



Internet of Things security nuggets

IoTnuggets

2018-1-BG01-KA202-047919

SYLLABUS

This project was financed by the EU programme ERASMUS+. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the European Union.



CONTENTS

Overview	3
Training approach	4
Syllabus.....	5
Learning Objectives.....	5
Topics	5
Understanding IoT Architecture.....	5
Need of Internet of Things (IoT) Security.....	6
IOT Communication Protocol.....	6
IOT Technology Standards.....	6
Security Classification & Access Control	6
Attacks & Implementation	6
Cryptography	6
Attack Surface and Threat Assessment.....	7
Security Management	7
Intrusion Detection and Prevention.....	7
IoT Security and the Law	7
Case Studies and Discussion.....	7
References and Contributions.....	10
Introduction to IoT Security	11
IoT Ethics and Privacy.....	11
Building Automation and Security	11
IoT in Energy and Environment.....	12
IoT in Infrastructure	12
IoT in Healthcare	13
IoT Consumer Electronics.....	13



OVERVIEW

The Internet dramatically changed the world around us. Billions of computers, devices and sensors work together in so called Internet of Things (IoT). The new sets provide different services and understanding for a single item. The network evolution becomes more complex and the cybersecurity needs increase. The understanding of cybersecurity challenges is the main goal of this course. The IoT set is secure as much as the weakest link or device in it. This course delivers the awareness of SMEs staff to new IoT realm. The course will introduce the security and vulnerabilities in IoT technologies and systems as well as cybersecurity policies, practices and principles.

Every module will include learning nuggets as readings, videos, case studies, and a quiz to help make sure you understand the material and concepts. This course offers a place to learn, reflect, and plan for a smart community approach to IoT.

The IoT ecosystems have own life, technologies and principles in cybersecurity to protect end user. The connected devices, operating systems, sensors, data storage, networking and communication protocols, and system services have to be projected together.

This training is developed under the project Erasmus+ Internet of Things Security Nuggets Erasmus+ Project N° 2018-1-BG01-KA202-047919 granted by European Commission.

IoTnuggets aims VET training how to apply the IoTnuggets Methodology to unearth a wide range of new options and ultimately to secure their SMEs and world that is facing digitalization rapidly. In this respect, it is developing new methodology and content, based on ICT, as it foresees full utilization of such tools and development of digital skills for vocation training in new more appropriate way with learning nuggets – fast and widespread methodology for informal training.



TRAINING APPROACH

The learning approach is a response to the needs of trainers for quick and adequate tailor-made course. The vision is that due to the fast-paced changes taking place in life and practice, the adaptation of the education process to this dynamic could and should happen in a (r)evolutionary way with “nuggets”.

Learning nuggets is a standalone mini learning activity, usually less than 5 minutes in length, that would vary in size and scope that learners undertake in a particular context in order to attain specific learning outcomes¹. A learning nugget task will take a prescribed length of time and may, or may not be assessed. Nuggets should be designed with a particular approach to learning and teaching in mind²

Learning nuggets are the essential elements of the Subscription Learning approach. In this context, the learning happens through a stream of intermittent nuggets which involves a variety of learning-related events which include "content presentation, diagnostics, scenario-based questions, job aids, reflection questions, assignments, discussions, etc."³ The nuggets are delivered to the learner in many format like email, text message, smart-phone notifications, or any other form of prompting. They are designed to be delivered on predetermined intervals to support learning. The series of learning nuggets are called learning threads. For utmost effective learning, sending a learning nugget could be dynamically triggered by many factors like learners' leaning need, results of a learning assessment or learners' performance.

Target group:

- VET providers and trainers in the ICT giield
- Software engineers and programmers who need and want to specialize in cybersecurity of the ecosystem of IoT

¹ Polsani, P. R. (2003). "Use and Abuse of Reusable Learning Objects". Journal of Digital Information. 3 (4). Retrieved 12 June 2017.

² Conole, G. C.; Fill, K. (2005). A toolkit for creating effective learning activities. Montreal: Ed-Media World Conference on Educational Multimedia, Hypermedia & Telecommunication.

³ "What is it: Subscription Learning Defined". SubscriptionLearning. Archived from the original on 1 October 2017. Retrieved 4 October 2015.



SYLLABUS

The following syllabus is an exhaustive description of security in the field of IoT. It has been developed with great level of detail, not with the objective of transferring every one of the items described to learning objectives, but to provide a broad context according to the diversity nature and level of knowledge learners. This broad context will allow to be adapted to learning outcomes for each nugget.

