Categorizing IoT Services According to Security Risks

Ostroški Dominik(✉), Mikuc Miljenko, and Vuković Marin

Faculty of Electrical Engineering and Computing,
University of Zagreb, Zagreb, Croatia
{dominik.ostroski,miljenko.mikuc,marin.vukovic}@fer.hr

Abstract. Internet of things has been a part of our lives, both at home and in workplace, for several years now. However, due to its popularity, numerous security issues are emerging related to devices, network communication or Internet of things (IoT) acquired data storage and processing in the cloud. This paper presents a model for categorization of existing and novel IoT services based on estimated security risks. The goal is to develop security requirements for each service category in such a way that service creators are able to classify their services and follow the requirements in order to harden the services in development. The paper proposes a categorization model based on DREAD (Damage potential, Reproducibility, Exploitability, affected users, and Discoverability) and gives examples of existing services classification. A set of simple questions is proposed at the end of the paper that should be answered by service creators in order to categorize its service into one of the proposed categories.

Keywords: Internet of Things · Security requirements · Service categorization · Security and privacy risks

1 Introduction

Internet of things (IoT) has been a part of our lives for several years now, while its beginnings date to more than several decades ago, in specific domains such as industry, logistics and retail [1]. With more and more integration of IoT in our lives, various devices began to gather more and more information about the environment, other systems and, perhaps most controversially, its users, resulting in possible exposure of users' private data. This risks became apparent with the first attacks targeted specifically on IoT devices, such as Mirai botnet [2], where a malware was used to gain control of web cameras and use them to perform further network DDoS attacks. When looking at the attacks in IoT domain nowadays, we conclude that there are three main parts of an IoT system from security point of view: (i) device with administration

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2021, LNICST 382, pp. 154–166, 2021.
https://doi.org/10.1007/978-3-030-78459-1_11

interface, (ii) network communication and (iii) cloud based platform for control, data acquisition and processing. Most of the attacks in the earlier years of IoT focused on administration interfaces (i) and network communication (ii) [3] and the devices typically became parts of a botnet used for further attacks. When looking at end-users and their privacy issues, there have been numerous examples of privacy breaches with or "around" IoT devices. Since IoT devices are typically low in processing and storage power, they gather data, possibly filter it, and then upload it to the cloud where the data storage, processing and knowledge discovery is performed (iii). As expected, most of the data breaches actually happened in the cloud, where malicious individuals or groups gained access to cloud-based platforms. Because of this, many researchers focused on privacy-preserving solutions in IoT over the years, with very interesting examples of how consumer data can be used for various malicious purposes. An interesting example of this is presented in [4] and [5] where it is shown how data acquired through wearable devices can even be used to outline maps of military bases. This examples show how the data acquired can be used in various malicious ways which were previously not possible, especially when data from more users is aggregated.

With regards to these issues from the domain of security and privacy, we find it necessary to create a model that will allow IoT service creators to try and assess security and privacy risks to their service and its users. The ultimate goal is to develop a framework that will allow the service creators to answer questions about their service and the model will estimate the risk and offer necessary security requirements to consider when developing and implementing the service. In this paper we propose a first step towards this goal - a model for categorization of IoT services based on security requirements. We use a DREAD model and apply it to common IoT services in order to establish a categorization of services with regards to security and privacy. In means of terminology, we use the notation of CVSS 3.0 vulnerability severity ratings [6] in order to describe the risk severity for IoT service category.

The rest of the paper is organised as follows. Next Section gives an overview of existing research on security issues in IoT, discusses recent IoT services with regards to security and notes most common attacks on IoT platforms and infrastructure. Section 3 attempts to group IoT services into categories according to potential security risks, using the DREAD model. In Sect. 4 we demonstrate the proposed service categorization on example IoT services. Finally, we conclude the paper in Sect. 5 and give guidelines for future work.

2 Previous Research

In this section, we examine state-of-the-art related to defining security requirements in IoT domain and give review of most well-known attacks on IoT systems categorized by area of application.

