Internet of Things Security Nuggets (IoT Nuggets)

Project number: 2018-1-BG01-KA202-047919

Funding programme: ERASMUS+ Key Action 2: Strategic Partnership, Horizontal priority of Open Education and innovative practices in a digital era.

REVEIW

ULSIT

Contents

IoT security from the view point of regulations

The IoT defies traditional classification and categorization and is still little understood. People have a hard time understanding the concept. To begin to manage IoT risk, institutional leaders must have some vocabulary for it. The IoT is still new, its effects are largely unknown and likely emergent, and its precedents and analogies are few. We need to surface some language and concepts so that it can be discussed [2]. Second, the other risks that the institution faces are still there: safety, liability, financial loss, reputation damage, technology challenges, business competition, and more remain.

As documented in "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures" Gap 2: Lack of awareness and knowledge There is a gap in relation to the increasing move towards connected and interdependent systems and devices as far as knowledge is concerned. In the interviews with IoT experts, differences in fundamental terminology were encountered, such as the difference between the concepts of safety and security. Security experts are more commonly familiar with "business IT" security, but not with IoT security.

There is an overall lack of awareness regarding the need of security in IoT devices. Even more worrisome is the lack of knowledge regarding the threats they are exposed to – most IoT consumers do not have a basic understanding of their IoT devices and the impact on their environment. This may result in the devices not being updated, with a subsequent breach of security.

Moreover, companies should train their employees in good security practices, recognising that technological expertise does not necessarily equate with security expertise. In general, there is a need to properly educate a new generation of consumers, developers, manufacturers, etc. about the use and the security risks posed by IoT, and how to be prepared. It is also necessary to train them in both safety and cyber security to increase awareness.

Many security incidents could be avoided if developers and manufacturers were aware of the risks they face on a daily basis, considering not only those affecting IoT devices but also those affecting the whole IoT environment. This is becoming a common need in order to raise awareness about current threats and risks and to provide knowledge on how to prevent, protect and act in case of a security incident [8].

The research within the project ... identified the following facts. Major world-imposed companies train the Internet security of things at different levels and certify the competencies of the students with tests and certificates. The universities shown in the table offer training with the content specified and award advanced training

The research within the project identified the situation with IoT security trainings in different countries and universities in relation with educational degree and the scope oand goals of trainings.

Major world-imposed companies train the Internet security of things at different levels and certify the competencies of the students with tests and certificates. The universities shown in the research offer training with the content specified and issue diplomas for training.

The study takes into account the three pillars of cybersecurity by most governing documents in Europe, namely the protection of information systems, change management and testing their safety and cyber forensics [10].

Chalanges

Securing IoT devices is challenging for a number of reasons. A rapidly increasing number of gadgets are being turned into smart devices and as manufacturers roll out new products more quickly, little priority is given to security. Eventually we could see almost every home device connected to the Internet, not necessarily with any consumer benefit but instead geared towards data collection, which is incredibly valuable for manufacturers. A lack of awareness among consumers and businesses is also a major obstacle to security, with the convenience and cost-saving benefits of IoT tech appearing to outweigh the potential risks.

Another challenge is securing not only the IoT devices but also the networks over which their data is transferred. In the past, businesses haven't always focused on building end-to-end security into the network. This is set to change as attitudes evolve, with 46 percent of organizations ranking 'securing IoT within the organization as a high priority for 2018, according to the Hiscox Cyber Readiness Report [3].

Security requirements and IoT

This document maps the Code of Practice for Consumer IoT Security against published standards, recommendations and guidance on IoT security and privacy from around the world. Around 100 documents were reviewed from nearly 50 organisations. Whilst not exhaustive, it represents one of the largest collections of guidance available to date in this area.

The scope of applicability This Code of Practice applies to consumer IoT products that are connected to the internet or home network and associated services. A nonexhaustive list of examples includes: • Connected children's toys and baby monitors, • Connected safety-relevant products such as smoke detectors and door locks, • Smart cameras, TVs and speakers, • Wearable health trackers, • Connected home automation and alarm systems, • Connected appliances (e.g. washing machines, fridges), • Smart home assistants. 'Associated services' are here considered as the digital services that are linked to IoT devices, for example mobile applications, cloud computing storage and third party Application Programming Interfaces (APIs) to services such as messaging [9] .

The purpose of the mapping is to serve as a reference and tool for users of the Code of Practice. Manufacturers and other organisations are already implementing a range of standards, recommendations and guidance and will seek to understand the relationship between the Code of Practice and existing material from industry and other interested parties. The mapping makes that exercise easier and, therefore, implementation of the Code of Practice more straightforward.

The mapping represents a snapshot in time. Security guidance across the IoT is rapidly evolving. Whilst gathering the information, it was observed that some

organisations have merged and others are developing their work further, issuing updated versions regularly.

The intention was not to map the entire global technical standards and recommendations space. The mapping was limited in scope to the documentation that claims to be IoT security and privacy related. This means that the mapping does not include those standards and regulations which might be classified as foundational or which underpin the IoT standards, such as the General Data Protection Regulation (GDPR). Also, due to the variance in styles between recommendations, functional equivalence is not possible and so the mappings should be read as indicative only [7].