Understanding the cybersecurity in each of 7 IoT layers is significant for learners. These layers are:

1	Device connection	IoT devices, IoT connectivity, Embedded Intelligence
2	Data Sensing	Capture Data, Sensors and tags, Storage
3	Communication	Focus on across, Networks, cloud, edge, Data transport
4	Data Analytics	Big data analysis, ai and cognitive, analysis at the edge
5	Data Value	analysis to action, APIs and processes, Actionable intelligence
6	Human Value	Smart Applications, Stakeholder benefits, Tangible benefits
7	Data protection regulations	

Learning Objectives

- Classify the components of the IoT ecosystem, including devices, computers, networks, operating system services, and distributed systems.
- Evaluate core cybersecurity principles from an IoT perspective
- Distinguish system, service, application, and network security and privacy threats and vulnerabilities on client and server systems.
- Analyze technologies commonly used in IoT sensors, storage, communication, and system services
- Analyze IoT devices and systems from a cybersecurity perspective
- Implement and use computer-based tools to examine IoT network and security issues
- Demonstrate techniques for exploitation and vulnerability mitigation in IoT devices and systems.

Topics

Understanding IoT Architecture

- IoT devices
- IoT connectivity (Device to device, device to cloud, device to gateway, cloud to Gateway)
- Embedded intelligence



- Data sensing (capture data, sensors and tags)

Need of Internet of Things (IoT) Security

- Main Challenges and Security Issues: poor cybersecurity awareness
- The lifecycle of an attack
- Confidentiality, integrity, availability, non-repudiation
- IoT vulnerabilities (weak authentication, unprotected communications, complex system administration, open access to organizational data).
- IoT safeguards (access control, audit, authentication, biometrics, cryptography, deception, denial of service filters, ethical hacking, firewalls, intrusion detection systems, response, scanning, security policy, threat management).
- Need for a comprehensive cybersecurity IoT policy.

IOT Communication Protocol

- Networks, Clouds, Edge, data transport.
- Application Layer Protocols (MQTT, CoAP, HTTP, Web socket, DDS, AMQP)
- Transport Layer Protocols (TCP, UDP)
- Network Layer Protocols (IPv4, IPv6, LowPAN)
- Link Layer Protocols (Ethernet, WiFi, WiMax, Cellular)

IOT Technology Standards

- Wired Communication Protocols (UART, USART, I2C, SPI, Ethernet, JTAG)
- Wireless Communication Protocols (Bluetooth, Zigbee, 6lowPAN, WiFi, Z-wave)

Security Classification & Access Control

- Data Classification and criteria (Public, Private, Sensitive, Confidential, Proprietary)
- Privacy Issues in IoT
- IoT Ecosystem Access Control
- Authentication, Authorization, Accounting
- Data Integrity

Attacks & Implementation

- Risk of IoT
- Vulnerability Exploitation
- Attacks of Privacy (Phishing, Pharming, DNS Hijacking, Defacement, Eavesdropping, Cyber Espionage)
- Web Based Attacks (Malware, Password, Access, Social Engineering, Data & Identity Theft, Reconnaissance)

Cryptology

- Cryptography
- Symmetric Key Algorithms (AES and DES)
- Asymmetric Key Algorithm (RSA)



- Attacks (Dictionary and Brute Force, Lookup Tables, Reverse Look Tables, Rainbow Tables)
- Hashing (MD5, SHA256, SHA512, RipeMD, Whirlpool)

Attack Surface and Threat Assessment

- OWASP Top 10 (IoT Hacking & Security)
- IoT Attack Surface
- Software and Cloud Components
- Firmware of the devices
- Web Application Dashboard
- Mobile Application used to Control, Configure, and Monitor Devices
- Threat Assessment

Security Management

- Identity and Access Management
- Key Management

Intrusion Detection and Prevention

- Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsider, Malware infection,
- Intrusion detection and prevention Techniques
- Anti-Malware software
- System Integrity Validation.

IoT Security and the Law

- Cybersecurity Regulations, Roles of International Law, the state and private sector in cyberspace, cyber security standards.

Case Studies and Discussion

The course will pass through some of the more common IoT devices in use in:

- Smart Homes
- Smart Retail Supply
- Smart Healthcare
- Smart Grid
- Smart Cities
- Smart Industry

and how they are used as well as security and privacy-related issues found with these devices.

Specific objectives for different target groups: All Users, Manager, Start Up's, Smart Factory. Their workplaces are different – office, home, street, industrial manufacturing, hotels. They have to be aware of several aspects of the IoT cybersecurity listed in the table below Table 1:

