Towards an Extensible IoT Security Taxonomy

Lars Wüstrich*, Marc-Oliver Pahl‡*, Stefan Liebald*
*Technical University of Munich, ‡IMT Atlantique
*{wuestrich,pahl,liebald}@s2o.net.in.tum.de; ‡ marc-oliver.pahl@imt-atlantique.fr

***Abstract*—Security is essential in the Internet of Things (IoT). IoT threat classifications are often non-intuitive to use. Identifying relevant properties of an attack is difficult and requires reading details of the attack. We therefore propose a simple-to-use naming scheme for IoT threat classification. It is based on the affected layers and the affected security goals. We evaluate the usefulness of the chosen approach by applying it to common IoT threats.**

***Index Terms*—IoT, security, cyber-physical systems, attacks, threat classification, naming scheme, taxonomy**

I. Introduction

The Internet of Things (IoT) consists of collaborating distributed heterogeneous devices. These devices are connected over a network. The devices run software that is connected with other software to implement complex scenarios [1].

The IoT has many different application scenarios, ranging from smart consumer devices that monitor their activities to large networked control systems [2]. In real-world settings often privacy- or safety-critical information such as personalized location data is involved. Especially in industrial settings, security breaches can endanger human lives [3]. It is therefore necessary to secure IoT systems.

Security taxonomies enable a consistent labeling of attacks and threats. They enable classifying attacks and evaluating attack mitigation strategies. Previously proposed IoT threat taxonomies are either ambiguous or cover the IoT only partially. Security taxonomies for computer systems miss the cyber-physical aspects of IoT systems.

This paper proposes an extensible IoT threat taxonomy based on two fundamental building blocks: the attacked architectural IoT layer and fundamental security principles. The taxonomy enables classifying and comparing different IoT attacks with regards to violated security goals and functionalities.

We combine properties into a naming scheme that makes it easier to use than other categorizations and standards like CWE or CAPEC-IDs [4], [5]. The proposed naming scheme enables an accurate description of threats. It is designed for systematic extension. New threats can therefore simply be added.

The IoT architecture can be categorized into three layers with different tasks [6], [7]. The first layer is the (1) *cyber-physical layer* in which the environment is sensed and actuated. Devices on the cyber-physical layer are connected through a (2) *middleware layer*. It handles addressing and transport of information. It connects the devices to the (3) *application layer* on which the gathered information is collected and processed for decision making.

Fundamental security goals are availability, confidentiality, authenticity, accountability, integrity and access control. They can be violated on each of the three layers.

Attacks are only carried out on a single layer [6]. However, the success of an attack on one layer can impact the security goals on the other layers. Depending on the attack, an adversary needs different levels of knowledge and different capabilities to be successful [8], [9].

The rest of the paper is structured as follows. After introducing related work in Section II, Section III introduces the layered structure of the IoT. This section also gives an overview of the security goals and attacker models for the IoT. The new taxonomy is introduced in Section IV and used to classify selected attacks on each of the IoT layers in Section V. Section VI evaluates the taxonomy.

II. Related Work

Diverse taxonomies for the IoT exist.

Like this work, most taxonomies split the IoT into functional layers. [6], [10], [11] and [7] split the architecture in a perception/physical, network and application layer.

[6] classifies attacks using these layers. The paper introduces additionally so-called encryption attacks to classify confidentiality attacks. They are independent from the layer. This extension indicates that solely relying on the abstraction of the functionality of the different layers is not enough to classify attacks. The IoT architecture is only one aspect considered in [7]. The authors also use threat vector, trust and compliance as categories. The purpose of each category varies strongly, making it hard to use. Attacks on the IoT cannot be explicitly classified as they can be assigned to multiple classes. This makes it difficult to provide a clean overview of IoT security, and to compare different attacks. Our taxonomy solves this problem by providing unified subdomains for each layer.

The authors of [11], [12] give an overview of IoT security. In addition to confidentiality, integrity and availability, they discuss general issues for the IoT like the heterogeneity of devices on the perception layer. The authors do not come up with a proposal for classifying IoT security threats.