IoT security and privacy areas and recommendations

The Internet of Things is an element of the cyber physical world that creates many new challenges to security and privacy. These are due to the nature of the Internet of Things, which is characterized by architectural synergy between new telecom services, cloud services and mobile devices, interoperability with the existing Internet. Different threat actors can attack IoT systems at different points in their architecture or organizational decisions. The protection from these attacks is a matter of prophylactic investigation of the security problems and weaknesses in it.In the project we outline four security and privacy areas:

- Authentication and physical threats: highly distributed deployments of a large number of IoT devices, such as RFID tags and wireless sensors,will generally be deployed in public areas without any protection, which makes the devices difficult to manage and vulnerable to physical attacks. For example, an illegitimate sensor may register itself claiming that it is at one location while it is actually at a different location. Or a sensor installed in a room monitoring the room temperature is moved to another room by a malicious person. This introduces the challenge of authenticating IoT devices, which involves recognizing the device and verifying its association with a correct topological address.
- Integrity: the unattended environment for IoT devices also makes data integrity a concern. Once deployed, most of these devices will operate in a self-supported manner. As with very limited maintenance or even no maintenance, tampering data is a much easier task than in a supervised wired network. Further, as a result of a natural loss of calibration or a deliberate perturbation of the measurement environment by an attacker, the data collected by IoT devices is quite likely to have low quality and might be corrupted at the environmental level. In short, IoT data may be noisy and easy to spoof and forge.
- Confidentiality: the communication method between devices and the gateway is primarily wireless, which results in confidentiality risks. For example, eavesdropping is a major concern in wireless networks. Unfortunately, unlike many other wireless environments, such as cellular and Wi-Fi networks, it is difficult for IoT networks to provide confidentiality for data transmission due to the resource-constrained nature of low-end devices, which are a large fraction of IoT devices [30]. Different from typical devices in traditional wired and wireless networks, such as smartphones, tablets, PCs and routers, most of the devices in future IoT networks are active sensors or passive RFID tags, which have very limited resources and capabilities. Constraints on power, computational

capability, storage and other aspects of an IoT device introduce a high barrier for it to perform the necessary operations to achieve data confidentiality, such as through encryption and key management.

- Privacy: as an existing public concern for monitoring and interacting with the real world, the consequence of information leakage in local IoT networks becomes exacerbated when integrated into the global Internet. By connecting real world objects and information through the Internet, data may become accessible to various organizations and domains across the Internet, instead of only being revealed to a small group, which makes it more likely to be exposed to sophisticated malicious parties and therefore increases the probability of being exploited and attacked.

Conventional security and privacy techniques are not necessarily appropriate for the IoT due to the special characteristics of the IoT. The attractive prospect of IoT applications, as well as the strong needs of increasing public confidence about security and privacy issues, requires new and comprehensive solutions to not only protect local IoT devices but also the broader Internet aspect of the IoT. In the following sections, we will examine the problems aforementioned and explore security and privacy techniques to support the IoT infrastructure based on the MobilityFirst network, one of the representatives of future Internet architectures.

Forensics and IoT

Protection and IoT

The implementation of the Internet of Things will result in the connection of tens of billions of wireless devices to the Internet. These devices will form an intelligent substrate pervading all aspects of life. From intelligent home control to advanced city management systems, devices will sense their environment as well as interconnect and communicate with each other to form intelligent smart spaces. Individually and collectively, these devices produce and consume large amounts of personally sensitive data. Japanese Government to Hack Home IOT Devices **(January 25 & 27, 2019)**

A recently-passed amendment to a Japanese law will allow the government in that country to access people's Internet of Things (IoT) devices to conduct a survey of unsecure IoT devices. The amendment allows employees of Japan's National Institute of Information and Communications Technology (NICT) to access people's devices using default passwords and password dictionaries and create a list of unsecure devices, which will be shared with authorities who can then alert consumers. The project is part of an effort to bolster cybersecurity prior to the 2020 Summer Olympic Games in Tokyo.

[Pescatore]

The way this is described makes it sound like the Japanese government is assuming that a major problem is users not configuring "things" correctly, vs. the "things" being built and sold without considering a due diligence level of security. This is kind of like testing the sandwich I bought at a fast food place and telling *me* it has e-coli vs. fining the restaurant that never put the mayonnaise in the refrigerator.

[Ullrich] This survey goes a step beyond what search engines like Shodan will do. The scan will actually try to log in to the devices. Currently, a device connected to the Internet will constantly be scanned for services like Telnet and SSH, and common username and

passwords will be attempted. It is highly unlikely that this government-authorized scan will cause any damage that these unauthorized scans haven't already caused. Owners of vulnerable devices will be notified and asked to improve their security. I find this an interesting experiment and hope it will help remove some of the problem devices.

Read more in: - www.zdnet.com: Japanese government plans to hack into citizens' IoT devices
- www3.nhk.or.jp: Govt. to access home devices in security su

Generic IoT Architecture

Internet-of-Things architecture can be conveniently viewed as an abstraction of several hierarchical layers. Three key layers in the abstraction are the application layer, the network layer, and the perception layer [4].

Many IoT objects have appeared a long time before the concept itself, but they did not have a global dimension, they were not included in the so-called "hyperconnected world". In this category, we mention: connecting IP-based networks, Cloud Computing and Data Analytics. Another IoT characteristic refers to the communications models described by the Internet Architecture Board: The Device-to-Device communication model represents two or more devices that directly connect and communicate between one another, or through an intermediary application server, over many types of networks, including IP networks or the Internet. The Device-to-Cloud communication model starts from the idea that the devices connect directly to an Internet Cloud service. The Device-to-Gateway model means that an intermediary between the Internet device and the Cloud Computing services, consisting of a software application operating on a local gateway device and providing several functionalities (such as data and protocol translation) and security. The Back-end-Data-sharing model presents a communication architecture that enables users to analyse and export data objects from a Cloud service in combination with data from other sources [14]

The for is complicated because of architecture

Chalanges [5]
[13]

The digital forensics of embedded technologies

Iot security and forensics [13]

Internet of Things, wearables, drones, 3D printers even emerging medical devices have a common overlooked thread – all of these new technologies are making use of embedded technologies in their product designs. The concept of connecting devices to the internet by adding network capability is simply an expansion of the embedded technology

platforms that have existed for quite some time.With the rapid growth and expansion of these new network connect technology platforms, one area of science is struggling to keep pace. Digital forensics is the branch of forensic science concerned with the recovery and investigation of data found on digital devices. As these new and updated platforms based on embedded technologies emerge, the industry and practitioners struggle to develop the tools and procedures to keep pace with the technology.

