Towards a Methodology for the Classification of IoT Devices

Dimitrios Sarris[1], Konstantinos Xynos[2], Huw Read[2, 3] and Iain Sutherland[2]
[1]Digital14, Dubai, UAE
[2]Noroff University College, 4608 Kristiansand S, Vest-Agder, Norway
[3]Norwich University, Northfield, Vermont, USA
dimitrios.sarris@digital14.com
kxynos@mycenx.com
hread@norwich.edu
iain.sutherland@noroff.no
DOI: 10.34190/EWS.20.013

Abstract: Within the scope of the Internet of Things (IoT), there are multiple sensors connected to the Internet that have the ability to report on the status of a system; a state change, the surrounding environment and conduct automated functions based on sensory input. IoT devices commonly have a small form factor, with specific forms of connectivity and power requirements. The business drive to get a product to market and to set the dominant standard, can result in limited governance, as standards appear to be mainly focused on the communication and interactivity aspects of the technology, and less on the overall security or identification of the device, data transmission or quality of firmware.This paper explores possible foundations for the classification of IoT devices according to environmental usage, as a means to facilitate the required governance through regulation and standardisation, which in turn would enable for easier auditing when such devices are deployed, maintained and, finally, decommissioned. The authors recommend the development of a classification framework that would allow an end user to understand if an end product can be used within their required use case/domain.

Keywords*:* Internet of Things; IoT; classification; connected living; framework;

1. Introduction

The increasing use of embedded or smart technologies has been facilitated by a variety of factors, including evolving network connectivity enabling the exchange of disparate forms of information, and the increase in capability and decreasing cost of integrated components leading to the uptake of "smart" devices in both commercial and domestic environments. This offers the possibility of efficient savings in energy and has become one of the forces behind wider adoption of IoT. Security is crucial in the sustainability of new systems and networks. Lack of governance and regulations on the inception, architecture, production and use of the IoT and the Internet of Everything (IoE) has resulted in an environment where malicious actors can influence online systems including financial transactions or affect a victim's physical assets. The Mirai botnet, which affected many IoT devices "took the Internet by storm" (Antonakakis, 2017) when it overwhelmed targets with massively distributed denial-of-service-attacks (DDoS) in 2016. The domain name system (DNS) organisation DYN received a throughput reportedly up to 1.2Tbps, knocking high-profile websites offline on the East Coast of the United States including Netflix, Twitter, CNN and others (Guardian, 2016). Mirai targeted IoT devices, DVRs, cameras, routers, and printers, but the devices used were created by a handful of manufacturers (Antonakakis, 2017) with hard-coded passwords.

In the USA the term Cyber Physical Systems is also widely used alongside IoT, the NIST report by Greer et al. (2019) provides clarity by identifying the history of these neologisms and goes as far as describing a unified perspective to clarify the relationship between the two. These risks are increasingly being highlighted in academic journals (e.g. Awasthi et al. (2018), Ashrad et al. (2020) and Fafoutis et al.(2017)) and in the popular press via news articles (Turner (2017), Sadam et al. (2017)) with regards to the impact of cyber-attacks on an organisation's finances.

Research by Gartner (2018) shows a trend in increasing investment in relation to the security of IoT (Table 1). However, as organizations do not have full control over the software and hardware being used in IoT devices (Gartner (2018)), they state, "*We expect to see demand for tools and services aimed at improving discovery and asset management, software and hardware security assessment, and penetration testing"*. Therefore the trend of increased spending in IoT security appears to be concentrated in the *consumer* market (i.e. organisations purchasing devices and securing them from harm) rather than in the *producer* market (i.e. manufacturers strengthening device security before they appear on the market), alluding to the "security as an afterthought" philosophy.

Table 1: Worldwide IoT Security Spending Forecast (Millions) (Gartner, 2018)

	2016	**2017**	**2018**	**2019**	**2020**	**2021**
Endpoint Security	240	302	373	459	541	631
Gateway Security	102	138	186	251	327	415
Professional Services	570	734	946	1,221	1,589	2,071
Total	**912**	**1,174**	**1,506**	**1,931**	**2,457**	**3,118**

The remainder of this paper is organised as follows; *2. Defining the Internet of Things* examines key literary sources to identify problem domains; *3. Related Work* discusses recent research around the area of defining and classifying IoT from the context of Cybersecurity; *4. Toward an IoT Classification Framework* details the perceived high level requirements and the proposed classification types for IoT devices; 5. The section on *Example Scenarios* provides instances of how the proposed IoT classification framework may be applied. Section 6 concludes the paper with a summary and proposed future work.