[10] only considers attacks on RFID systems. Another scope-limited overview of attack models on cyber-physical systems is given in [9]. The authors define an attack-space

Funded by the German Federal Ministry of Economic Affairs and Energy (BMWi) DECENT (0350024A) and the German-French Academy SCHEIF.

978-1-7281-8086-1/20/$31.00 ©2020 IEEE

for networked systems and classify attacks depending on an attacker's system knowledge and the available resources.

A holistic overview of IoT security is given in [13]–[15]. These also make use of the layers but define security goals that are not standard.

A different way of classifying attacks is [16]. Instead of layers the authors categorize by the type of device utilization and functionality, i.e. reducing, misusing or extending it to the adversary's benefit. Even though this type of classification is possible, it is not concise with regards to an attack's effects on the IoT security.

Finally, different surveys focus on different aspects of IoT security [8], [17]–[21]. [18] focuses on the security of commonly used IoT frameworks like Azure IoT or AWS IoT with regards to authenticity, access control and confidentiality. More focused on the constraints of computing power and power supply, [19] explores different schemes for authenticity on the middleware layer. The survey conducted in [20] solely focuses on trust in the IoT. It defines specific categories that can be used to assess trust in various ways and evaluate its establishment in different frameworks. [8] focuses on different attacker types and threats to critical infrastructures and services. The authors classify different characteristics of an adversary with regards to access and capabilities. They provide a threat assessment regarding risk, affected layers, and required attacker capabilities on networked systems. The lack of security goals prevents assessing how the security of an attacked systems is affected.

A taxonomy created for threats on the web ecosystem [22] uses security goals for a fine granular classification of attacks. Developed for the web it is missing the cyber-physical aspect of the IoT. [23] introduces a taxonomy for attacker models for cyber-physical systems. It considers different types of attacks on cyber-physical systems to assess available attacker actions.

The presented works are either ambiguous, or incomplete, or hard to use with regards to the whole IoT environment. This makes it hard to compare and classify attacks and solutions. Our proposed taxonomy covers the whole IoT domain along with commonly used security goals. It provides a concise way to categorize threats while remaining easy to use.

III. IoT structure, security goals, and attacker types

A. The IoT Structure

The IoT can be structured into three layers with distinct tasks [11][6][7]:

1) cyber-physical (CP) layer,
2) middleware (MW) layer, and
3) application (APP) layer.

The lowest *cyber-physical layer* represents sensors and actuators used to interact with the physical world. Devices on this layer do not implement complex application workflows. They are often limited in computation power and resources [24].

The *middleware layer* on top of the CP layer provides connectivity. Transport and addressing of information between different IoT devices are often simplified by a middleware that helps to connect devices from different manufacturers [1]. Middleware offers a unified interface to the application layer [25].

The third *application layer*. is responsible for collecting and processing data from CP layer devices. It comprises complex IoT workflows. Therefore, devices working on the application layer are equipped with more resources than the devices on the CP layer [24].

Not all IoT devices implement all three layers. However, all are connected through the MW layer. A sensor could e.g. only work on the CP and MW layers. Other devices might not be able to interact with their environment directly but are used to process the collected data and make decisions. They only operate on the MW and APP layers.

The layers form the first building block of our taxonomy. We use them to describe what is targeted by a specific attack.

The second building block becomes the attacked functionality of the IoT. We base it on commonly used security goals, further structuring the attack space according to commonly accepted security standards.

B. Security Goals

The security of a system can be assessed by analyzing how well it addresses relevant security goals. General goals are *availability*, *accountability*, *authenticity*, *integrity*, *confidentiality*, and *access control* [26], [27]. They are defined as follows:

Availability: A system is called available when it can assure that information and communications functionalities are always available when expected [28].

Accountability: A system is called accountable if it removes the option of plausible deniability for actions [26].

Authenticity: An authentic system assures that all entities are credible and trustworthy. This can be verified by using an identity and other characteristics of entities [26].