Embedded technologies are electronics or computing systems with specific functions that may exist as part of a larger platform. An embedded technolo gy design includes some or all of the following components: a PCB (printed circuit board), microcontroller, RAM, flash memory, and networking capabilities (e.g. Bluetooth, WiFi, GSM). In the case of modern embedded technologies designs, the larger Platform may include other wireless connected devices and centralized storage systems (e.g. wearable device connected to smartphone, synchronizing to the cloud).

The Internet - enabled refrigerators and kitchen appliances are great examples of a new embedded technology device which is not a full computer in the traditional form factor we have grown ccustomed to, yet the devices enough technology inside for it to talk to a network, receive commands and send statuses. When you call your investigation team to ask them was this internet - enabled refrigerator the source of infection on your network, they will likely look with blank stares as they try to figure out how to get started examining the device. Is there data with evidentiary value within these new technology devices? Does it exist on the device or across a network connection retrieving and storing the information[17]?

The Critical Issue of IoT Security

Autonomous IoT devices are usually small, inexpensive and don't have much computing power. That also means they have little capability to protect themselves from being hacked.

Here are a few reasons why we need solid research on how to provide security solutions for IoT:

- Almost every IoT system is cloud-based. Even if most cloud-based applications are secure, the cloud is another point of entry that could be a security risk.
- We don't completely trust IoT devices or systems. For example, if we're riding in a futuristic self-driving car, how do we know that car hasn't been compromised in some way?
- Imagine that your house is an IoT device. Things go in and out through windows and doors, but squirrels find a hole in the attic and get in via a path you didn't intend. This happens in computing, and can happen to IoT devices. We don't yet know all the side channels that can be used for attacks.

An Interdisciplinary Approach to Security Works

Although IoT security may seem like an IT-only problem, it helps to think about it from nontraditional perspectives. For instance, consider the concept of resilience. **Most computer networks** aren't particularly resilient. Removing a small piece of software can bring a whole network down [1]. This can be for example time protocol demon [18].

IoT initiatives into real-world urban applications "seeks to bring an interdisciplinary approach to enable a Smart City to be more connected and sustainable by combining methods from computer science, the social sciences, interaction design, and architecture in order to improve how cities are managed and maintained and enhance citizen well-being [12].

IoT Security in education

Education is also key and makers of IoT devices, ISPs and the government must play a vital role in boosting awareness of IoT security among consumers and businesses. At a government level, it may also be necessary to provide education to boost the digital literacy of policymakers. More regulation and standardization is needed to ensure that IoT devices adhere to a certain level of security, while manufacturers must develop clear privacy policies for their IoT devices and ensure that consumers know how to adjust the security settings. Even simple steps such as not setting default passcodes as "0000" or "1234" could help keep devices more secure in the future.

While security has too often taken a back seat in the development of IoT technology, manufacturers must begin to build protection into their devices. Network providers can also help address the IoT security threat by creating end-to-end infrastructure that meets industry-wide standards. Providers that offer a secure network will have a competitive advantage in the long run [3].

IEEE Guide to the Internet of Things Course Program

New online course program from IEEE covering industry applications for the Internet of Things, along with challenges and future opportunities. Includes topics such as IoT software, limitations of wireless technology, reference architecture and use cases.

Course Titles Include:

What is the Internet of Things?

IoT Software: Fundamental Concepts and State of the Art

Exploring IoT Industry Applications

The Evolution of Internet of Things for Healthcare

Limitations of Wireless Technology for Healthcare IoT

Paving the Way for Future IoT Applications in Healthcare

Reference Architecture and Use Cases

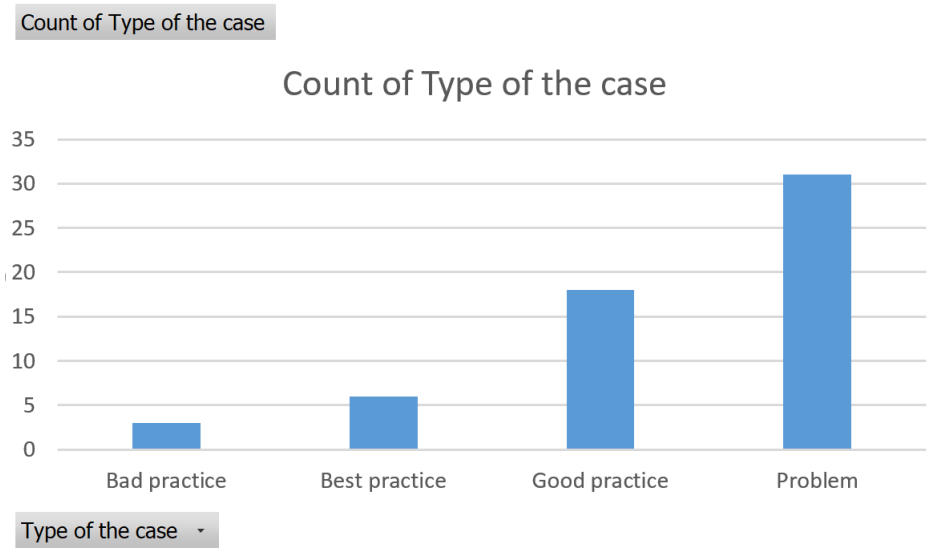
Social Internet of Things
The Emerging Paradigm of the Social Internet of Things
Existing Platforms

In two short years, there could be nearly 30 billion autonomous Internet of Things devices on our networks. Unlike computers and smartphones, these sensors, appliances, controllers and other devices talk to each other **without requiring human interaction**.