2. Defining the Internet of Things

The term IoT has changed significantly sine 1999 (Ashton, 2009) to incorporate an expanding range of devices, interactions, connectivity and new efficiencies and capabilities for existing equipment and environments. Research into publication trends conducted by Greer et al. (2019) into the terminology identified 3 temporal phases; low numbers and low growth in 2005-2009, increased IoT publications in 2010-2013, rapid growth after 2014. Their research into IoT definitions largely revealed terminology from the networking and IT communities.

451 Research (2015) defines IoT as "*... the apps and systems enabling the virtualization of the physical world*". This is a broad definition and could be argued that it encompasses a number of devices which would generally be considered to the part of IoT. The definition is broad enough to even include VR (Virtual Reality. Dedlic (2016) considers a similarly broad definition but focuses on scale and complexity with the following definition: "*At the very high level of abstraction, the Internet of Things (IoT) can be modelled as the hyper-scale, hyper-complex cyber-physical system*." Note the synonymous use of "*cyber-physical system"*; the work by Greer et al. (2019) conversely sought to define cyber-physical systems and IoT as two distinct entities.

A more environmental approach is taken by Yachir et al (2016) with a focus on value-added services as: "*The Internet of Things (IoT) envisions a world where smart objects connected to the Internet, share their data, exchange their services and cooperate together to provide value-added services that none of these objects could provide individually.*" The concept of individual IoT devices not being of much use on their own, but rather when working together, help create a distinction from traditional IT equipment. Gartner (2020) defines IoT as "t*he network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.*"

It can be seen from the various definitions that the term IoT covers a broad range of devices used in numerous environments. A single connected sensor, to more complex devices that provide enhanced control or information by being connected to such devices. A single IoT device tends to perform a limited set of activities. Once they are connected and work as a collective their true flexibility is shown. These communication abilities further the complexity that follows such interconnected systems and increasing possible risk factors. Although an IoT appliance can be thought of as a single device, it is suggested that an 'IoT solution' is defined as the collection of IoT devices that are part of a deployment and that a deployment can include one or more IoT devices. This definition is proposed as a means to identify more complex systems that are made up of a number of IoT components. The reason behind this is the need to know when small systems are introduced into an environment and when they need updating or replacing. Knowing when a single IoT device within an IoT solution has an issue or a weakness (e.g. such as publicised common vulnerabilities and exposures (CVE), (MITRE, 2020)), to coin the old adage, 'a chain is only as strong as its weakest link', decisive action must be carried out to update, replace, or mitigate the Cyber vulnerability to strengthen the environment.

The growth in the use of IoT presents a number of challenges as the variety of devices supporting data processing and storage continue to evolve. Not limited to these factors, IoT and other technologies such as cloud computing allow for a wider adoption since devices may not need to process information, instead merely providing notification of state changes to remote servers.

These technologies range from fixed systems in smart homes to mobile and highly portable technology. Examples include wearable devices and clothing (Hexoskin, 2016), drinking containers (Disney Food Blog, 2016), (Glassify, 2016) and smart housing systems, including; automation (IFTTT, 2020), security systems (Verisure) and infotainment systems (Amazon, 2016). There are a number of possible ways to view IoT devices based on both capability and functionality.

Furthermore, there are several options available to manufacturers when deciding how the devices will communicate. These can include any one or a combination of the following: Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution (LTE), GSM, Zigbee, Z-Wave, Ultra-Wideband (UWB), LoRa, CAN bus, and others. In particular, Zigbee and Z-Wave, have become prevalent in-home automation, both being tailored for typical IoT use cases; low power consumption, intermittent data transfer and wireless mesh networking.

3. Related Work

The huge increase in connected devices and spending on IoT validates the expected wide adoption of IoT technology (Gartner, 2018). Security researchers are increasingly concerned regarding the possible misuses that will occur. The security of IoT devices and systems need to be incorporated into any device from the design phase, up to its integration and life span, including when it gets decommissioned. The principles of Confidentiality, Integrity, Availability, and Non-repudiation are also of the utmost importance in the wider ecosystem of devices to avoid introducing further vulnerabilities into an environment. This is particularly important when maintaining a system with updates and if needed secure decommissioning when the device reaches the end of life.