Integrity: Integrity assures that information is not accidentally or maliciously altered without notice [28].

Confidentiality: A system is called confidential when information is only disclosed to appropriate entities and processes [28].

Access Control: Access control ensures that only authorized entities can access protected resources [29].

Ensuring IoT security requires addressing security goals on all three layers introduced in Sec. III-A. If some security goals are missed, adversaries can manipulate a system. The different tasks and limitations of each layer's entities limits the usable security mechanisms to achieve a security goal [24].

C. Attacker model

Besides affected layer and attacked security goal, we can distinguish different attacker models. Attack-specific, an adversary needs different *capabilities* and *knowledge* about the targeted IoT system. These capabilities can be categorized into (1) the *level of access*, and (2) *resources available* [8].

The level of access describes the physical or logical IoT parts an adversary requires access. We distinguish between three different access levels: (1) *physical access* (2) *remote access* (3) *both*.

Depending on the level of access, the adversary can execute different types of operations. An example is the monitoring of power consumption for executing a side channel attack. An attacker can have a global view or only observe a part.

Attacks can be categorized as *passive* or *active*. In passive attacks, attackers do not influence the targeted entity but only observe. An active attack requires influencing a system [30].

Some attacks require varying levels of *insider knowledge* about a system. This includes used protocols, devices, and device resources. Insider knowledge facilitates targeting specific IoT parts. *Without* system knowledge an adversary can only perform basic attacks like cutting cables, damaging devices or replaying messages. *Basic* system knowledge, e.g. insights on protocols, enables aiming efforts towards exploiting specific vulnerabilities. *Advanced* knowledge, e.g. known communication patterns, enables developing and executing highly sophisticated attacks that are specifically adapted towards a targeted environment.

D. Methodology

There are multiple factors that need to be considered when classifying IoT threats. Our taxonomy categorizes an attack by

- IoT layer,
- violated security goals,
- required attacker knowledge, and
- required attacker capabilities.

The taxonomy allows further sub-categorize attacks according to the violated security goals on each layer. This distinction makes it possible to accurately describe which parts of the IoT are targeted by an attack while remaining easy to use.

Another advantage of combining the layered model with the security goals on the respective layer is the capability to assess to which extend an attack affects the IoT. This makes it possible to compare attacks regarding violated goals and difficulty of execution regarding attacker prerequisites. Comparing the violated security goals on each layer as a result of the attack and its difficulty becomes simple.

The taxonomy can assess which security goals are maintained by different protocols and frameworks. The layers and security goals imply which goals are protected. This facilitates an overview of the state of IoT security as well as identifying shortcomings of existing solutions.

The taxonomy is structured as follows: The first part of the naming scheme uses the targeted layer, i.e. cyber-physical (CP), middleware (MW) and application (APP) layer. The second part uses the previously introduced security goals availability (AVAIL), accountability (ACC), authenticity (AUTH), integrity (INT), confidentiality (CONF) and access control (ACL) to specify the classes further.

IV. Naming Scheme

Our proposed taxonomy classifies an attack by combining the targeted layer and security goal. The target layer identifies which layer is affected by the attack:

- CP: Cyber-Physical
- MW: Middleware
- APP: Application

Attacks can affect security goals on multiple layers, but they are only executed on a single layer.

When looking not only at the execution but at the impact of an attack, this naming scheme can be used as well. In that case multiple layers can be affected.

The second used taxonomy characteristic in the identifier is the security goal:

- AVAIL: availability
- AUTH: authenticity
- ACC: accountability
- INT: integrity
- CONF: confidentiality
- ACL: access control

Following, we exemplify the taxonomy identifier use for the CP layer.

CP.AVAIL is used to denote attacks that target the goal of availability in CP. This category includes attacks that render devices on the CP layer unavailable. Examples are physical tampering and destruction of sensors, or the interference of signals used for data transmission.

Attacks aiming at the authenticity are classified with the AUTH tag. Impersonating a sensor, e.g. through RFID cloning, would therefore be classified as CP.AUTH.