All of this new technology presents a major security risk. Recently, at the University of Kansas, we won a research grant from the National Security Agency to study how we can make IoT devices safer from cyberattacks.

We put together a multidisciplinary team of computer scientists, electrical and computer engineers, psychologists, sociologists and philosophers to provide unique perspectives and find solutions to the problem.

READ: *Check out what experts are saying about what is on the horizon for campus IoT security!*



UNIK4750 – Measurable Security for the Internet of Things, PhD

Course content. The course provides a methodology for measurable security, privacy, and dependability of industrial systems. Based on e.g. a smart grid example we will establish and develop the methodology to perform a multi-metrics analysis from components to sub-systems to systems. The course will allow you to compare security-related application goals with the results from the system analysis.

Learning outcome. After completing the course you will be able to:

- Describe application-driven security and establish challenges of sensor-driven systems;
- Provide industrial examples, e.g. Smart Grid and automatic meter readings;
- Establish application-driven security goals as well as the semantics of your system;
- Generate matrices to describe the security impact of components and sub-systems, and perform a multi-metrics analysis to establish the system security;
- Analyze application goal versus system security and suggest improvements.

The Internet of Things: Education and Technology

While these concerns are significant, they do not, however, seem to dampen enthusiasm for the IoT. This confidence – or at the very least lack of care – can be due to the complexities with how consumers and citizens view the relationships between information, technology, trust, privacy and power. We are at once increasingly sceptical and more liberal with our expectations of privacy.

Indeed, particularly since the 9/11 terror attacks in 2001 there has been a widespread shift in the expectations of citizens in the US, and increasingly Europe, Australia and New Zealand, that personal freedoms must be curtailed to safeguard against terrorism. For example, the implementation of the Patriot Act in the US (with Patriot standing for Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) in the aftermath of these attacks integrated a number of incursions and sweeping changes into personal privacy, including the ability of law enforcement agencies to search an individual's home without notice and without informing that individual (Rubel, 2007). This 'status quo' in privacy went unchecked and unconsidered for a number of years.

However, in 2013 Edward Snowdon's leaks involving the National Security Agency (NSA) and PRISM – the code name for the NSA body which collects internet -based communications and carries out covert surveillance against American citizens – offered a correction in public attitudes towards privacy. Nevertheless, with ongoing violence, particularly in Europe, involving Islamic State, the need to 'empower' police and anti-terrorist organisations remains a powerful trope in the public imagination.

Furthermore, the role of social media has blurred expectations of privacy – users of Facebook for example utilise the platform to share personal information to both friends and strangers despite its long history of poor privacy protections. In 2005 users' passwords were being sent across the web without encryption. According to Debatin, Lovejoy, Horn, & Hughes (2009):Even the most lauded privacy feature of Facebook, the ability to restrict one's profile to be viewed by friends only, failed for the first 3 years of its existence: Information posted on restricted profiles showed up in searches unless a user chose to opt-out his or her profile from searches. This glitch was fixed in late June 2007, but only after a technology blogger made the loophole public and contacted Facebook.

However, despite this, Facebook has often only made adjustments or introduced protocols when users have outraged en masse. Therefore, with governments seemingly

regularly invading the privacy of citizens, and with corporate capitalism insinuating itself as the dominant means by which we relate to each other and world, people now seem to be more willing to put their faith in corporations to protect their privacy. The attractions of the IoT – the interaction with real-time data and delivery of information, contextually aware systems meeting spoken and unspoken demands, personalisation of environments and control over micro-experiences – offers up privacy as the terrain upon which a struggle over self and security take place. Indeed, the IoT is positioned in the space where the circulation of personal information is required for the system to effectively operate – the desire to have personal information known, tracked, logged and interpreted is the core trope of the IoT.

Ensuring that information is not being transmitted to an unsanctioned third party – either human or machine – is therefore a core tension within the IoT architecture.

For example, Thingful is a search engine for the IoT (https://www.thingful.net/) which offers an interface to search for and locate any IoT device in the world. It assures users that "Our mission is to enable an interoperable Internet of Things, in which connected objects find and use each other's data with the active consent of their owners" (Thingful, 2017a, para. 1).

However, it is not made clear how this active consent is obtained, except that users/owners are invited to input or register a device. Further, in a video presentation at the ODI (Open Data Institute) Summit in London in 2015, founding partner of Thingful Usman Haque made rather opaque claims about the nature of the search engine and the way data is managed (Open Data Institute, 2015):[15]

EIT Digital's new Internet of Things security course

EIT Digital has launched a new massive open online course (MOOC). The new 'Web Connectivity and Security in Embedded Systems' course is the latest in EIT Digital's growing suite of MOOCs on the Coursera education platform.

The Web Connectivity and Security in Embedded Systems MOOC is the third installment of EIT Digital's course on Hardware and Cyber Physical Systems. It compliments existing MOOCS on Development of Real-Time Systems and Embedded Hardware and Operating Systems [6].