The National Institute of Standards and Technology (NIST) provides considerations for managing IoT Cybersecurity and privacy risks (NIST, 2019). In particular, its focus is to provide support to federal agencies and other organisations in the USA to better understand and manage the risks throughout a devices' lifecycle. Three high-level issues that affect the management of cybersecurity of IoT devices (compared to traditional IT equipment) were identified;

1. IoT devices interact with the physical realm in ways traditional IT does not,
2. IoT equipment cannot be "*accessed, managed, or monitored*" using the same techniques as traditional IT, and
3. IoT devices' cybersecurity capabilities differ in their availability, efficiency and effectiveness when contrasted with traditional IT (NIST, 2019).

Furthermore, three mitigation goals of protecting device security, data security, and individuals' privacy are identified as the most significant risks an organisation will face when implementing IoT infrastructure.

More recently, NIST released documentation for IoT device manufacturers, "*foundational activities and core device cybersecurity capability baseline"* (NIST, 2020). This guidance (in its second draft at the time of writing) provides voluntary recommendations to manufacturers that they should consider performing before IoT devices reach the market. Six activities are identified, which all stem from identifying the product's customers and defining use cases early in development to determine which cybersecurity capabilities should be implemented. It does express the need of having unique identifiers, both physical and logical, for IoT devices. However, a general classification of such devices is outside the scope of their work and is left to the manufacturer to determine the most appropriate course of action.

In a similar vein, the European Telecommunications Standards Institute (ETSI) have released a technical specification, "*Cyber Security for Consumer Internet of Things".* It discusses a set of 13 cybersecurity provisions for implementation by device manufacturers; adherence providing assurance that companies "*can help in ensuring that [devices and services] are compliant with the General Data Protection Regulation*" (ETSI, 2019). Like NIST (2020), it also does not attempt to provide a classification or taxonomy of IoT devices.

It should be emphasised that both NIST (2019) and ETSI (2019) are voluntary implementations; the additional burden placed on an organisation (be it financial, delayed time to market, etc.) provide disincentives to adoption. However, the strength of the European General Data Protection Regulation (GDPR, 2016) will provide support for the uptake as, a) there are existing legal requirements, and b) the ETSI guidance is domain-specific within the realm of IoT. The United States, without any formal Federal equivalent of GDPR, delegates such decision-making to individual states. However, recent Californian legislature introduced in 2018 and coming into effect on January 1st 2020 (SB-327, 2018) which provides requests similar security mechanisms and controls as ETSI (2019) became the first "IoT law" in the USA related to strengthening Cyber on such devices. Given the strength of California as a state (e.g. having the highest GDP of all 50 states), one can hope that when vendors comply with local Californian laws, they will provide the same goods and services throughout the United States. It doesn't provide a classification or taxonomy of IoT devices, but relies on a more generic term of "connected device", which is defined as "*...any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address*" (SB-327, 2018).

ENISA (2017) have also provided a handbook on baseline security recommendations for IoT. It goes into detail starting from defining an IoT device, its communication, to threat analysis and attack scenarios. Our proposed classification framework would look at supplementing this very technical documentation but, simultaneously, try to avoid providing the end user with too much technical information. The handbook is oriented more towards the manufacturers and testers of of IoT devices. It would provide a good testing basis of identifiable issues within an IoT device.

Other frameworks have been proposed such as the IoT Security Compliance Framework (IoT Security Foundation, 2018). But these are very technical in nature, focussed mainly on providing guidance for managers developing products or services and on those developing IoT devices. Although a highly valuable resource, a simpler and more accessible domain-based system is worth exploring as a user focussed solution to IoT issues and how they evolve over time.

4. Toward a Classification of IoT Devices

The classification of IoT needs to include several points that provides the user assurance of the end-product. It should make it clear to the end user of what requirements have been met and if the item is fit for the intended purpose. The intention is to highlight the suitability of the IoT device for a domain, rather than to provide another classification system mapping to standards, regulation and/or code of practice (DCMS, 2018).