For threats that target the accountability of a layer are classified in the ACC category. It includes threats that enable adversaries to issue commands to devices on the cyber-physical layer without any notice.

Attacks on the integrity of the IoT are classified by the INT category. CP.INT includes attacks like the manipulation of measured values of the different devices. The class of CONF is used for attacks on the confidentiality. This includes attacks on the cryptography used on the different layers. Side-channel attacks that e.g. analyze the power consumption of a device to extract secrets are also included in this class. Attacks on the access control are classified by ACL. This class includes attacks that enable the unauthorized use of resources.

Following this scheme, the resulting classes are CP.AVAIL, CP.AUTH, CP.ACC, CP.INT, CP.CONF and CP.ACL for the CP layers. The classes MW and APP have that same subclasses with the respective prefix.

Attacks violating multiple security goals can be classified by a combination of the categories. An attack that is classified as CP.ACC, CP.INT CP.AVAIL is the covert attack since it uses a combination of different attacks to succeed. Each of the used attacks can also be classified on their own.

This approach makes classifying IoT threats intuitive and easy. It highlights the affected layer, making it easy to assess the attacked part of the IoT.

V. Beginning a Threat Taxonomy

An attack is classified with regards to the targeted layer and security goal. In the following classify common attacks applying our taxonomy and naming scheme.

A. Attacks on the cyber-physical layer

Attacks on the cyber-physical layer (CP) target both, hard and software.The distribution of IoT devices in the environment facilitates adversary access.

1) **Replay Attacks**: In a replay attack [31], the adversary retransmits previously captured secured messages or signals. This can cause a device to change its state. To execute it, the adversary does not need extensive knowledge over the system [9]. Access to devices and the capability to record and replay a signal are sufficient for this attack. As the attacker then impersonates a legitimate sender, this attack is classified as CP.AUTH.
2) **Sleep Deprivation Attack**: This attack is targeted at battery-powered devices [6], [32], [33]. In order to save energy, some devices have a sleep mode. The attacker interacts with the device to prevent it from entering the low powered mode to drain its battery. This renders the device unavailable (CP.AVAIL). For a success, adversary needs network access to interact with the node. It also needs knowledge about the commands it can send to the node to keep it from the sleep mode.
3) **Physical attacks**: IoT devices embedded into the environment they can also be physically damaged [6]. The goal of the adversary is to render the device and its functionality unusable which violates the goal of availability (CP.AVAIL). The attacker does not need any prior knowledge about the system to succeed.
4) **Jamming Attacks**: There are various jamming attacks [34], [35] which create interference. Depending on the specific type of an attack, an attacker chooses to jam the wireless connection between the nodes in the network to make the communication between devices slow or impossible (CP.AVAIL).
5) **Covert Attack**: Another class of attacks on the CP are covert attacks. An example is the Stuxnet worm that was used to attack the Iranian nuclear program [36]. In the attack, adversary changes the input to the system and simultaneously manipulates the output of the system to keep the effects undetected [37]. The adversary needs extensive knowledge of the attacked system. Since this attack consists of multiple components, each of the component can be classified on each own. Parts that manipulate the input and output of the devices, are classified as CP.INT. Other parts issue commands on behalf of the controller which are classified as CP.ACC and finally damage the devices (CP.AVAIL). Depending on the goal of the covert attack, also other security goals are violated which can be additional categories for this attack. Resulting of this, the covert attack can be categorized by the combination of the attacked goals, i.e. CP.AVAIL,CP.INT,CP.ACC.
6) **Side Channel Attacks**: Another class of attacks that predominantly affects devices on CP due to their limited computing power and level of exposure are side channel attacks. Side channel attacks are used to extract the secret key that is used by the devices to encrypt and sign their data. By analyzing physical characteristics like power consumption of the device during computations the secret is inferred [38]. The adversary needs knowledge of the analyzed protocol and physical access to the device in order to execute the attack. This type of attack is classified as CP.CONF.
7) **Calibration Parameters Tampering**: Sensors and actuators are calibrated before they are deployed. An adversary that does calibration parameter tempering [39] is able to change the calibration of the devices to falsify the measurements. This violates the goal of integrity (CP.INT).