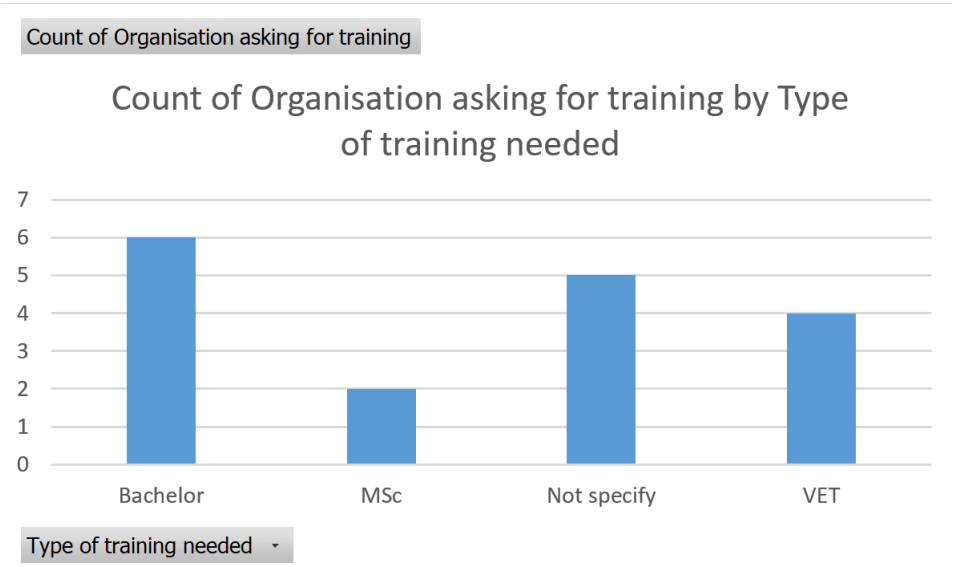
This latest installment explores several technologies that bring modern devices together to facilitate a network of connected things and make devices internet enabled. The course centers on the problem of web connectivity in cyber-physical systems and on security measures. Each module ends with a graded quiz, and there is a final peer reviewed exam at the end of the MOOC. After completing this course, students will have the basic knowledge and skills for designing network architecture for cyber-physical systems, will be able to define security requirements for their system, as well as being able to implement a proper security and privacy technique to protect it.

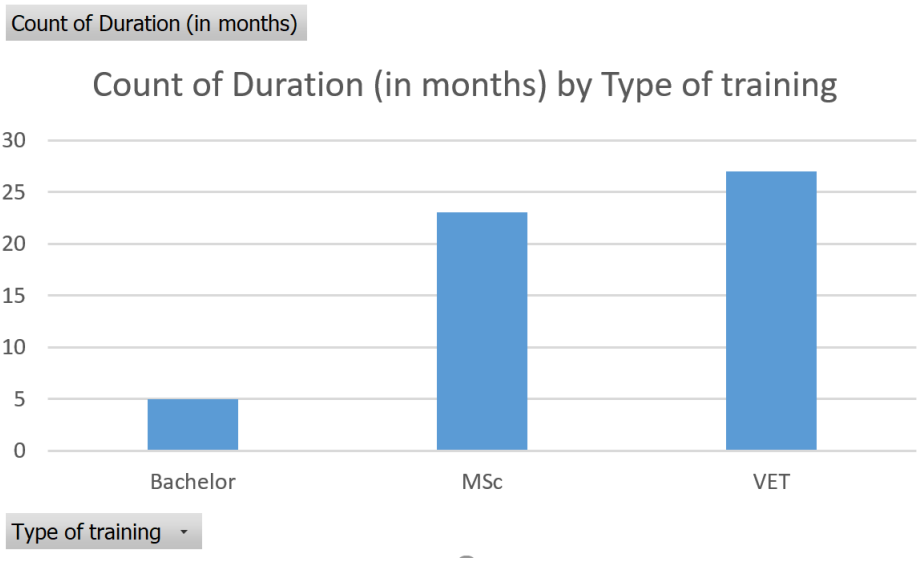
EIT Digital MOOC programmes are part of the online learning programme of the EIT Digital Academy. The new course is, like all other MOOCS, aimed at bachelors and masters students as part of their on-campus courses, but is also accessible for anyone who likes practical programming and making IoT applications.

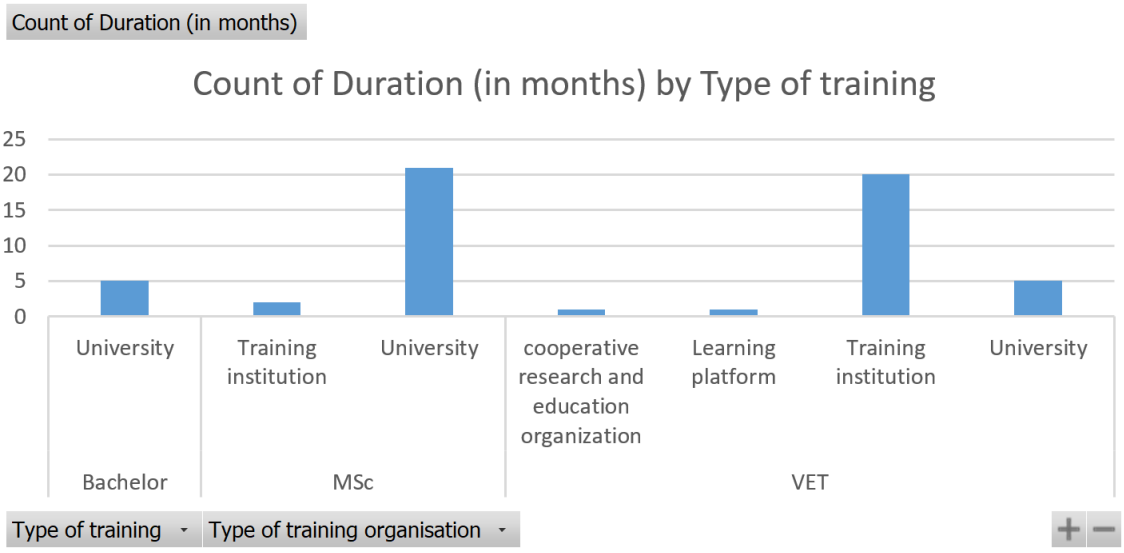
'*Our MOOCS are interesting for lifelong learning*,' says Martijn Klabbers, Online Education Activity Lead at EIT Digital and Project Developer and Manager at Eindhoven University of Technology. '*We see a lot of professionals in our MOOCS. For professionals these MOOCS are ideal as a refresher course and for getting an update on the latest developments. MOOCS can also be used to prepare professionals for the online courses in our Professional School which are more practice-oriented*.'