Table 1 Syllabus v Profiles

		All Users	Manager	Start Up's	Smart Factory
Understanding IoT Architecture	IoT devices	x		x	x
	IoT connectivity	x		x	x
	Embedded Intelligence	x		x	x
	Data Sensing	x		x	x
Need of Internet of Things (IoT) Security	IoT Security challenges	x	x	x	x
	Confidentiality	x		x	
	Integrity	x		x	
	Availability	x		x	
	No-Repudiation	x			
	Access Control	x	x	x	
	Weak Authentication	x	x	x	x
	Unprotected Communications	x	x		x
	Biometrics	x			
	Denial Of Service Filtering		x	x	x
	Ethical Hacking		x	x	
	Firewalls			x	x
	Intrusion Detection Systems			x	x
	Threat Management		x		x
	Security Policy		x	x	
Audit		x	x		
IOT Communication Protocol	Networks, Clouds, Edge, Data Transport		x		x
	TCP/IP Reference Model			x	x
	Application Layer Protocols (MQTT, CoAP, HTTP, Web socket, DDS, AMQP)				x
	Network Layer Protocols (IPv4, IPv6, LowPAN)			x	x
	Link Layer Protocols (Ethernet, WiFi, WiMax, Cellular)	x		x	x
IOT Technology Standards	Wireless Communication Protocols (Bluetooth, Zigbee, 6lowPAN, WiFi, Z-wave)	x		x	x
Security Classification & Access Control	Data Classification and criteria (Public, Private, Sensitive, Confidential, Proprietary)	x		x	x
	Privacy Issues in IoT	x	x		
	IoT Ecosystem Access Control		x		x
	Authentication			x	x
	Authorization			x	x
	Accounting			x	x
	Data Integrity		x		x
Cryptology	Cryptography	x			

	Symmetric Key Algorithms (AES and DES)				x
	Asymmetric Key Algorithm (RSA)				x
	Attacks (Dictionary and Brute Force, Lookup Tables, Reverse Look Tables, Rainbow Tables)		x	x	x
	Hashing (MD5, SHA256, SHA512, RipeMD, Whirlpool)			x	x
Attacks & Implementation	Risk of IoT	x	x	x	
	Vulnerability Exploitation	x	x		x
	Attacks of Privacy	x	x	x	x
	Web Based Attacks	x	x	x	x
Security Management	Identity and Access Management				x
	Key Management			x	x
Intrusion Detection and Prevention	Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access, Malware infection	x	x		
	Intrusion detection and prevention Techniques				x
	Anti-Malware software				x
	System Integrity Validation.				x
IoT Security and the Law	Cybersecurity Regulations and standards.		x		
Case Studies and Discussion	Smart Homes	x	x	x	
	Smart Retail Supply	x	x	x	
	Smart Healthcare	x	x	x	
	Smart Grid	x	x	x	
	Smart Cities	x	x	x	
	Smart Industry	x	x	x	

REFERENCES AND CONTRIBUTIONS

This syllabus is the result of research work on competence frameworks, specifically in the field of security carried on by the experts of the IoTnuggets project, and also the collaboration of a group of experts from the University of Deusto in the field of IoT and cybersecurity between Those of us who want to highlight Borja Sanz (University of Deusto), José Ignacio Vázquez (University of Deusto). There has been also vey interesting contributions from industry, and specially, Carlos Laorden (Etxe-tar) and Carlos Polo (NTS).

In addition to their contributions, a vast internet research has been carried on, focused on basic concepts, awareness about the importance of security and threats and specific risk environments and security application. A deep search on different level training courses about cybersecurity and IoT have also been carried on in Spanish Universities o different VET training courses.

Due to the methodology used in IoTnuggets videos, use cases and short material have been focused and references taken into consideration for the composition of the syllabus and elaboration of materials are indicated below organized by themes.





Introduction to IoT Security

Secure all the (Internet of) Things <http://searchsecurity.techtarget.com/feature/Secure-all-the-things> (accessed on 02/19)

Internet of things security is relevant to business, says researcher
<http://www.computerweekly.com/news/2240220811/Internet-of-things-security-is-relevant-to-business-says-researcher> (accessed on 02/19)

Hacked by your fridge? When the Internet of Things bites back
<http://www.theguardian.com/media-network/media-network-blog/2014/feb/28/internet-things-hacked-security> (accessed on 02/19)

The Internet of Things Brings Far-Reaching Security
<http://www.cio.com/article/2462407/mobile-security/the-internet-of-things-brings-far-reaching-security-threats.html> (accessed on 02/19)

IoT Ethics and Privacy

Ethical Challenges of the Internet of Things <http://www.scmagazine.com/ethical-challenges-of-the-internet-of-things/article/331460/> (accessed on 02/19)

The Ethics of Autonomous Cars
<http://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/> (accessed on 02/11)

Wolf Richter: Goal of Booming “Internet of Things”: Monitoring, Sensing, Remote Control – Factory Workers First, You Next <http://www.nakedcapitalism.com/2014/08/wolf-richter-goal-of-booming-internet-of-things.html> (accessed on 02/19)

Tech savvy homeowners expect connected homes, woory about privacy, breaches
<http://www.scmagazine.com/tech-savvy-homeowners-expect-connected-homes-worry-about-privacy-breaches/article/357467/> (accessed on 02/19)