B. Attacks on the middleware layer

Attacks in MW target the transport of information as well as mechanisms provided by the middleware. Therefore this category contains attacks on the routing and addressing of information as well as attacks on features of the middleware.

1) **Sybil Attack**: In a Sybil attack, the adversary assumes multiple identities of other nodes in the network [40]. The attacker uses these identities to influence common decision-making of connected nodes in his favor. The attacker needs network access to perform the attack as well as knowledge over the decision-making protocols. Since the attacker can assume multiple identities this attack is classified by MW.AUTH.
2) **Denial of Service**: The denial of service attack targets the availability on the middleware layer (MW.AVAIL). There are several possibilities to execute this attack. One method is to flood the network with requests and traffic such that the nodes become unresponsive [41]. To execute the attack it is sufficient for the adversary to have network access. No further knowledge about the attacked system is required.
3) **Sinkhole Attack**: Another attack classified as MW.AVAIL is the sinkhole attack [42]. In this type of attack, the adversary attracts as much as traffic by as possible by exploiting the used routing protocol. It then decides how to proceed with the captured data, e.g. to it. For this type of attack, the attacker needs network access. It also requires knowledge about the used routing protocol to be able to exploit it. The sinkhole attack can additionally be classified as MW.INT since it enables the adversary also to manipulate the information it captures.
4) **Cryptanalysis**: When attacking the confidentiality on the middleware layer (MW.CONF), an adversary also has various attack vectors. In case the attacker has knowledge over the used cryptographic protocols it can take different efforts to extract the key through cryptanalysis. If it can intercept traffic and participate in the exchange of messages, it can also execute one of various man-in-the-middle (MitM) attacks [43]. There is also the possibility

to decrypt captured traffic by brute-forcing all possible keys.

Similar to the CP layer, the attacker can also use other side channels on the MW like timings to draw conclusions on secrets used to encrypt information. These attacks however, are not targeted at the hardware, but the software the runs the middleware.

C. Attacks on the application layer

Attacks on the application layer are aimed at disrupting services that collect and process the data. Due to the variety of applications there is no specific attack type on this layer but a class of attacks that can be executed.

1) **Phishing**: A class of attacks that violates the authenticity of the application layer (APP.AUTH) are phishing attacks [44]. In this attack the adversary assumes the identity to trick unknowing victims into giving them confidential information.
2) **DoS**: Similar to MW, an attacker can perform a DoS attack on the application layer to attack single or multiple applications of the IoT and render them unavailable (APP.AVAIL).
3) **Malicious Updates**: In case an attacker is able modify the running application by using malware, a Trojan horse or is able to install a malicious update, the integrity on the application layer is violated (APP.INT). In order to succeed, the attacker needs access to the network or to the source from which the software is installed. An example of such an attack can be found in [45].
4) **Cryptanalysis**: Similar to MW, an adversary can also use cryptanalysis to attack the encryption schemes used by the software running in APP. Analogously to MW, this attack is classified in the APP.CONF category.
5) **Privilege Escalation**: When an attacker can achieve privilege escalation it is able to extend its capabilities to use the systems functionality. This attack is classified as APP.ACL. It needs extensive knowledge over the used software and its internal functionality to elevate its privilege.

All attacks that were introduced can be seen classified by the taxonomy in Figure 1.

This list is far from complete. However, it exemplifies how all attacks can be classified. By combining the different layers and the fundamentals of security it can provide a complete overview of the domain. In case the taxonomy needs to be more fine-grained each of the security goal classes can further be divided into the needed categories. However, classifying new attacks can already be done by using this easy to use taxonomy as they also target one of the fundamental security goals.