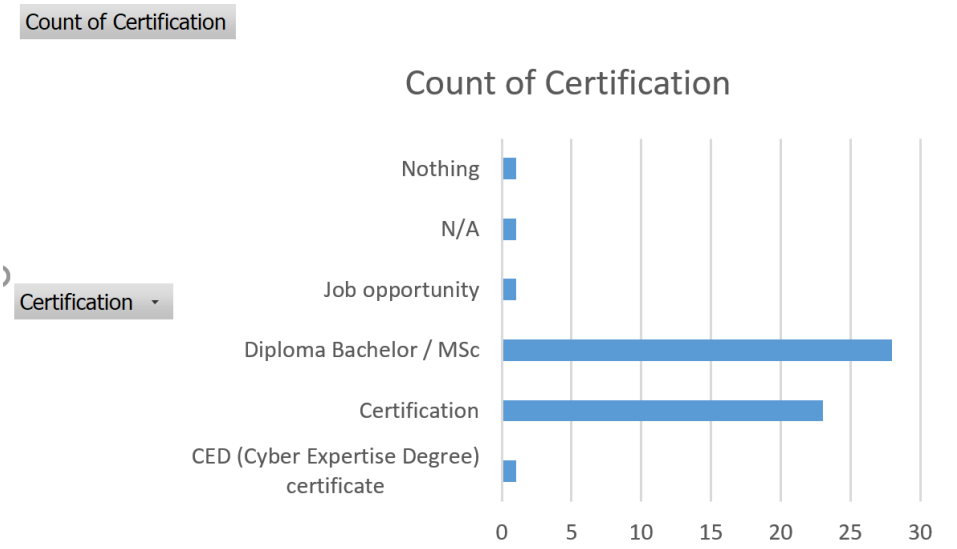
The new MOOC takes six weeks to complete including about five to seven hours of studying per week. The complete Hardware and Cyber Physical Systems course is equivalent to five European Credit Transfer and Accumulation System points (ECTS) - the standard for comparing the study attainment and performance of students of higher education across the European Union and other collaborating European countries.

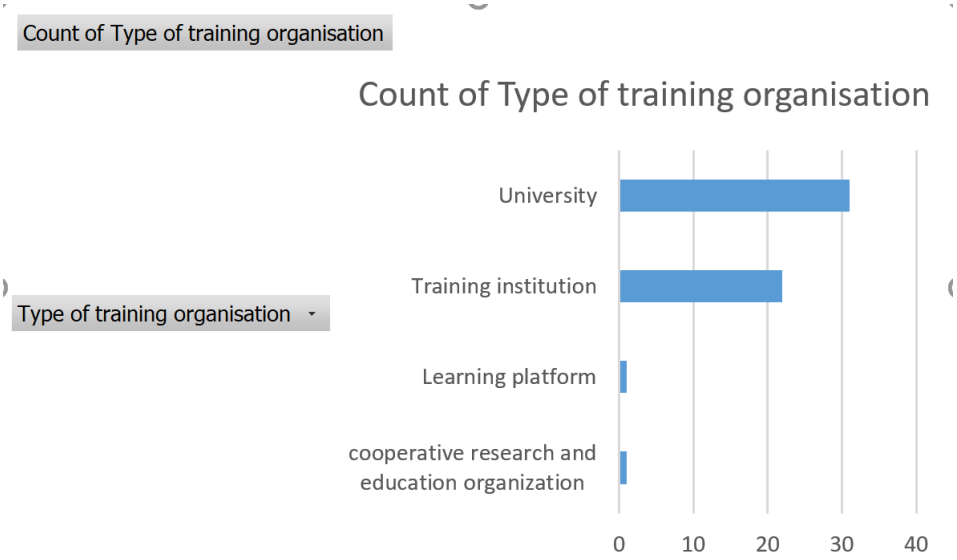
Learners can take the course for free or pay 50 Euros to receive a certificate. EIT Digital uses Coursera as the technical delivery platform for its MOOC offering. EIT Digital now has nine MOOCs on this platform and is set to launch more in the following months. Content for EIT Digital MOOCs is provided by EIT Digital's academic partners [11].