This ensures a level of trust can be associated with the device and in-line with the classification requirements. The classification will have to clearly define if a device has been built for one of the following domains: government, military/defence, industrial, healthcare, automotive, household, or open standards; it would be marked as such. The classification would also include no more than one subdomain, that would bring some specialisation to the top-level domain. Future work will look at setting out what requirements would need to be defined for each classification domain and sub-domain.

Classification domains of IoT devices would include details includin; how the device is constructed (quality of components, original components, etc.), operations, communication of security/bug issues to end user, and whether the firmware/software be maintained regularly. Classification would, initially, be up to the manufacturer of appointing a classification domain for each device created, in principle at the time of manufacturing, similar to the concept of allocating a unique MAC address for any network card. The classification process should be documented at all times.

Regulations, if created and wherever required, will mandate the "use by" and "use of" IoT, where classification is the means to identify at a high level the operating domain of a device, such that enforcement of the appropriate security requirements is possible in order to comply.

'Government' and 'Military/Defence' will include standards that need to be clearly defined, if not already, by local and/or international governments. This will depend on who is using the IoT device and its context. Devices can be classified differently by government bodies depending on the use case. Ideally a central government body should focus on governmental classification or reclassification. IoT devices classified under this category should,

in principle, include the highest level of security baseline and trust, by utilizing current or future digital and physical non-repudiation technologies.

'Industrial' would include items that are specified for a wide area of industries. Industrial requirements would focus on the general needs of a manufacturing environment without many specialised requirements. Any special requirements could be written up within a subdomain. The authors appreciate there are a wide variety of industries with unique requirements and standards. Therefore it is suggested that more detailed information be included in a subdomain, like 'Industrial:Oil and Gas' or 'Industrial:Manufacturing' etc. Although manufacturers would be welcome to include the generalisation of the term showing that they have avoided including any special cases that would be included within a subdomain. Industrial features for consideration in IoT would normally include minimal downtime and the need to operate within inhospitable environments e.g. high temperature, humidity, high levels of particulate matter, electrical noise, or magnetic fields.

'Healthcare' IoT is one of the most sensitive levels of classification, especially when utilised for internal / critical applications. A high level of security baseline is expected on its creation and usage. IoT classified as 'Healthcare' may include: in-body solutions for patients, apparatus used in the diagnosis, treatment and monitoring of patients. The standards that define the 'Healthcare' IoT elements, would ideally be unanimously defined and have global reach, by organizations similar to World Health Organization (WHO), to enable strict governance and control, and minimize the potential of human casualties.

'Household' would include devices that ensure confidentiality is upheld at all times and provides confidence to the consumer when installing IoT device. This should also follow a standard baseline of security that is required and expected by a consumer device installed within a living environment.

'Automotive' IoT devices will have to reflect the strong cooperation of the automotive industry that will define their stringent requirements. This is irrespective of whether the items have been built internally or by their external automotive partners. A clear focus will be to ensure vehicle safety.

Lastly, 'Open' will determine that the device has been developed without a specific domain in mind. Although there might be a strong case to classify everything as 'open', manufacturers should take care as future regulation could disallow the usage of such devices in certain environments resulting in a limited market.

As can be seen in Figure 1, an IoT device or solution will go through a classification process. The item should be classified during manufacture. This clearly states what domain the manufacturer was envisaging. The classification can change during deployment, based on the characteristics of the device, how it is maintained, and what security or risks that may arise over the course of its lifetime. Any reclassification of the product will happen as a consequence of the manufacturer not adhering to the specified classification requirements and standards will make the product unfit for its intended classification. The end user could make an informed decision to decide to continue/discontinue with the product's placement/usage etc. In extreme cases regulation could even dictate a certain classification for an IoT device within a particular operating domain.

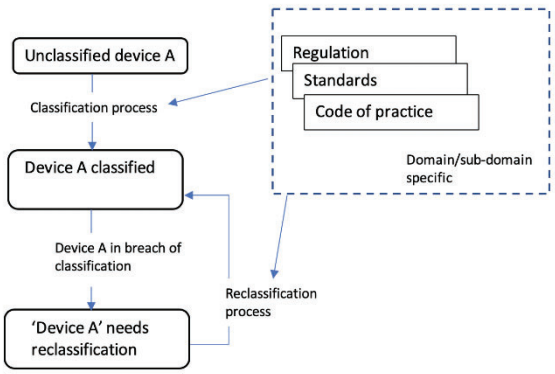

Figure 1: State diagram of proposed classification process

An open page or resource (e..g, public/private wiki) needs to be maintained and must be publicly accessible. It will list the IoT devices and/or IoT solutions and the current/historical classification of a device. It may also include an optional field detailing the reasoning for the classification, or re-classification.