Privacy matters in the ‘internet of things; innovation race
<http://www.telegraph.co.uk/technology/internet-security/10805051/Privacy-matters-in-internet-of-things-innovation-race.html> (accessed on 02/19)

Does Privacy Exist on the Internet of Things? <http://www.business2community.com/tech-gadgets/privacy-exist-internet-things-0985734> (accessed on 02/19)

80% of consumers fear privacy invasion in the Internet of Things revolution
<http://tech.firstpost.com/news-analysis/80-percent-consumers-fear-privacy-invasion-internet-things-revolution-231621.html> (accessed on 02/19)

Building Automation and Security

Tridium vulnerability throws building controls wide open to hackers



<http://www.infosecurity-magazine.com/view/30620/tridium-vulnerability-throws-building-controls-wide-open-to-hackers/> (accessed on 02/19)

Another Honeywell ICS vulnerability rears its head in building control

<http://www.infosecurity-magazine.com/view/31203/another-honeywell-ics-vulnerability-rears-its-head-in-building-control/> (accessed on 02/19)

Videos:

How hackers can invade your home <http://money.cnn.com/video/technology/2013/08/14/t-hack-my-baby-monitor-and-house.cnnmoney> (accessed on 02/19)

How hackers can unlock your door <http://money.cnn.com/video/technology/2013/12/10/t-hackers-unlock-door.cnnmoney/index.html> (accessed on 02/19)

How hackers can turn out your lights

<http://money.cnn.com/video/technology/2013/12/10/t-hackers-turn-out-your-lights.cnnmoney/index.html> (accessed on 02/19)

IoT in Energy and Environment

Report: Australia energy grid, gov't, vulnerable to cyber threat

<http://www.scmagazine.com/report-australia-energy-grid-govt-vulnerable-to-cyber-threat/article/345516/> (accessed on 02/19)

The 'Smart Grid' Will Expose Utilities to Smart Computer Hackers

<http://www.nytimes.com/cwire/2011/04/19/19climatewire-a-smart-grid-will-expose-utilities-to-smart-28110.html?pagewanted=1> (accessed on 02/19)

Smart Grids Require Better Protection from Cyberattacks, Experts Say

<http://www.smartplanet.com/blog/bulletin/smart-grids-demand-better-protection-from-cyberattacks/> (accessed on 02/19)

IoT in Infrastructure

NY Times: Stuxnet was a US-Israeli effort to disrupt Iran's nuclear program

<http://www.infosecurity-magazine.com/view/15331/ny-times-stuxnet-was-a-usisraeli-effort-to-disrupt-irans-nuclear-program> (accessed on 02/19)

Stoking the Flames of Cyber War <http://www.infosecurity-magazine.com/view/27434/stoking-the-flames-of-cyber-war> (accessed on 02/19)

Hacking a Car with a \$20 Gadget <http://www.infosecurity-magazine.com/view/36867/hacking-a-car-with-a-20-gadget/> (accessed on 02/19)

Videos:

Hackers control car's steering and brakes



<http://money.cnn.com/video/technology/security/2013/08/02/t-hack-my-car.cnnmoney/>
(accessed on 02/19)

IoT in Healthcare

The Prognosis for Medical Device Security

<http://money.cnn.com/video/technology/security/2013/08/02/t-hack-my-car.cnnmoney/>
(accessed on 02/19)

GAO Report – FDA Should Expand Its Consideration of Information Security for Certain Types of Devices <http://www.gao.gov/products/GAO-12-816> (accessed on 02/19)

The Insecure Pacemaker: FDA Issues Guidance for Wireless Medical Device Security

<http://www.infosecurity-magazine.com/view/34151/the-insecure-pacemaker-fda-issues-guidance-for-wireless-medical-device-security/> (accessed on 02/19)

Radio Frequency Wireless Technology in Medical Devices. Guidance for Industry and Food and Drug Administration Staff.

<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf> (accessed on 02/19)

IoT Consumer Electronics

Hey does your Smart TV have a mic? Enjoy your surveillance, bro

http://www.theregister.co.uk/2014/05/10/smarttv_bugging/ (accessed on 02/19)

5 Things to Consider before Wiring up your Smart Home

http://www.theregister.co.uk/2014/05/10/smarttv_bugging/ (accessed on 02/19)

Man Hacks Monitor, Screams at Baby Girl <http://www.nbcnews.com/tech/security/man-hacks-monitor-screams-baby-girl-n91546> (accessed on 02/19)

Refrigerator among devices hacked in Internet of things cyber attack

<http://www.latimes.com/business/technology/la-fi-tn-refrigerator-hacked-internet-of-things-cyber-attack-20140116-story.html> (accessed on 02/19)

Videos

The camera in your TV is watching you

<http://money.cnn.com/video/technology/security/2013/08/01/t-tv-is-watching-you.cnnmoney/> (accessed on 02/19)