Count of Duration (in months)
Count of Duration (in months) by Type of training
30
25
20
15
10
5
0
Bachelor
MSc
VET
Type of training


Count of Duration (in months)
Count of Duration (in months) by Type of training
25
20
15
10
5
0
University
Training institution
University
cooperative research and education organization
Learning platform
Training institution
University
Bachelor
MSc
VET
Type of training
Type of training organisation





Security issues concerning state of the art technologies

To address the critical security, safety and privacy risks of these devices while retaining open connectivity options, scalability (due to high number of devices), interoperability and application independence (different devices and purposes), we require new solutions. Nowadays, securing data, objects, networks, infrastructure, systems and people under IoT is increasingly relying on Cognitive Systems, Machine Learning, Artificial Intelligence and Distributed Ledger technologies (DLT) and new decentralised approaches [16].

How blockchain might help to secure IoT devices in the future. Best known as the backbone of cryptocurrency Bitcoin, blockchain is a shared ledger where data is automatically stored across multiple locations. The indisputable digital paper trail makes it ideal for financial applications, but it could also be applied to IoT.

IoT devices increase the amount of entry points into a home or business network, which in turn could give hackers access to devices such as computers that contain sensitive data. Using blockchain technology could reduce the risk of IoT devices being put at risk by a security breach at a single point. By getting rid of a central authority in IoT networks, blockchain would enable device networks to validate and protect themselves. For example, devices in a common group could potentially stop or alert the user if asked to carry out tasks that appear unusual, such as being commandeered by hackers to carry out Distributed Denial of Service (DDoS) attacks [3].

Atzori et al. (2010) also demonstrate that security and privacy issues are irrevocably intertwined. Not only is the ability to secure the IoT – despite authentication and passwords, encryption and data management – extremely difficult, it is actually counterintuitive to the intentions and expectations of the system that promotes the free movement and accessibility of data in realtime. Indeed, free and accelerated sharing, communication, transmission and interaction are core tropes of the IoT. However, these needs of mobility and timeliness, along with the advocacy of context aware technology that is embedded in the IoT construct, means that privacy – the ability to control who knows what about us when – is extremely compromised. Indeed, these low-tech, highly mobile constructs of the IoT can lead to extraordinarily invasive conditions of surveillance where "unseen by users, embedded RFID The Internet of Things: Education and Technology

tags in our personal devices, clothes, and groceries can unknowingly be triggered to reply with their ID and other information" (Atzori et al., 2010, p. 2793). These circumstances create situations where individuals are being monitored and transmitted in time and space information such as where they are, where they have been, how much time they spent in a location are just a few examples. Our prior research shows that people with disability are particularly resistant to intensive monitoring of this kind (see Ellis, Kent, Locke, Hollier, & Denney, 2017). All of this overvigilance can lead to consumer outrage and protest. Such was he case in 2003 when Italian clothing company Benetton revealed they intended to tag an entire line of their clothes at more than 5000 stores globally, involving 15 million chips (Violino, 2003).

While Benetton eventually reneged on the idea after the 'I'd rather go naked' campaign launched by CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) drew public spotlight to the plan, the company still received widespread criticism. However, other companies have not been deterred and, with less fanfare, have slipped RFID tags into their inventory. Gillette had already purchased 500 million tags in 2003. In 2004 Wal-Mart and Abercrombie and Fitch utilised RFID in their logistics, the latter following Benetton's idea but instead placing the tags in all their items instead of just one collection.

Yet this does not mean that no attempts have been made to counter these issues. As early as 2001 a US patent application was lodged for a device which addressed the

privacy and security issues involved in RFID tracking. It claimed that "the widespread use of RFID tags on merchandise such as clothing would make it possible for the locations of people, animals, and objects to be tracked on a global scale – a privacy invasion of Orwellian proportions" (Hind, Matthewson, & Peters, 2002, para. 0011). Tellingly, however, commercial interests always seem to win – just 3 months later the same team lodged another patent to identify and track persons using RFID -tagged items in store environments. Indeed, over the years, it appears as though the widespread – and socially and commercially accepted – potential of RFID has masked or silenced much of the anxiety about its possible privacy problems.

This lack of concern is in part due to the perceived benefit of – and trust in – the middleware used in the IoT. This software is tasked with solving security problems and therefore "must include functions related to the management of the trust, privacy and security of all the exchanged data" (Atzori et al., 2010 p. 2793). Yet exactly how middleware will achieve this has been the subject of much speculation. The general consensus appears to be that middleware must solve a problem specific to the IoT as "traditional security countermeasures and privacy enforcement cannot be directly applied to IoT technologies due to their limited computing power" (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015 p. 146). Importantly, middleware must also be able to provide security at all three major layers of the IoT network – the perception layer (RFID tags), the network layer (wireless networks) and application layer (devices).

However, the context-aware nature of the IoT means that devices are constantly gathering and distributing personal information – ranging from a person's location, to their purchase preferences, to the ambient temperature of their living environment or even the serial number of their pacemaker. Thus, any security system must address the issues of "authentication, confidentiality, and access control" to offer a secure and robust privacy paradigm (Sicari et al., 2015, p. 148). The heterogeneous nature of the IoT network also means that different devices with different protocols must be able to talk to each other with a common security protocol that is able to maintain "anonymity, trustworthiness and attack resistance" (Sicari et al., 2015, p. 148). These difficulties mean that "Most existing middlewares' authentication-based partial security solutions are insufficient for a number of IoT applications" (Razzaque, Milojevic -Jeric, Palade, & Clarke, 2006, p. 90), thereby demonstrating how difficult it is to provide viable and functional security protocols to ensure complete privacy protection throughout the IoT.