In the future, a non-profit transparent committee could be setup (similar to a Working Group, IEEE, etc.) that would test and validate claims made by the manufacturers and set the date for retesting of devices or retest based on public evidence and reporting as such. This would allow for the devices to be observed and located in the event of any major issues that may be found with an IoT device.

The classification of solutions should automatically be set according to the most stringent classification of the IoT device(s) included in it, to eliminate the possibility of classification breaches and unauthorized access/use of such solutions.

5. Example Scenarios

Two example scenarios are presented below to demonstrate how to apply the proposed classification framework and illustrate the current challenges.

5.1 Scenario 1 - Embedded software issues

An organization makes use of sensors to gather room temperatures, using an inexpensive WiFi module widely found online. There is no known and non-intrusive way to check that the firmware does not have any malicious code loaded into it (e.g., manufacturing or delivery). It is not possible to check whether the firmware has been altered from the original one installed by the manufacturer. Firmware alterations could occur at the factory, in transit, or even after the module has been installed. Therefore, this device cannot be used within all the possible environments that might require the device to operate without any interruptions that might be caused by malicious code.

It may be argued that a temperature sensor presents a limited threat, except when the sensor is relied upon for monitoring critical systems and a chain reaction may be created. If the readings of the temperature sensor are used to regulate the temperature of an air-conditioned room containing heat sensitive servers, this could cause short-term or long-term issues. The incorrect readings could cause the air-conditioning system to not appropriately cool the servers and cause them to fail after incorrectly shutting down due to overheating.

If the item was classified as ‘Manufacturing’ then it would not be fit for purpose, since it’s accuracy and reliability is not up to standard for that classification, as seen in Figure 2(a). Therefore, it would be re-classified as ‘Household’ or ‘Open’ depending on requirements. In the example presented in figure 2(a) the device is reclassified as ‘Open’. With the inclusion of detailed documentation, when the reclassification occurs, it is possible to have the item under a less stringent classification. The consumer would still be able to understand why the item changed its classification and decide if it fits the use case.

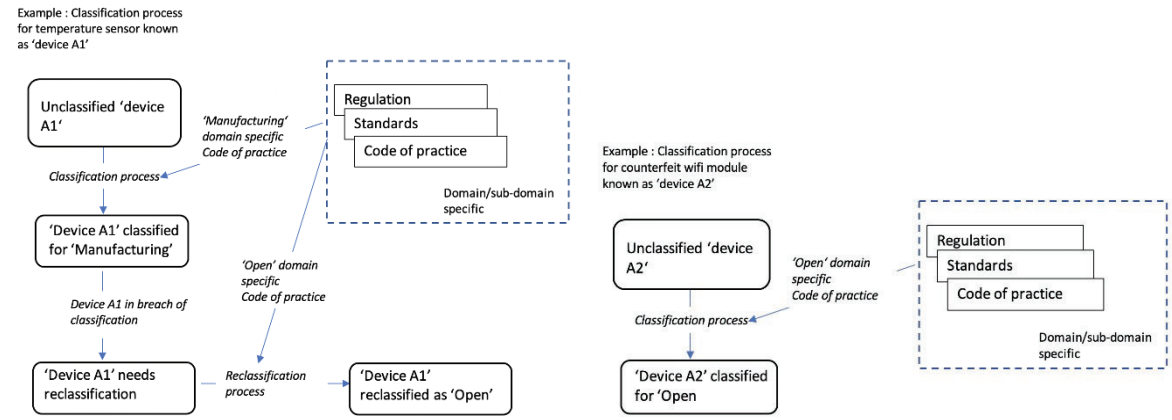

Figure 2: a) Scenario 1: classification and reclassification process; b) Scenario 2: classification process

