp. 522–533, 2016.

[124] J. Guarnizo, A. Tambe, S. S. Bunia, M. Ochoa, N. Tippenhauer, A. Shabtai, and Y. Elovici, "Siphon: Towards scalable high-interaction physical honeypots," *arXiv preprint arXiv:1701.02446*, 2017.

[125] E. Vasilomanolakis, S. Srinivasa, C. G. Cordero, and M. Mühlhäuser, "Multi-stage attack detection and signature generation with ics honeypots," in *IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies (DISSECT). IEEE*, 2016.

[126] D. I. Buza, F. Juhász, G. Miru, M. Félegyházi, and T. Holczer, "Cryplh: Protecting smart energy systems from targeted attacks with a plc honeypot," in *International Workshop on Smart Grid Security*. Springer, 2014, pp. 181–192.

[127] S. Litchfield, D. Formby, J. Rogers, S. Meliopoulos, and R. Beyah, "Rethinking the honeypot for cyber-physical systems," *IEEE Internet Computing*, vol. 20, no. 5, pp. 9–17, 2016.

[128] S. Dowling, M. Schukat, and H. Melvin, "A zigbee honeypot to assess iot cyberattack behaviour," in *Signals and Systems Conference (ISSC), 2017 28th Irish*. IEEE, 2017, pp. 1–6.

[129] C. Fachkha, E. Bou-Harb, A. Keliris, N. Memon, and M. Ahamad, "Internet-scale probing of cps: Inference, characterization and orchestration analysis," in *Proceedings of NDSS*, vol. 17, 2017.

[130] M. Galluscio, N. Neshenko, E. Bou-Harb, Y. Huang, N. Ghani, J. Crichigno, and G. Kaddoum, "A first empirical look on internet-scale exploitations of iot devices," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–7.

[131] Shodan, http://shodan.io.

[132] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, "A search engine backed by internet-wide scanning," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 542–553.

[133] Y. Meidan, M. Bohadana, A. Shabtai, J. D. Guarnizo, M. Ochoa, N. O. Tippenhauer, and Y. Elovici, "Profiliot: A machine learning approach for iot device identification based on network traffic analysis," 2017.

[134] D. Formby, P. Srinivasan, A. Leonard, J. Rogers, and R. Beyah, "Whos in control of your control system? device fingerprinting for cyber-physical systems," in *Network and Distributed System Security Symposium (NDSS)*, 2016.

[135] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, "Youve got vulnerability: Exploring effective vulnerability notifications," in *USENIX Security Symposium (Aug. 2016)*, 2016.

[136] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

[137] D. Shreenivas, S. Raza, and T. Voigt, "Intrusion detection in the rpl-connected 6lowpan networks," in *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*. ACM, 2017, pp. 31–38.

[138] L. Yang, C. Ding, M. Wu, and K. Wang, "Robust detection of false data injection attacks for the data aggregation in internet of things based environmental surveillance," *Computer Networks*, 2017.

[139] N. K. Thanigaivelan, E. Nigussie, R. K. Kanth, S. Virtanen, and J. Isoaho, "Distributed internal anomaly detection system for internet-of-things," in *Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual*. IEEE, 2016, pp. 319–320.

[140] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005, pp. 49–63.

[141] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach," *Computer Communications*, vol. 98, pp. 52–71, 2017.

[142] D. Midi, A. Rullo, A. Mudgerikar, and E. Bertino, "Kalisa system for knowledge-driven adaptable intrusion detection for the internet of things," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 656–666.

[143] S. Farahani, *ZigBee wireless networks and transceivers*. newnes, 2011.

[144] A. Elahi and A. Gschwender, *ZigBee wireless sensor and control network*. Pearson Education, 2009.

[145] P. Radmand, M. Domingo, J. Singh, J. Arnedo, A. Talevski, S. Petersen, and S. Carlsen, "Zigbee/zigbee pro security assessment based on compromised cryptographic keys," in *P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on*. IEEE, 2010, pp. 465–470.

[146] A. P. Sarr, P. Elbaz-Vincent, and J.-C. Bajard, "A new security model for authenticated key agreement," in *International Conference on Security and Cryptography for Networks*. Springer, 2010, pp. 219–234.

[147] Anonymous, "Internet census 2012: Port scanning/0 using insecure embedded devices," *URL http://internetcensus2012.bitbucket.org/paper.html*, 2012.

[148] Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman, "Analysis of the https certificate ecosystem," in *Proceedings of the 2013 conference on Internet measurement conference*. ACM, 2013, pp. 291–304.