In [7] the authors present a systematic approach to understanding the security requirements for IoT. When developing these requirements, they offer various scenarios and outline potential threats and attacks in the IoT. Based on

the characteristics of the IoT, they group possible threats and attacks into five areas: communication, devices/services, users, mobility, and resource integration. They then examine the existing IoT security requirements in the literature and describe in detail their approach to IoT security requirements.

Abomhara et al. [8] Examine the requirements of the IoT security architecture in relation to three main topics: data protection for individuals, confidentiality of business processes, and reliability of third parties. The article recommends the use of cryptographic techniques and light-weight security mechanisms for the things that are at the edge of the network.

The research by Sicari et al. [9] discusses contributions providing confidentiality, security, access control, and privacy for the IoT and security of middleware. The authors discuss trust management, authentication, privacy issues, data security, network security, and intrusion detection systems.

As stated in [10], the connection of each thing creates new problems with data security and data protection, such as the confidentiality, authenticity, and integrity of the data that things "feel and exchange". This author lists the standard security requirements resilience to attacks (the system must avoid individual points of failure and should adapt to node failures), data authentication(retrieved address and object information must be authenticated) and access control (information providers must be able to carry out access control for the transmitted data). When protecting the privacy of the customer, measures need to be taken that only the information provider is able to infer from observing the use of the lookup system.

In [11] the authors analyzed three forms of IoT security: communication, application interface, and data security. They reviewed the current IoT technologies, approaches, and models and found a security gap in existing communication technologies, application interfaces, and data security. They also gave an overview of related work in the IoT.

The authors in [12] conducted a comprehensive study of existing IoT technologies and their security problems. They focused on smart homes and the urban environment and discussed possible IoT security solutions to improve the latter. These security solutions focused not only on the security problems of today's endpoints but also on predicting future attacks on data protocols and connectivity.

In [13], the authors presented a classification of attacks from different networks related to IoT. The classification distinguished between common and specific attacks from each network and used certain criteria such as security attributes, congestion, and disturbances. In addition, some current security solutions are presented in detail that demonstrate the security requirements for IoT protection [14].

Alqassem [15] proposes a requirements engineering framework ensuring privacy and security. They identify the complexity of analyzing security in IoT systems and states that the key components in IoT are only two: RFID systems and networks of sensors. The framework proposed in this study was aimed at

building an effective model that can handle the heterogeneity of the IoT network by tackling the privacy and security concerns at the earliest stage possible.

In [16] authors analyze the security aspects for each layer of the IoT architecture and on this basis propose a risk classification of the layers of the IoT architecture. The analysis of the security vulnerabilities revealed that the greatest security risk is the perception layer of the IoT architecture due to the specific limitations of the devices and transmission technologies used on this layer. The highest level of risk for the IoT application was determined for the finance, production and multimedia sectors due to the largest increase in its use.

Last, but definitely not the least, the OWASP Foundation began work on IoT Security Verification Standard (ISVS) [17], similar to the well-accepted and very useful Application Security Verification Standard (ASVS) [18] used for (web) applications. Although they state that ISVS is still in very early stages of development, we expect it to become a standard for security requirements once it is finished.

Based on the previous work, IoT services can be categorized into seven categories by area of application. These are: smart city, smart energy, intelligent transport systems, industry automation, smart health, public safety, and smart agriculture. In the rest of this chapter will be given a review of attacks on IoT systems based on proposed categories.

Some smart city applications are smart waste management, smart parking, smart street lighting, smart water grids, smart home, and smart HVAC. In 2011 the control system of the city water utility in Springfield, Illinois was hacked. Hackers gained remote access to the control system causing the system to turn on and off repeatedly leading to the burnout of a water pump Cybersecurity firm ForeScout Technologies has discovered that thousands of vulnerable IoT devices in heating, ventilation, and air conditioning (HVAC) systems are vulnerable to cyber-attacks. Their research showed that nearly 8,000 connected devices, mostly located in hospitals and schools, have security vulnerabilities that allow unauthorized access and are very vulnerable to cyber-attacks [19]. Changing the temperature setpoints or switching off devices used for heating, ventilation, and air conditioning can harm people in facilities where these devices are vital, such as tunnels or hospitals.