5.2 Scenario 2 - Counterfeit chipsets

In this case we will look at counterfeit chipsets, and one well documented case is that of Nordic's nRF24L01+ (Mahidharia, 2015). These are relatively cheap 2.4GHz modules that are ultra-low power 2 Mbps RF transceivers. Anecdotally, it is known that such devices are quite popular with tinkerers, hobbyists and prototype developers. There are a flood of cheap fakes/counterfeits/clones that can be found on Amazon, Alibaba and other such marketplaces (Tehranipoor et al, 2017). In the case of Nordic's nRF24L01+ counterfeits, they are known to have a different manufacturing technology of 350nm, instead of the 250nm found in the genuine ones. Mahidharia (2015) also reports that due to the technology and larger die, this could mean that the module would have higher power usage and lower sensitivities.

At first glance, these devices pose a very limited threat to the majority of hobbyists. The issue could become more prominent when the solutions are distributed to end users, who are not aware of the quality of hardware and software (e.g., firmware) operating the device.

The case is only made worse when the software and hardware is fully controlled by the vendor increasing the possibility of backdoors existing and/or being activated at will. The undeniable questions about the build quality also raises questions about the possibility of causing other issues like shorter battery life and even the possibility of a fire.

Based on the proposed IoT classification, IoT solutions (the product) including such devices should be classified as 'Open', the classification process can be seen in the state diagram figure 2(b). It would then be reported that the device uses a non-genuine component and one that the final IoT solution has chosen to include, possibly because it is a cheaper component. A wiki entry about the product's classification would be documented and the reasoning for the classification as well.

The consumer would then be able to verify the product (IoT solution) that includes the nRF24L01+ clone and decide on an acceptable level of risk. To determine on how to progress with installation, usage of solution, look at replacing the device or even decommission the device.

6. Conclusions and Future Work

The current state of cybersecurity within the specific domain of IoT has been discussed, with particular emphasis on the need for a formal classification model of devices, primarily based on their use case/domain of operation. The intention is not to produce further codes of practice or additional security criteria, but to develop an applied classification that considers the intended domain for the IoT device.

Two scenarios were presented to highlight the challenges associated with similar IoT devices/different domains, and explanations to support the formal creation of an IoT classification framework were defined.

This preliminary work can be used to move toward a formal classification, complementary to current Cyber frameworks such as NIST, ETSI and ENISA. It will further facilitate securing IoT systems used by organisations and individuals, and providing protection from the deployment of IoT devices.

Future work will include guidelines on the exact classification process and the trigger for reclassification; a process and methodology for the application of the relevant documents (regulations, standards and codes of practice) for each domain. This will detail how the proposed system will interact with the standards existing in these different areas, in particular those where there is rapid growth in the adoption of IoT devices such as industrial systems, automotive environments and home automation.

References

451 Research, (2015), "Explaining the Internet of Things Ecosystem and Taxonomy", [last accessed 20 Jan 2020], [online] :https://451research.com/images/Marketing/IoT/IoT_Taxonomy_12.1.15.pdf

Antonakakis et al, (2017), "Understanding the Mirai Botnet", 26th USENIX Security Symposium, 2017, August 16, 2017

Ashrad, J., Azad, M. A., Abdeltaif, M.M., Salah, K., (2020), "An intrusion detection framework for energy constrained IoT devices", Mechanical Systems and Signal Processing, Vol. 136, Feb 2020.

Ashton, K., (2009), "That Internet of Things thing", RFID Journal, 2009.

Awasthi, A., Read, H. O. L., Xynos, K., Sutherland, I., (2018), "Welcome pwn: Almond smart home hub forensics", In proceedings of the eighteenth annual DFRWS USA, Portland, Oregon, USA. [online]: https://doi.org/10.1016/j.diin.2018.04.014

DCMS (2018) Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, UK Government, Department for Digital, Culture Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

ENISA, (2017), "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", Nov 2017, [last accessed 20 Jan 2020], [online]: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ETSI, (2019), "CYBER; Cyber Security for Consumer Internet of Things", DTS/CYBER-0039, ETSI, February 2019, [last accessed 20 Jan 2020], [online]: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Fafoutis, X, Marchegiani, L, Papadopoulos, GZ, Piechocki, R, Tryfonas, T & Oikonomou, G, (2017), "Privacy Leakage of Physical Activity Levels in Wireless Embedded Wearable Systems". *IEEE Signal Processing Letters*, vol 24., pp. 136-140