Conclusions and Recommendations

Students with disabilities are under represented in higher education in Australia and have a lower completion rate for their studies than their fellow students. The IoT therefore offers great potential for both the greater inclusion of students with disabilities in higher education

and a better and more customised learning experience for all students. However, this research has shown that the technology, while evolving, is not yet at a point where it could be effectively deployed in learning and teaching at the university level.

Nevertheless, it does show great potential. The ability to analyse information from a range of different sources and present it, to alter physical and digit al nvironments to best meet learners' and teachers' needs, and to present customised information and communications options to best suit the needs of a user through a device that they are familiar with presents the opportunity to champion a social model approach to disability where each environment is customised to meet the needs of an individual, rather than that individual being forced to adapt to an inaccessible environment.

For this potential to be realised, consideration of the wider significance of the relationships between technology and society, education and disability, access and literacy, is needed.

Concerns about privacy and security and interoperability associated with the technology will need to be overcome, and careful consideration of how the technology can best be adapted to a learning and teaching environment will be needed. However, interviews from this study

with students with disability indicate a willingness to overcome these limitations and embrace the potential of these new technologi

es as they develop over time.

This report recommends, in relation to the deployment of the IoT in an educational setting, that:

- Curtin University should not immediately deploy IoT technologies, but that careful consideration and planning be undertaken for how this might best be done in the future and what implication this might have.
- Priority should to be given to incorporating IoT within specific edagogical issues regarding learning and teaching, with particular consideration being given to the integration of students with disabilities. This is in addition to Curtin's current focus on integrating IoT technologies primarily in association with facilities management.
- Any IoT equipment associated with learning should have the ability to provide its output to students via a learning management system or app. This would ensure that students with disabilities can process the data with their preferred assistive technology.
- Any future implementation of IoT solutions should focus around the use of personal smartphones as the primary IoT interface device for students with disabilities.
- All IoT-related implementations must also consider privacy, security and interoperability.
- Any IoT solution must be accompanied by training to ensure that all staff and students are able to use it effectively.
- The applicability of using a digital assistant as a real time captioning device warrants further research.

• A trial of the use of existing technologies and further consultation with industry and students should be undertaken over 2018.

https://docs.google.com/spreadsheets/d/1LoQJiGLO39sPiuSh-wQm-oGEVlYXn8AzmfUY0l_Lv1A/edit#gid=2070465107

https://docs.google.com/spreadsheets/d/1cG9YzMX9clNADY4IdmxSRXLt5ZXpL28sUUFlzr8iCpA/edit#gid=668078068

https://docs.google.com/spreadsheets/d/19MwJdRLlxTa80yu5Uj1h9VxKqgJor_b9ShJGmzfHCSo/edit#gid=704184015

https://articles.forensicfocus.com/2017/05/17/internet-of-things-mobility-forensics/

https://www.uio.no/studier/emner/matnat/its/UNIK4750/index-eng.html#course-content

https://eit.europa.eu/newsroom/eit-digitals-internet-of-things-security-course

[1] Perry Alexander. Why IoT Security Requires an Interdisciplinary Approach, 1 2019. [Online; accessed 30. Jan. 2019].

[2] Chuck Benson. The Internet of Things, IoT Systems, and Higher Education, 1 2019. [Online; accessed 31. Jan. 2019].

[3] Srinivasan C. R. Is the Internet of Things Impossible to Secure? *https://www.securitymagazine.com/articles/89098-is-the-internet-of-things-impossible-to-secure*, 6 2018.

[4] Kejun Chen, Shuai Zhang, Zhikun Li, Yi Zhang, Qingxu Deng, Sandip Ray, and Yier Jin. Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice. *Journal of Hardware and Systems Security*, 2(2):97–110, may 2018.

[5] Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. Internet of things security and forensics: Challenges and opportunities. *https://arxiv.org/pdf/1811.09239.pdf*.

[6] Coursera. Web Connectivity and Security in Embedded Systems Coursera, 1 2019. [Online; accessed 31. Jan. 2019].

[7] Media Department for Digital, Culture and Sport. *Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security*. 2018.

[8] ENISA. *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*. 2017.

[9] UK Department for digital cultureq media and sport. *Code of Practice for Consumer IoT Security*. 2018.

[10] http://ec.europa.eu/information_society/newsroom/image/document/2017 3/factsheet_cybersecurity_update_january_2017_41543.pdf. *EU cybersecurity initiativesworking towards a more secure online environment*. 2017.

[11] https://eit.europa.eu/newsroom/eit-digitals-internet-of-things-security course. EIT Digital's new Internet of Things security course, 10 2016. [Online; accessed 30. Jan. 2019].

[12] Intel.com. Smart cities uk: Imperial college and intel iot projectвЂ"the internet of things worldwide with intel inside, 2017.

[13] Umit Karabiyik and Kemal Akkaya. Digital forensics for iot and wsns. *https://arxiv.org/ftp/arxiv/papers/1807/1807.10438.pdf*.

[14] Lyman Chapin Karen Rose, Scott Eldridge. *The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World*. 2015.

[15] Mike Kent Leanne McRae, Katie Ellis. Internet of things (iot): Education and technology the relationship between education and technology for students with disabilities. *2017 Curtin Learning and Teaching Innovation Grant*, 2017.

[16] Konstantinos Loupos. Fighting for cybersecurity: eight new EU funded projects for a more secure IoT - Digital Single Market - European Commission, 10 2018. [Online; accessed 31. Jan. 2019].

[17] S Watson and A Dehghantanha. Digital forensics : the missing piece of the internet of things promise. *University of Salford, Manchester*, 16(2):102–112, may 2016.

[18] Sofia Willian Dimitrov. *ICT Security Model*. Avangard Prima, 2018.