Most notable smart energy services are smart grids, remote monitoring and data collection for oil and gas production, and smart renewable energy. On December 23, 2015, hackers managed to successfully compromise the information systems of three energy companies in Ukraine and temporarily cut off electricity supply to consumers. It is thought to be the first known successful cyberattack on the power grid, resulting in several outages that caused some 225,000 customers to lose electricity in various areas [20]. The most significant, malicious software that targets remote monitoring and data collection systems is Stuxnet. It was launched solely to target a centrifuge at a uranium enrichment plant at a nuclear power plant in Iran. Although Iran has not released specific details about the effects of the attack, the Stuxnet worm has destroyed numerous uranium enrichment centrifuges [21]. A Utah renewable energy producer was hit by

a cyberattack that briefly cut off contact with a dozen wind farms in the spring of 2019 [22]. Although this attack had no serious consequences, it was the first attack to cut off communication between the power grid operator and the power generation station.

Intelligent Transport Systems (ITS) are management and information systems that use integrated communication and data processing technologies to improve the mobility of people and goods, increase safety, reduce traffic congestion, manage incidents effectively and meet transport policy objectives [23]. They include smart cars, roadway reporting, and traffic flow controls, and communications applications and systems. In 2016, the San Francisco Municipal Transport Agency was hit by a cyberattack that displayed a hacker message on their systems[24]. The underground stations displayed the message "System not working". Unable to charge customers, free rides were allowed which led to a loss of profit. In 2017, 70% of storage devices that recorded data from police surveillance cameras were infected with ransomware [25]. Due to the attack, the local police could not record for 3 days, and the attack hit 120 of the 180 network video recorders. A group of university researchers devised how to hack autonomous cars by putting stickers on street signs [26]. The researchers analyzed image sorting algorithms used by autonomous vehicle vision systems and then visually manipulated street signs with stickers to deceive machine learning models. In one example, they used stickers to trick the autonomous car's visual system into reading the STOP sign as a 45-mile-per-hour sign. The consequences of such attacks can be devastating in the real world.

As industrial automation and process management systems become available to businesses they become increasingly digitally connected. Data collection, exchange, and analysis is a valuable practice of companies today, as it is often used to increase efficiency. The most notable services in industrial automation are smart logistics and Supervisory control and data acquisition (SCADA) systems. Smart logistics provide the ability to monitor not only the location of things but also the characteristics of things. For example, during the transport of some drugs or chemicals, temperature, object orientation, and pressure inside the tank are treated as sensitive data. SCADA systems for power substations and distribution networks or even nuclear power plants are potential targets for cyber attacks. In the attack on the German iron factory, the attackers accessed the iron plant's office network and used this approach to enter the production network, from where they could cause damage to the blast furnace [27]. There was an accumulation of failures of individual components of the control system. System failures resulted in an incident in which the furnace could not be closed properly, leading to enormous damage to the entire system. In 2019, 8 attacks by hacker groups on industrial companies were recorded [28]. Most of the attacks were aimed at stealing intellectual property and gaining control of control and management systems, which could have devastating effects on companies.

IoT technologies encourage the development of smart systems to support and improve health systems and are applied to interconnect available medical resources and provide reliable and efficient health services to the elderly and

patients. The two most common use cases of IoT in healthcare are remote health monitoring systems and remote surgery. A team of researchers from the University of Washington in Seattle successfully discovered security holes in the Raven II surgical robot [29]. By attacking using the "man in the middle" technique, which changes the commands flowing between the operator and the robot, the team managed to maliciously disrupt a wide range of robot functions, making it difficult to capture objects with robotic hands, and even completely change the original commands. During denial-of-service attacks, in which attackers flooded the system with useless data, robots became slower and harder to use. In situations where precise movements can mean the difference between life and death, such as surgery or in search and rescue missions, these types of cyberattacks can have serious consequences. The most common form of attack on wearable devices and implanted medical devices is an acoustic attack that uses ultrasonic or other audio frequencies at the resonant frequencies of the device to attack the devices [30]. Acoustic attacks have been shown to work against implanted heart defibrillators and pacemakers, insulin pumps, and devices that monitor activity among other medical devices [31]. These attacks can acquire confidential medical data, alter data that cause system malfunctions and deliver inappropriate therapies, and cause devices to lose power to become unusable [32].