Gartner, (2018), "Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018". [online] : https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

Gartner, (2020), "Gartner Glossary - Internet of Things (iot)", [last accessed 20 Jan 2020], [online]: https://www.gartner.com/en/information-technology/glossary/internet-of-things

GDPR, (2016), "General Data Protection Regulation", REGULATION (EU) 2016/679, European Parliament, 2016. [online] : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Greer C., Burns M., Wollman D., and Griffor E., (2019) "Cyber-Physical Systems and Internet of Things", NIST Special Publication 1900-202, March 2019, https://doi.org/10.6028/NIST.SP.1900-202IDC, (2014), "Internet of Things (IoT) Taxonomy Map", [last accessed 20 Jan 2020], [online] : http://www.idc.com/downloads/IoT_Taxonomy_Map_V2_Nov2014.pdf

IFTTT, (2020), "IFTTT for Business", 2020. [last accessed 20 Jan 2020], [online]: https://platform.ifttt.com/

IoT Security Foundation (2018) IoT Security Compliance Framework v2, [last accessed 26 Jan 2020], [online] https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

Kemal A. Delic., (2016), "On Resilience of IoT Systems: The Internet of Things (Ubiquity symposium)". Ubiquity 2016, February, Article 1 (February 2016), 7 pages. http://dx.doi.org/10.1145/2822885

Lu, X., Qu, Z., Li, Q., and Hui, P., (2015), "Privacy information security classification for internet of things based on internet data", International Journal of Distributed Sensor Networks, 11(8). [online] : http://dsn.sagepub.com/content/11/8/932941.full

Mahidharia, A., (2015), "NORDIC NRF24L01+ – REAL VS FAKE", Hackaday, [last accessed 20 Jan 2020], [online] http://hackaday.com/2015/02/23/nordic-nrf24l01-real-vs-fake/

MITRE, 2020, "Common Vulnerabilities and Exposures", MITRE, 2020. https://cve.mitre.org/

Morgan, J, (2014) "A Simple Explanation Of 'The Internet Of Things'", [last accessed 20 Jan 2020], [online] : https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/

NIST, (2019), "Internet of Things (IoT) Cybersecurity and Privacy Risks", NISTIR 8228, U.S. Department of Commerce, June 2019.

NIST, (2020), "Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline", U.S. Department of Commerce, January 2020.

Sadam, R. and Dasgupta, S. (editting), (2017), "Mondelez 2nd-qtr revenue growth hit by global cyber attack", [last accessed 20 Jan 2020], [online]: https://www.reuters.com/article/us-cyber-attack-mondelez-intl-idUSKBN19R33R

SB-327, (2018), "A*n act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.",* Senate Bill 327, Ch. 886, September 2018. [last accessed 20 Jan 2020], [online]: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Tehranipoor, M., Guin, U. and Bhunia S., (2017) "Invasion of the Hardware Snatchers: Cloned Electronics Pollute the Market", [online]: https://spectrum.ieee.org/computing/hardware/invasion-of-the-hardware-snatchers-cloned-electronics-pollute-the-market

Turner, G, Verbyany, V. , and Kravchenko, S, (2017), "New Cyberattack Goes Global, Hits WPP, Rosneft, Maersk" [last accessed 9 Jan 2020], [online]: https://www.bloomberg.com/news/articles/2017-06-27/ukraine-russia-report-ransomware-computer-virus-attacks

Woolf, N., (2016), "DDoS attack that disrupted internet was largest of its kind, experts say", The Guardian, October 2016, [last accessed 20 Jan 2020], [online]: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Yachir, A., Amirat, Y., Chibani, Y. and Badache, N., (2016), "Event-Aware Framework for Dynamic Services Discovery and Selection in the Context of Ambient Intelligence and Internet of Things," in *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 1, pp. 85-102, Jan. 2016. doi: 10.1109/TASE.2015.2499792

Verisure, (2016), "Home alarm system", [last accessed 20 Jan 2020], [online]: https://www.verisure.no/

Zeptobars, (2015), “Nordic NRF24L01+ - real vs fake : weekend die-shot”, [last accessed 20 Jan 2020], [online]: https://zeptobars.com/en/read/Nordic-NRF24L01P-SI24R1-real-fake-copy