[149] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing." *IACR Cryptology ePrint Archive*, vol. 2005, p. 388, 2005.

[150] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, 2017.

[151] "Baby monitor hacker delivers creepy message to child," https://www.cbsnews.com/news/baby-monitor-hacker-delivers-creepy-message-to-child/.

[152] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM, 2002, pp. 41–47.

[153] https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.

[154] A. Dunkels, O. Schmidt, N. Finne, J. Eriksson, F. Österlind, N. Tsiftes, and M. Durvy, "The contiki os: The operating system for the internet of things," *Online], at http://www. contikios. org*, 2011.

[155] F. Osterlind, "A sensor network simulator for the contiki os," *Swedish Institute of Computer Science (SICS), Tech. Rep. T2006-05*, 2006.

[156] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2012.

[157] M. Campagna, "Sec 4: Elliptic curve qu-vanstone implicit certificate scheme (ecqv)," *vol*, vol. 4, p. 32, 2013.

[158] T. Aura, "Cryptographically generated addresses (cga)," 2005.

[159] A. F. Molisch, K. Balakrishnan, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, "Ieee 802.15. 4a channel model-final report," *IEEE P802*, vol. 15, no. 04, p. 0662, 2004.

[160] R. Moskowitz, T. Heer, P. Jokela, and T. Henderson, "Host identity protocol version 2 (hipv2)," Tech. Rep., 2015.

[161] BullGuard, http://www.dojo-labs.com/.

[162] CUJO, https://www.getcujo.com/.

[163] "Rattrap," https://www.myrattrap.com/.

[164] Luma, https://lumahome.com/.

[165] "Arachni. web application security scanner framework," http://www.arachni-scanner.com/.

[166] "Owasp zed attack proxy project," https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

[167] "w3af - open source web application security scanner," www.w3af.org.

[168] C. Mellon, "Cbmc. bounded model checking for software," http://www.cprover.org/cbmc/.

[169] J. E. Forrester and B. P. Miller, "An empirical study of the robustness of windows nt applications using random testing," in *Proceedings of the 4th USENIX Windows System Symposium*. Seattle, 2000, pp. 59–68.

[170] "Kippo - ssh honeypot," https://github.com/desaster/kippo.

[171] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Hey, you have a problem: On the feasibility of large-scale web vulnerability notification," in *USENIX Security Symposium (Aug. 2016)*, 2016.

[172] F. Li, G. Ho, E. Kuan, Y. Niu, L. Ballard, K. Thomas, E. Bursztein, and V. Paxson, "Remedying web hijacking: Notification effectiveness and webmaster comprehension," in *Proceedings of the 25th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2016, pp. 1009–1019.

[173] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016.

[174] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing iot data," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb 2018, pp. 51–55.

[175] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the internet of things," in *2018 10th International Conference on Communication Systems Networks (COMSNETS)*, Jan 2018, pp. 561–564.

[176] O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, April 2018.

[177] K. Kataoka, S. Gangwar, and P. Podili, "Trust list: Internet-wide and distributed iot traffic management using blockchain and sdn," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Feb 2018, pp. 296–301.

[178] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, Feb 2018.

[179] A. Azmoodeh, A. Dehghantanha, and K. K. R. Choo, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," *IEEE Transactions on Sustainable Computing*, pp. 1–1, 2018.

[180] Y. Liu, Y. Kuang, Y. Xiao, and G. Xu, "Sdn-based data transfer security for internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 257–268, Feb 2018.

[181] W. Wang, P. Xu, and L. T. Yang, "Secure data collection, storage and access in cloud-assisted iot," *IEEE Cloud Computing*, pp. 1–1, 2018.

[182] J. He, Y. Zhang, J. Lu, M. Wu, and F. Huang, "Block-stream as a service: A more secure, nimble, and dynamically balanced cloud service model for ambient computing," *IEEE Network*, vol. 32, no. 1, pp. 126–132, Jan 2018.

[183] O. Day and T. M. Khoshgoftaar, "A survey on heterogeneous transfer learning," *Journal of Big Data*, vol. 4, no. 1, p. 29, 2017.

[184] "2017 study on mobile and iot application security," https://www.arxan.com/wp-content/uploads/2017/01/2017_Security_IoT_Mobile_Study.pdf.

[185] L. Atzori, A. Iera, and G. Morabito, "From "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things," *IEEE Communications Magazine*, vol. 52, no. 1, pp. 97–105, 2014.