Internet of Things-based public safety applications offers a number of benefits, including greater situational awareness and improved decision-making, reduced response times and improved emergency response capabilities, improved citizen safety and infrastructure security, improved prevention and escalation of critical situations, and dissemination of information to citizens [33]. Some applications of IoT in public safety are critical communication systems and smart systems for emergency response. Successful attacks on these systems can result in the transmission of inaccurate messages, denial of service, data leakage, and changes in GPS coordinates used to calculate positioning [34]. Faults in the operation of these systems affect a large number of people. An attack can result in greater loss of life in emergencies because rescuers cannot coordinate effectively and the public is not alerted in a timely manner, or inaccurate information is transmitted.

While beneficial to industry productivity, the use of Internet-connected devices has revealed potential cyber-attacks and vulnerabilities in the agricultural sector. IoT systems in agriculture are usually used for purpose of smart irrigation and crop monitoring. One of the most common threats to smart farming is a malware injection attack [35]. Malware can steal data on agricultural material consumption, purchase information, data on agricultural machinery, etc. It can also recruit smart devices as part of a botnet used to commit malicious acts. Furthermore, malware can interfere with the functions of physical smart equipment which in turn can have a devastating effect on a particular crop or farm. Attacks on smart irrigation systems can have an even greater impact. An attack that consumes water and empties a city water tank can result in the inability to provide water to residents until the local water tank is filled, with an attack on smart irrigation systems increasing water consumption and

causing financial loss, and by applying a distributed attack against smart irrigation systems on the same pipeline system as city water, an attacker can reduce the flow of water in all households connected to the pipeline. An attack targeting urban infrastructure is a very dangerous attack, as preventing people from accessing critical infrastructure resources can result in disaster, depending on the number of people affected [36].

3 IoT Service Categorization

In this section, a security analysis of all the aforementioned Internet of Things services using the DREAD model is made. We will use the DREAD model to evaluate the likelihood of an attack by exploiting a particular threat. It is worth noting that several literature reviews have adopted various methods for modelling threats, such as popular STRIDE model developed by Microsoft, which provides mnemonic for security threats in six categories [37–39], PASTA, which represents the Process for Attack Simulation and Threat Analysis and is a seven-step risk-centric methodology [40] and VAST (visual, agile and simple threat modelling) [41]. In addition to performing threat detection, most threat modelling attempts did not rate the identified threats, except in some reviewed papers that used the DREAD model to rate and calculate the device risk score. We chose DREAD over other models because it provides a categorization of vulnerabilities based on the threats and the aggregation of risk values to a single numerical value and is capable to determine the severity of a threat.

Using the DREAD model (Table 1), we obtain a risk assessment for a given service by asking the following questions [42]:

- Damage potential: How big is the damage if a successful attack occurs?
- Reproducibility: How easy is it to reproduce an attack?
- Exploitability: How easy is it to launch an attack?
- Affected users: How many users were affected by the attack?
- Discoverability: How easy is it to find a vulnerability?

The risk assessments in this chapter are based on actual attacks on existing systems and on the characteristics of these systems.

Based on previous research and risk assessment, we propose the following 4 safety categories:

- Low risk services - DREAD rating 5–6
- Medium risk services - DREAD rating 7–9
- High risk services - DREAD rating 10–12
- Critical services - DREAD rating 13–15

In Table 2 all previously mentioned IoT services have been rated using DREAD model. Variations in grades are possible depending on the expert conducting the research. We believe that, based on the data collected and previous work, we have given the most objective assessment.