VI. Evaluation

The introduced naming scheme makes use of fundamental properties of the IoT as well as basic security goals. By construction, this ensures versatile applicability of the naming

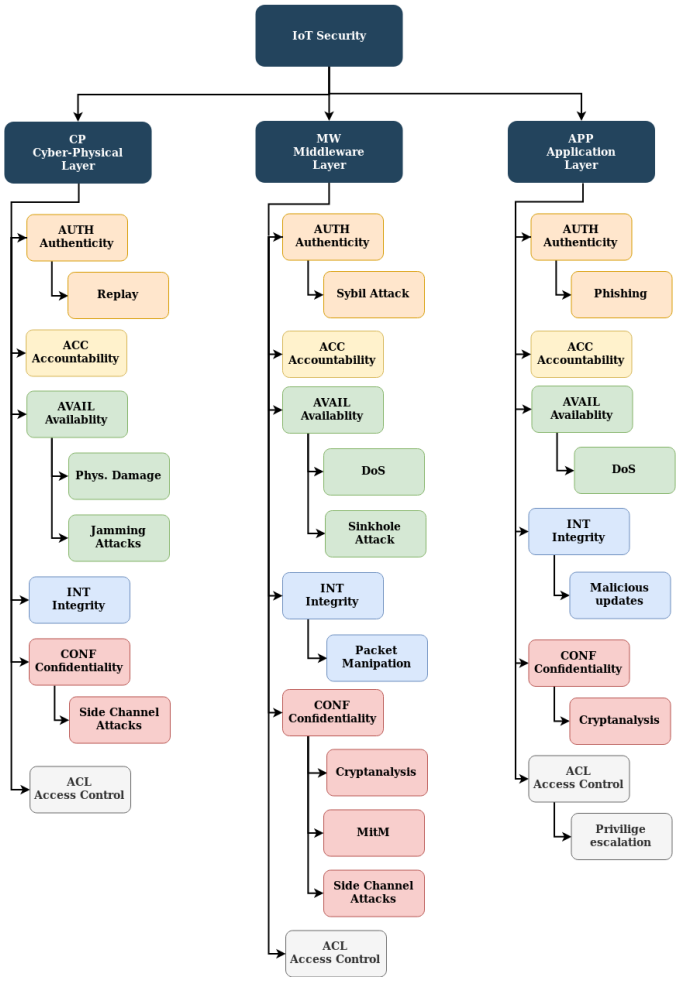

Fig. 1. The beginning of a threat taxonomy for the IoT using our naming scheme

scheme. More advanced security goals can be considered as a combination of standard goals. However, in order to validate our naming scheme, we compared the classification of existing taxonomies like [6], [7].

This comparison resulted in similar but more distinct classification of the different attacks. In general, our taxonomy results in a similar classification with the benefit of adding an easy to use and comparable naming scheme. Previous taxonomies like [6] required an additional class for encryption attacks that covered multiple layers of the IoT architecture. Therefore, our naming scheme gives more structure to the attack space. In addition, it is simple to use. This is not provided through the existing taxonomies or standards like CVE- or CAPEC-IDs [4], [5] where only numbers are used for classifying vulnerabilities and attack vectors.

VII. Conclusion

Security is essential in the IoT. Providing a simple-to-use naming scheme for security threats can help making the IoT more secure. Such a scheme was missing and is introduced by this paper. Our naming scheme is based on the affected

architectural layer and the attacked security properties. By-construction it is therefore able to classify any attack.

As next steps, we want to create a real threat taxonomy based-on the cited surveys using our taxonomy. We hope to provide a contribution towards more security-awareness in the important IoT domain.

REFERENCES

[1] M.-O. Pahl and S. Liebald, "Information-Centric IoT Middleware Overlay: VSL," in *2019 International Conference on Networked Systems (NetSys) (NetSys'19)*, Garching b. München, Germany, 2019.

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

[3] M. G. Angle, S. Madnick, J. L. Kirtley, and S. Khan, "Identifying and anticipating cyberattacks that could cause physical damage to industrial control systems," *IEEE Power and Energy Technology Systems Journal*, vol. 6, no. 4, pp. 172–182, 2019.