Table 1. Thread rating table

Rating	High(3)	Medium(2)	Low(1)
Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
Reproducibility	The attack can be reproduced every time and does not require a timing window	The attack can be reproduced, but only with a timing window and a particular race situation	The attack is very difficult to reproduce, even with knowledge of the security hole
Exploitability	A novice programmer could make the attack in a short time	A skilled programmer could make the attack, then repeat the steps	The attack requires an extremely skilled person and in-depth knowledge every time to exploit
Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use	The bug is obscure, and it is unlikely that users will work out damage potential

4 Example Service Categorization

In order for services that are not listed in this paper to be classified in one of the safety categories without conducting a risk assessment according to the DREAD model, we propose the following model of service evaluation. The service can be assigned a grade from 7 to 15 based on answering the following questions and adding up the received grades.

- How many people use the service?
  - Less than 10 (1)
  - 10 to 100 (2)
  - More than 100 (3)
- Does the system collect personal, financial or medical information about users or confidential company information?
  - No (1)
  - Yes (2)
- Are the devices in the system physically secured or easily accessible?
  - Physically insured (1)

Table 2. Threat rating using DREAD model

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total	Rating
Smart city							
Smart parking	2	2	2	2	2	10	High
Smart waste management	1	2	1	1	1	6	Low
Smart street lighting	2	2	1	3	2	10	High
Smart water grid	3	2	1	3	1	10	High
Smart home	3	3	3	1	3	13	Critical
Smart HVAC	3	2	1	3	1	10	High
Smart energy							
Smart grid	3	2	2	3	2	12	High
Remote monitoring and data collection	3	2	1	2	1	10	High
Smart renewable energy	3	2	1	3	2	11	High
Intelligent transport systems							
Smart vehicles	3	2	2	1	2	10	High
Roadway reporting and traffic flow controls	2	3	2	2	2	11	High
Communications applications and systems	2	3	2	2	3	12	High
Industry automation							
Smart logistic	2	2	2	2	1	9	Medium
SCADA	3	2	2	2	1	10	High
Smart healthcare							
Remote health monitoring	2	3	2	1	2	10	High
Remote operation	3	2	2	1	1	9	Medium
Public safety							
Critical communication	2	2	2	2	2	10	High
Smart Emergency Response	3	2	2	3	2	12	High
Smart agriculture							
Smart irrigation	3	3	2	3	2	13	Critical
Corp monitoring	2	3	2	1	2	10	High

    - Easily accessible (2)
- Is the system connected to a public or private network?
    - Private network (1)
    - Public Network (2)
- Are the devices active (Active devices collect data and then generally do something based on the collected data, such as changing the colour of traffic lights or starting a machine) or are they passive (Passive devices collect data and send it somewhere)?
    - Passive (1)
    - Active (2)
- Are devices upgradeable? Could new software versions be put on them?
    - Yes (1)
    - No (2)

– Is there authentication when accessing the device?
  - Yes (1)
  - No (2)

After receiving a rating based on Table 3, you can classify the service into one of the security categories.

Table 3. Security categories based on the rating obtained by the proposed model

Security category	Rating
Critical services	14–15
High risk services	11–13
Medium risk services	9–10
Low risk services	7–8

For example, we will take 3 real services and categorize them according to the proposed model into one of the security categories. The services we will categorize are an air quality system, a portable device for athletes, and smart greenhouses. The air quality system is used by a small number of people (1), it does not collect personal or confidential data (1). The devices are physically secured (1) and can be connected to the public network (2). The devices in the system are passive (1), not upgradeable (2) and there is authentication to access the device (1). Based on this assessment, we obtain a grade of 9, which classifies the air quality monitoring system into medium risk systems.

Only one person uses a sports carrying device (1). These devices collect personal and medical information about the people who use them (2), but they are passive devices (1). The devices are constantly located next to the person wearing them so that they are physically secured (1) and do not connect to the public internet (1). The devices are upgradeable (1) and there is authentication when accessing the device (1). Based on this assessment, we get a grade of 8 and we can classify wearable sports equipment as low risk services.

The system in smart greenhouses is used by more than 10 people (2). The devices collect sensitive information (2), are physically secured (1), and are not connected to the public network (1). The devices are active (2), upgradeable (1) and there is authentication to access the device (1). Based on this assessment, we get a score of 10 and we can classify smart greenhouse systems as medium risk services.

5 Conclusion

The paper proposes a model for categorizing IoT services based on security risks to the services and their users. The purpose of the proposed categorization is to allow IoT service creators to assess the security and privacy risks to services

they are developing. Ultimately, the goal is to provide guidelines for hardening the services while in development, since one of great issues in security in general is lack of security considerations during design and implementation phases. In this paper we propose four service categories, corresponding to risk levels low, medium, high and critical, based on DREAD model. We give a simple set of questions that should be answered by service creators in order to get a total score for the service, thus categorizing it into one of the proposed categories. Finally, we demonstrate how existing services can be categorized into on of the proposed categories.

In future work, we plan to further examine existing IoT services, especially the services that were breached on any level (i.e. device, network or cloud platform) and determine the drawbacks that eventually lead to service compromise, and also expand the number of services that we look at so we can get more generalized solution. Based on the detected flaws and issues, the plan is to further tune the questions and categorization in order to get a better fit for possible new IoT services. Finally, guidelines for service creators should be implemented in form of security requirements to be used during service design and implementation. Each service category should have a list of security requirements that should be considered. It is our opinion that in this way service creators can be more aware of possible risks and take precautions when they really should; in the early phases of service development.

Acknowledgement. This work has been supported by Croatian Science Foundation under the project 1986 (IoT4us: Human-centric smart services in interoperable and decentralised IoT environments).

References

1. Suresh, P., Daniel, J.V., Parthasarathy, V., Aswathy, R.: A state of the art review on the Internet of Things (ToT) history, technology and fields of deployment. In: 2014 International Conference on Science Engineering and Management Research (ICSEMR), pp. 1–8. IEEE (2014)
2. Antonakakis, M., et al.: Understanding the Mirai botnet. In: 26th Security Symposium (Security 17), pp. 1093–1110 (2017)
3. Davis, D.B.: ISTR 2019: Internet of Things cyber attacks grow more diverse (2019)
4. Hassan, W.U., Hussain, S., Bates, A.: Analysis of privacy protections in fitness tracking social networks-or-you can run, but can you hide? In: 27th Security Symposium (Security 18), pp. 497–512 (2018)
5. Hern, A.: Fitness tracking app Strava gives away location of secret us army bases, January 2018
6. Common vulnerability scoring system v3.0: Specification document
7. Pal, S., Hitchens, M., Rabehaja, T., Mukhopadhyay, S.: Security requirements for the Internet of Things: a systematic approach. Sensors **20**(20), 5897 (2020)
8. Abomhara, M., Køien, G.M.: Security and privacy in the Internet of Things: current status and open issues. In: 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8. IEEE (2014)
9. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)