[4] R. A. Martin, "Common weakness enumeration," *Mitre Corporation*, 2007.

[5] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," *Technical report*, 2018.

[6] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 2015, pp. 180–187.

[7] S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the internet of things (iot): a security taxonomy for iot," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 163–168.

[8] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3453–3495, 2018.

[9] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 55–64.

[10] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of rfid attacks," *Gen*, vol. 15693, p. 14443, 2010.

[11] 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.

[12] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in internet of things," *Future Generation Computer Systems*, vol. 83, pp. 326–337, 2018.

[13] R. Uttarkar and R. Kulkarni, "Internet of things: architecture and security," *International Journal of Computer Application*, vol. 3, no. 4, pp. 12–19, 2014.

[14] L. Li, "Study on security architecture in the internet of things," in *Proceedings of 2012 International Conference on Measurement, Information and Control*, vol. 1. IEEE, 2012, pp. 374–377.

[15] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for internet of things security," in *2014 Euro Med Telco Conference (EMTC)*. IEEE, 2014, pp. 1–5.

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

[17] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: vulnerabilities, attacks and countermeasures," *IEEE Communications Surveys & Tutorials*, 2019.

[18] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of iot frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[19] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[20] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[21] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, vol. 3. IEEE, 2012, pp. 648–651.

[22] C. Silva, R. Batista, R. Queiroz, V. Garcia, J. Silva, D. Gatti, R. Assad, L. Nascimento, K. Brito, and P. Miranda, "Towards a taxonomy for security threats on the web ecosystem," in *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2016, pp. 584–590.

[23] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 427–449.

[24] 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.

[25] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," *IEEE Internet of things journal*, vol. 3, no. 1, pp. 70–95, 2015.

[26] C. Eckert, *IT-Sicherheit: Konzepte-Verfahren-Protokolle*. Walter de Gruyter, 2013.

[27] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97–102, 2013.

[28] T. R. Peltier, *Information security risk analysis*. Auerbach publications, 2010.

[29] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40–48, 1994.

[30] R. Barnes, B. Schneier, C. Jennings, T. Hardie, B. Trammel, C. Huitema, and D. Borkman, "Confidentiality in the face of pervasive surveillance: A threat model and problem statement," 2015.

[31] P. Syverson, "A taxonomy of replay attacks," NAVAL RESEARCH LAB WASHINGTON DC, Tech. Rep., 1994.

[32] O. A. Osanaiye, A. S. Alfa, and G. P. Hancke, "Denial of service defence for resource availability in wireless sensor networks," *IEEE Access*, vol. 6, pp. 6975–7004, 2018.

[33] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," *International Journal of Distributed Sensor Networks*, vol. 2, no. 3, pp. 267–287, 2006.

[34] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Communications surveys & tutorials*, vol. 13, no. 2, pp. 245–257, 2010.

[35] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[36] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[37] C. Schellenberger and P. Zhang, "Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system," in *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*. IEEE, 2017, pp. 1374–1379.

[38] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Science & Business Media, 2008, vol. 31.

[39] D. Quarta, M. Pogliani, M. Polino, F. Maggi, A. M. Zanchettin, and S. Zanero, "An experimental security analysis of an industrial robot controller," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 268–286.

[40] J. R. Douceur, "The sybil attack," in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[41] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *computer*, vol. 35, no. 10, pp. 54–62, 2002.

[42] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.* IEEE, 2003, pp. 113–127.

[43] G. N. Nayak and S. G. Samaddar, "Different flavours of man-in-the-middle attack, consequences and feasible solutions," in *2010 3rd International Conference on Computer Science and Information Technology*, vol. 5. IEEE, 2010, pp. 491–495.

[44] T. Moore and R. Clayton, "An empirical analysis of the current state of phishing attack and defence." in *WEIS*, 2007.

[45] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "Iot goes nuclear: Creating a zigbee chain reaction," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 195–212.