10. Babar, S., Mahalle, P., Stango, A., Prasad, N., Prasad, R.: Proposed security model and threat taxonomy for the Internet of Things (IoT). In: Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (eds.) CNSA 2010. CCIS, vol. 89, pp. 420–429. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14478-3_42
11. Sain, M., Kang, Y.J., Lee, H.J.: Survey on security in Internet of Things: state of the art and challenges. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 699–704. IEEE (2017)
12. Bastos, D., Shackleton, M., El-Moussa, F.: Internet of Things: a survey of technologies and security risks in smart home and city environments (2018)
13. Davoli, L., Veltri, L., Ferrari, G., Amadei, U.: Internet of Things on power line communications: an experimental performance analysis. In: Kabalci, E., Kabalci, Y. (eds.) Smart Grids and Their Communication Systems. ESIEE, pp. 465–498. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1768-2_13
14. Suryani, V., et al.: A survey on trust in Internet of Things. In: 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), pp. 1–6. IEEE (2016)
15. Alqassem, I.: Privacy and security requirements framework for the Internet of Things (IoT). In: Companion Proceedings of the 36th International Conference on Software Engineering, pp. 739–741 (2014)
16. Cvitić, I., Vujić, M., et al.: Classification of security risks in the IoT environment. Ann. DAAAM Proc. **26**(1) (2015)
17. Owasp: IoT security verification standard (2020)
18. Owasp: Application security verification standard (2020)
19. Researcher at Forescout Technologies Inc.: Discovering and defending against vulnerabilities in building automation systems (BAS), June 2020
20. Case, D.U.: Analysis of the cyber attack on the Ukrainian power grid. Electr. Inf. Shar. Anal. Cent. (E-ISAC) **388** (2016)
21. Holloway, M
22. Cimpanu, C.: Cyber-attack hits Utah wind and solar energy provider, October 2019
23. Huq, N., Vosseler, R., Swimmer, M.: Cyberattacks against intelligent transportation systems. TrendLabs Research Paper (2017)
24. Rodriguez, J.F.: 'You hacked' appears at muni stations as fare payment system crashes, November 2016
25. Williams, C.: Hackers hit d.c. police closed-circuit camera network, city officials disclose, January 2017
26. Eykholt, K., et al.: Robust physical-world attacks on deep learning visual classification. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1625–1634 (2018)
27. Goldman, J.: Cyber attack causes physical damage at German iron plant (2014)
28. Kaspersky, I.: Threat landscape for industrial automation systems (2019)
29. Langston, J.: UW researchers hack a teleoperated surgical robot to reveal security flaws (2015)
30. Fu, K., Xu, W.: Risks of trusting the physics of sensors. Commun. ACM **61**(2), 20–23 (2018)
31. Li, C., Raghunathan, A., Jha, N.K.: Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system. In: 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, pp. 150–156. IEEE (2011)

32. Halperin, D., et al.: Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. In: 2008 IEEE Symposium on Security and Privacy (sp 2008), pp. 129–142. IEEE (2008)
33. Zhang, Q., Fitzek, F.H.P.: Mission critical IoT communication in 5G. In: Atanasovski, V., Leon-Garcia, A. (eds.) FABULOUS 2015. LNICST, vol. 159, pp. 35–41. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-27072-2_5
34. Loukas, G., Gan, D., Vuong, T.: A review of cyber threats and defence approaches in emergency management. Future Internet **5**(2), 205–236 (2013)
35. Gupta, M., Abdelsalam, M., Khorsandroo, S., Mittal, S.: Security and privacy in smart farming: challenges and opportunities. IEEE Access **8**, 34564–34584 (2020)
36. Bennett, C.: Russia tied to cyberattack on Ukrainian power grid, February 2016
37. Abomhara, M., Gerdes, M., Køien, G.M.: A stride-based threat model for telehealth systems. NISK J., 82–96 (2015)
38. Alhassan, J.K., Abba, E., Olaniyi, O., Waziri, V.O.: Threat modeling of electronic health systems and mitigating countermeasures. In: International Conference on Information and Communication Technology and Its Applications (ICTA 2016). Federal University of Technology, Minna, Nigeria (2016)
39. Amini, A., Jamil, N., Ahmad, A., Zaba, M.: Threat modeling approaches for securing cloud computin. JApSc **15**(7), 953–967 (2015)
40. Lin, X., Zavarsky, P., Ruhl, R., Lindskog, D.: Threat modeling for CSRF attacks. In: 2009 International Conference on Computational Science and Engineering, vol. 3, pp. 486–491. IEEE (2009)
41. De Cock, D., Wouters, K., Schellekens, D., Singelee, D., Preneel, B.: Threat modelling for security tokens in web applications. In: Chadwick, D., Preneel, B. (eds.) CMS 2004. ITIFIP, vol. 175, pp. 183–193. Springer, Boston, MA (2005). https://doi.org/10.1007/0-387-24486-7_14
42. Meier, J., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., Muruka, A.: Threat modeling (2003)